Article

An intelligent and secure package sensoring logistics system based on a subliminal channel

Chin-Ling Chen[1,2,3], Yong-Yuan Deng[3,*], Chun-Ta Li[4,*], and Shunzhi Zhu[1,*]

[1]School of Computer and Information Engineering, Xiamen University of Technology, Xiamen, P.R. China
[2]School of Information Engineering, Changchun Sci-Tech University, Changchun 130600, China
[3]Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung, Taiwan, R.O.C.
[4]Department of Information Management, Tainan University of Technology, 529 Zhongzheng Road, Tainan 71002, Taiwan
*Correspondence: E-Mail: allen.nubi@gmail.com (Y.Y. Deng); th0040@mail.tut.edu.tw(C. T. Li); szzhu@xmut.edu.cn (S. Zhu)

Abstract: As e-commerce services and Internet technology have rapidly developed in recent years, many services and applications integrating these technologies can now be completed online. These commercial activities include online auctions, online ticketing and online payments. The client shops from the store online, andthe store delivers the goods to the client. The goods can be divided into digital products without entities, as well as actual entities. If it is a physical product, the store will deliver the package to the client through itslogistics. However, there have been many cases of switched goods purchased by clients in recent years. Earlier, some scholars proposed a security mechanism with a subliminal channel for E-cash and digital content. Only the sender and the receiver would know that the secret information was hidden in the signature. So the privacy of this subliminal message couldbe ensured. We apply this concept to the logistics environment to design secure logistics architecture with subliminal messages. The client can check the subliminal message of the received package, and know whether the package has been switched by malicious people. In addition, the proposed scheme also applies sensor technology;the client can check the GPS location, the temperature and humidity at any time during the delivery process. So intelligent logisticswouldthereby be achieved. This paper proposes an intelligent and secure package sensoring logistics system based on a subliminal channel. The proposed architecture uses the related mechanisms tosolve the problems of a logistics system, including how to achieve mutual authentication, data integrity, anti-switch package, package location and status tracing, resisting replay attacks, forward and backward secrecy, and non-repudiation issues.

Keywords: sensor; intelligent logistics; subliminal channel; BAN logic; mutual authentication; anti-switch package; package tracing

---

1. Introduction

1.1 Background

With the rapid development of the Internet, e-commerce services have flourished. Many shopping and financial transactions can be completed online. These commercial activities include online auctions, online ticketing and online payments. In the past, we needed to go to a physical place to

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 January 2019 doi:10.20944/preprints201901.0052.v1

buy lottery tickets and complete other B2B, B2C, C2C, O2O, etc., business deals. Now, we can process these transactions via the Internet [1].

People conduct online transactions through the Internet. The purchase of goods can be divided into digital products without entities, as well as entities. There are many researches on the transaction security for non-entity digital goods, so that merchants can safely deliver digital goods to consumers, and prevent the digital goods from being copied or stolen [2-4]. If it is a physical product, the store will entrust their logistics to deliver the goods to the client. In general, we can wait for the arrival of the merchandise after completing the purchase of the merchandise.

However, with the increasing number of logistics transactions, the risk of shipping also increases. Recently, there have been many cases of switched goods which were purchased by clients.The clients pay the store to buy high-priced goods A, but receive low-cost goods B. Although most of the losses are suffered by the stores and the logistics, consumer disputes reduce consumer trust in online shopping [5-7].

Such a situation mostlyoccurs due to the distribution process; the commodity is switched by malicious people. Before the clients sign and unseal the goods, there is no way to know whether the goods in the package are the products they purchased from the stores. After the clients uncover the goods and make a report to the store, they may also suffer the suspicion of the store, so that the clients and stores are in a state of mutual distrust. Some logistics-related literature mentions this problem, but currently no literature focuses on the security mechanism to solve this issue [8-9]. Therefore, to avoid such situations, we provide a completely new architecture for logistics security.

Earlier, some scholars proposed a security mechanism with a subliminal channel for E-cash and digital content [10-12].The sender and the receiver agreed in advance on a secret message, withthe sender hidingamessage in the signature.When the receiver receives the message, it can restore the secret message hidden in the signature to know whether the message has been tampered with.Other people who are not the sender or receiver can't know that the secret information is hidden in the signature, so the privacy of this subliminal message can be ensured.

We apply this concept to the logistics environment to design secure logistics architecture with subliminal messages [13-15]. When the clients buy merchandise from the store, they generate a good deal of subliminal messages, and the store delivers the merchandise to the client through the logistics. The client will check the subliminal message hidden in the signature; if the client finds the subliminal message in the signature is different from the original agreement with the store, it means that the original package has been switched by malicious people.

In addition, when clients buy high-priced merchandise from a store or fresh food that requires full control of temperature, the clients will request to know the status of the delivery at any time. At present, in the production and distribution of frozen goods, cold chain logistics technology has been applied so that the goods are always in a stable low-temperature environment in production, storage, transportation and sales to maintain the quality of the products, mainly includingfood, agricultural products and medical fields, to achieve the concept of intelligent logistics [16].

Intelligent logistics, namely the integration of the front-end smart incubator sensed temperature and humidity data, and location information, to provide advanced information fusion, data analysis, temperature and humidity tracking capabilities,offers users a comprehensive information query platform [17]. The client hopes that he/she can query the GPS location, temperature and humidity information anytime during the package delivery process. Therefore, it is necessary to apply the sensor-related technology and cryptography-related mechanism to establish a secure and traceable logistics system under the concept of intelligent logistics.

We combined the concept of intelligent logistics with the subliminal message-equipped security mechanismto propose intelligent secure logistics architecture based on the subliminal channel.In addition to the subliminalmessage contained in the merchandise, when the store delivers the goods to the logistics, the logistics will attach a sensor on the package to provide immediate delivery status query of the product.

For the distribution of physical goods purchased by the clients, this study provides a complete logistics solution that can effectively solve the current shortage of logistics services.When the clients

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 January 2019 doi:10.20944/preprints201901.0052.v1

purchase goods from the store, they agree on a subliminal message, the store hides the message in the signature and delivers the goods to the logistics.The logistics will attach a sensor on the packageand deliver the package to the deliverer.

During the transportation of goods, the client can check the location of the goods at any time. If there is a requirement for the temperature and humidity, the sensor can also provide the relevant data so that the client can fully grasp the status of the delivery of the goods [18].When the merchandise is delivered, the client may also check the subliminal messagehidden in the signature to confirm whether the product has been switched.

The remainder of this paper is arranged as follows. Section 2 gives a brief preliminary introduction and security requirements. Section 3 presents the proposed intelligent and secure package sensoring logistics system based on a subliminal channel. Section 4 presents a security analysis, computation cost and communication performance of the proposed scheme. Section 5 offers conclusions.

2. Preliminary introduction and security requirements

2.1 Preliminary introduction

2.1.1 BAN Logic Model

The BAN logic model [19] is used to provethe correctness of a scheme. Recently, many authentication schemeshave applied BAN logic to provethe correctness of authentication and key establishment. The notation of BAN logic is described as follows:

$P|\equiv X$: *P* believes *X*, or *P* would be entitled to believe *X*.

$P \triangleleft X$: *P* sees *X*. Someone has sent a message containing *X* to *P*, who can read and repeat *X*.

$P|\sim X$: *P* once said *X*. *P* at some time sent a message including *X*.

$P |\Rightarrow X$: *P* has jurisdiction over*X*. *P* is an authority on *X* and should betrustedon this matter.

$<X>_Y$:This represents *X* combined with *Y*.

$\#(X)$: The formula *X* is fresh, that is, *X* has not been sent in a messageat anytime before the current run of the protocol.

$P \overset{K}{\leftrightarrow} Q$: *P* and *Q* may use the shared key *K* to communicate.

$P \overset{S}{\Leftrightarrow} Q$:The formula *S* is a secret known only to *P* and *Q* and possibly to principalstrusted by them.

2.1.2Diffie-Hellman Key Exchange

The Diffie-Hellman key exchange [20] is a method forsecurely exchanging cryptographic keys over a public channel and was one of the first public-key protocols, as originally conceptualized by Ralph Merkle and named after Whitfield Diffie and Martin Hellman. It is one of the earliest practical examples of public key exchange implemented within the field of cryptography.

Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical channel, such as paper key lists transported by a trusted courier. The Diffie-Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications by using a symmetric key cipher.

The following problems exist for the Diffie-Hellman method:

Computational Diffie–Hellman (CDH) Problem: Given aP and bP , where $a,b \in R$, Z_q^* and P are the generator of G , compute the value abP .

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 January 2019 doi:10.20944/preprints201901.0052.v1

Decisional Diffie-Hellman (DDH) Problem: Given aP , bP and cP, where $a,b,c \in R$, Z_q^* and P are the generator of G , confirm whether or not $cP = abP$, which is equal to confirming whether or not $c = ab \bmod q$.

2.1.3Subliminal Channel

The concept of the subliminal channel was first proposed by Simmons [21-23]. A subliminal channel is a covert signalthat can be used to send a secret message to the designated receiver,but the message cannot be recognized by any undesignatedreceiver.

In 1984, Simmons defined the narrowband and broadband subliminalchannels [21]. He showed that in any digital signature scheme, x bits are used to communicate;the signatureprovides y bits of security against forgery, alteration or transplantationof a legitimate signature, where $x>y$. The remaining $x–y$bits are potentially available for subliminal communication. If thesubliminal channel uses all, or nearly all, the $x–y$ bits, it is calledbroadband, while if it uses only a very small fraction of the $x–y$bits, it is called narrowband.

Simmons proposed protocols for the digital signaturesin the subliminal channel [22-23]. He created a model of the subliminal channel usedin the digital signature.Even if outsiders read the transmission messageand check the signature of the subliminal channel, they willnot find any errors or discrepancies.

2.2 Security Requirements

The security requirements of a robust package sensoring logistics system based on subliminal channel are listed as follows:

2.2.1 Mutual Authentication

In the information transmission process, the message receiver must be able to verify the identity legitimacy of the sender. Thus, each party must be able to verify the identity legitimacy of the other party in a robust logistics system environment. If the two parties can confirm each other's identities, then mutual authentication can be achieved [24].

2.2.2 Data Integrity

Any information transferred in an unencrypted network environment is vulnerable to malicious attack in the form of modification, where the message delivered to the receiver is not the original message transmitted by the sender. The integrity of the transmitted data must therefore be ensured, and protected against tampering in transmission [25].

2.2.3 Anti-Switch Package

Malicious attacks attempt to switch the high value package to the lower value one. It means the package received by the receiver isn't the original one that sent by the sender. Thus, an intelligent and secure package sensoring logistics system based on subliminal channel must achieve an anti-switch package [26].

2.2.4 Intelligent and Secure Package Tracing

During the delivery process of merchandise, especially high-price goods, it is important to get the GPS location of the package anytime. Especially for some fresh food delivery service, it is also important to monitor the temperature during the delivery process. Thus, in a robust logistics system, a legal user must be able to query the GPS location or temperature anytime during the delivery process [26].

2.2.5 Resisting Replay Attacks

Malicious attacks may also intercept the transmitted message between the sender and the receiver, and then impersonate a legitimate transmitter in order to send the same message to the intended receiver. This constitutes a serious security risk that must be prevented [27].

2.2.6 Forward and Backward Secrecy

If the session key between the sender and the receiver is compromised at any point by an attacker, the attacker may use the session key for future malicious communications, or use it to obtain previous messages [28-29].

2.2.7 Non-Repudiation

In the information transmission process, the message receiver must be able to verify the identity legitimacy of the sender. Once the receiver confirms that the message was sent from the sender, the sender can't deny the message that he/she had sent. The sender uses his/her private key to sign the message, and the receiver can verify the digital signature from the sender [30].

3. The Proposed Scheme

3.1 System Architecture

The system framework of the proposed scheme in this study is shown in Figure 1.
There are six parties in the scheme:

(1) Certificate Authority: A trusted third party agency which provides the public key and private key to the registrant.
(2) Store: An online shopping store. People can shop there, and the store sends the goods to the customers.
(3) Client: A person who buys things from the store online; he/she will sign for the delivery package.
(4) Logistics: A company collects the packages that is entrusted to be sent by the store, and delivers them to the client.
(5) Deliverer: A person who is employed by the logistics company, and assists logistics to deliver the package to the client.
(6) Package: Merchandise sent by the store to the client;the tag and sensor are attached outside the package.

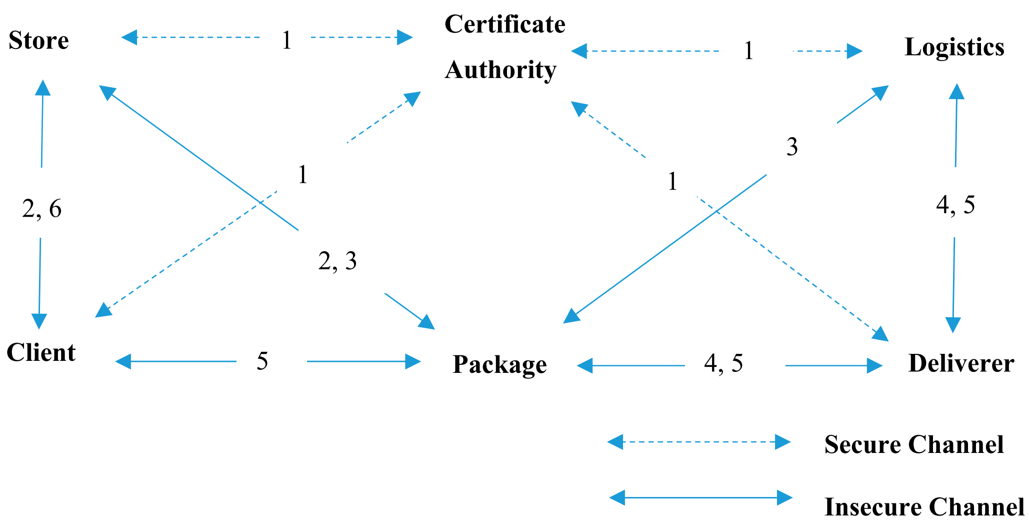

Figure 1. System framework of the proposed scheme

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 January 2019 doi:10.20944/preprints201901.0052.v1

1. All stores, clients, logistics, and deliverers must register with the certificate authority through a secure channel. The stores, clients, logistics, and deliverers will get public keys and private keys from the certificate authority.
2. The client purchases merchandise from the store, and they negotiate a subliminal message. The store sends the related messages to the client, and prepares to write the subliminal message onto the tag attached outside the package.
3. The store takes the package to the logistics for delivery. After mutual authentication between the store and logistics; the store sends the related shopping information to the logistics, including subliminal message, and writes it onto the tag via logistics.
4. The deliverer takes the package from the logistics. After mutual authentication between the deliverer and the logistics, the logistics writes the related delivery information onto the sensor attached outside the package. The package is sent to the client by the deliverer.
5. The client checks the information on the tag provided by the deliverer. The client sends the receipt about the package, and the deliverer will transfer the receipt to the logistics.

3.2 Notations

PK_x, SK_x	: x's public key and private key, issued by Certificate Authority
r_{xy}	: A random number selected for parties x and y
$skey_x$	: Partial public parameters for party x
$skey_{xy}$	: The session keyfor parties x and y
C_{xy}	: The encrypted messagefor parties x and y
Sig_{xy}	: The signed messagefor parties x and y
$E_{PK_x}(m)$	: Use x's public key PK_x to encrypt the message m
$D_{SK_x}(m)$	: Use x's private key SK_x to decrypt the message m
$S_{SK_x}(m)$	: Use x's private key SK_x to sign the message m
$V_{PK_x}(m)$	: Use x's public key PK_x to verify the message m
$E_{skey_{xy}}(m)$	: Use the session key $skey_{xy}$ to encrypt the message m
$D_{skey_{xy}}(m)$	: Use the session key $skey_{xy}$ to decrypt the message m
k, y_s, r_s, S_s	: The parameters for the subliminal channel
SM_{xy}	: The subliminal messagefor parties x and y
Q_{xy}	: The client x wants to query the delivery status of the package y
$h(m)$	: The message$m$ calculated by one-way hash function $h(\ )$
ID_x	: x's identity
TID	: A transaction number which is changed every round
$M_{\inf}$	: The client's shopping information
$D_{\inf}$	: The client's delivery information
$S_{\inf}$	: The sensor's sensoring information, like GPS location or temperature
$R_{\inf}$	: The receipt signed by the client
$x \stackrel{?}{=} y$	: Determines if x is equal to y

3.3Purchase Phase

The client and the store must negotiate a secret key through a key agreement; they can then communicate with each other. The client proposes a subliminal message in the purchase phase. The purchase phase of the proposed scheme is shown in Figure 2.

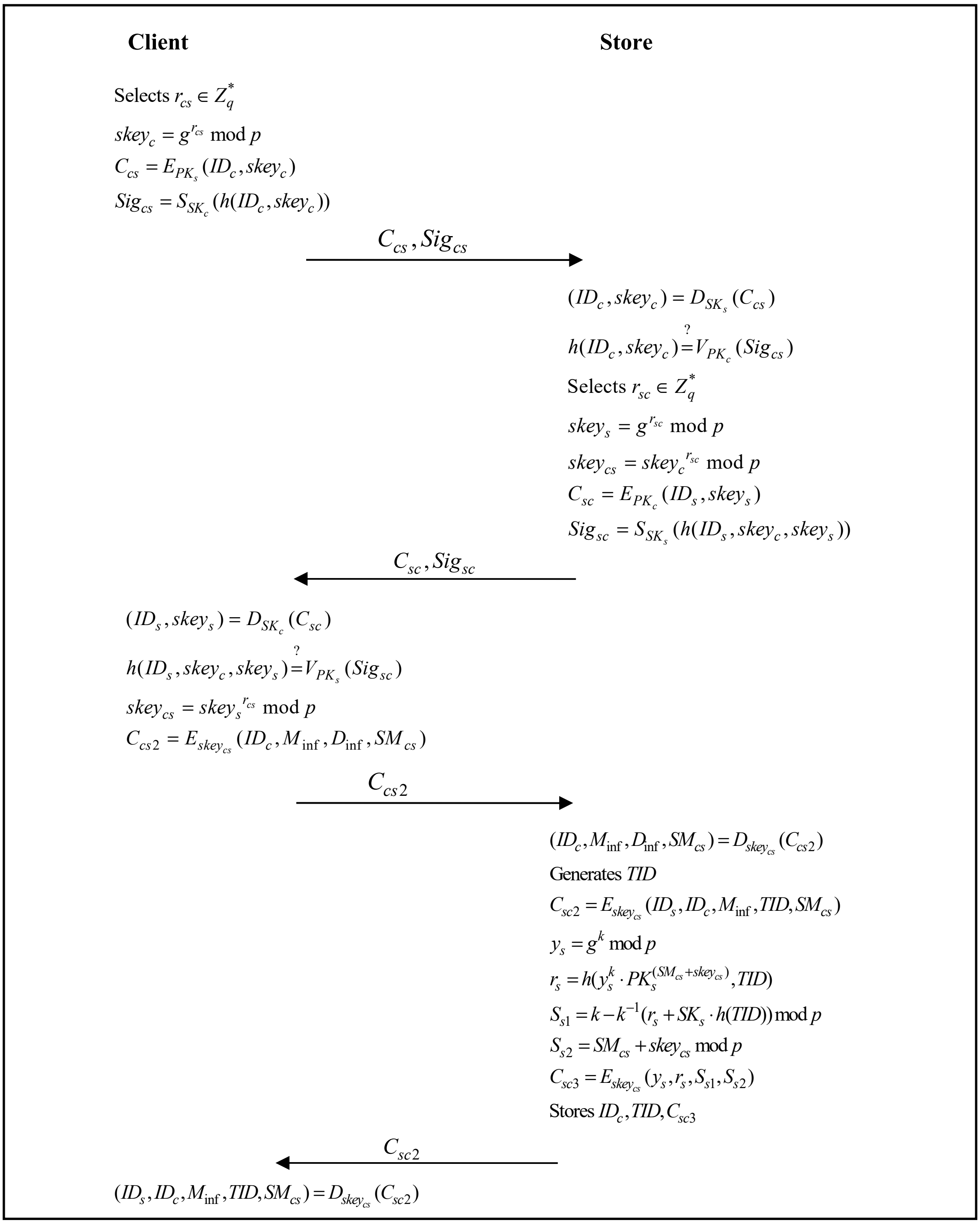

Figure 2. Purchase phase of the proposed scheme

Step 1: The client selects $r_{cs} \in Z_q^*$, calculates

$$skey_c = g^{r_{cs}} \bmod p, \tag{1}$$

$$C_{cs} = E_{PK_s}(ID_c, skey_c), \tag{2}$$

$$Sig_{cs} = S_{SK_c}(h(ID_c, skey_c)), \tag{3}$$

and then sends (C_{cs}, Sig_{cs}) to the store.

Step 2: The store decrypts

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 January 2019 doi:10.20944/preprints201901.0052.v1

$$(ID_c, skey_c) = D_{SK_s}(C_{cs}), \quad (4)$$

and verifies

$$h(ID_c, skey_c) \stackrel{?}{=} V_{PK_c}(Sig_{cs}). \quad (5)$$

If it passes the verification, then the store authenticates the legality of the client. The store selects $r_{sc} \in Z_q^*$, calculates

$$skey_s = g^{r_{sc}} \bmod p, \quad (6)$$

$$skey_{cs} = skey_c^{\,r_{sc}} \bmod p, \quad (7)$$

$$C_{sc} = E_{PK_c}(ID_s, skey_s), \quad (8)$$

$$Sig_{sc} = S_{SK_s}(h(ID_s, skey_c, skey_s)), \quad (9)$$

and then sends (C_{sc}, Sig_{sc}) to the client.

Step 3: The client decrypts

$$(ID_s, skey_s) = D_{SK_c}(C_{sc}), \quad (10)$$

and verifies

$$h(ID_s, skey_c, skey_s) \stackrel{?}{=} V_{PK_s}(Sig_{sc}). \quad (11)$$

If it passes the verification, then the client authenticates the legality of the store. The client calculates

$$skey_{cs} = skey_s^{\,r_{cs}} \bmod p, \quad (12)$$

$$C_{cs2} = E_{skey_{cs}}(ID_c, M_{\inf}, D_{\inf}, SM_{cs}), \quad (13)$$

and then sends C_{cs2} to the store.

Step 4: The store decrypts the message

$$(ID_c, M_{\inf}, D_{\inf}, SM_{cs}) = D_{skey_{cs}}(C_{cs2}), \quad (14)$$

and generates the transaction number TID, calculates

$$C_{sc2} = E_{skey_{cs}}(ID_s, ID_c, M_{\inf}, TID, SM_{cs}), \quad (15)$$

encrypts the subliminal message with the following calculation

$$y_s = g^k \bmod p, \quad (16)$$

$$r_s = h(y_s^k \cdot PK_s^{(SM_{cs}+skey_{cs})}, TID), \quad (17)$$

$$S_{s1} = k - k^{-1}(r_s + SK_s \cdot h(TID)) \bmod p, \quad (18)$$

$$S_{s2} = SM_{cs} + skey_{cs} \bmod p, \quad (19)$$

$$C_{sc3} = E_{skey_{cs}}(y_s, r_s, S_{s1}, S_{s2}), \quad (20)$$

stores (ID_c, TID, C_{sc3}), and then sends C_{sc2} to the client.

Step 5: The client decrypts

$$(ID_s, ID_c, M_{\inf}, TID, SM_{cs}) = D_{skey_{cs}}(C_{sc2}), \quad (21)$$

and keeps the transaction number TID, the subliminal message SM_{cs}.

3.4Package Collection Phase

The store and the logistics must negotiate a secret key through a key agreement; they can then communicate with each other. The store and the logistics also generate some information and write it onto the tag attached outside the package.The package collection phase of the proposed scheme is shown in Figure 3.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 January 2019 doi:10.20944/preprints201901.0052.v1

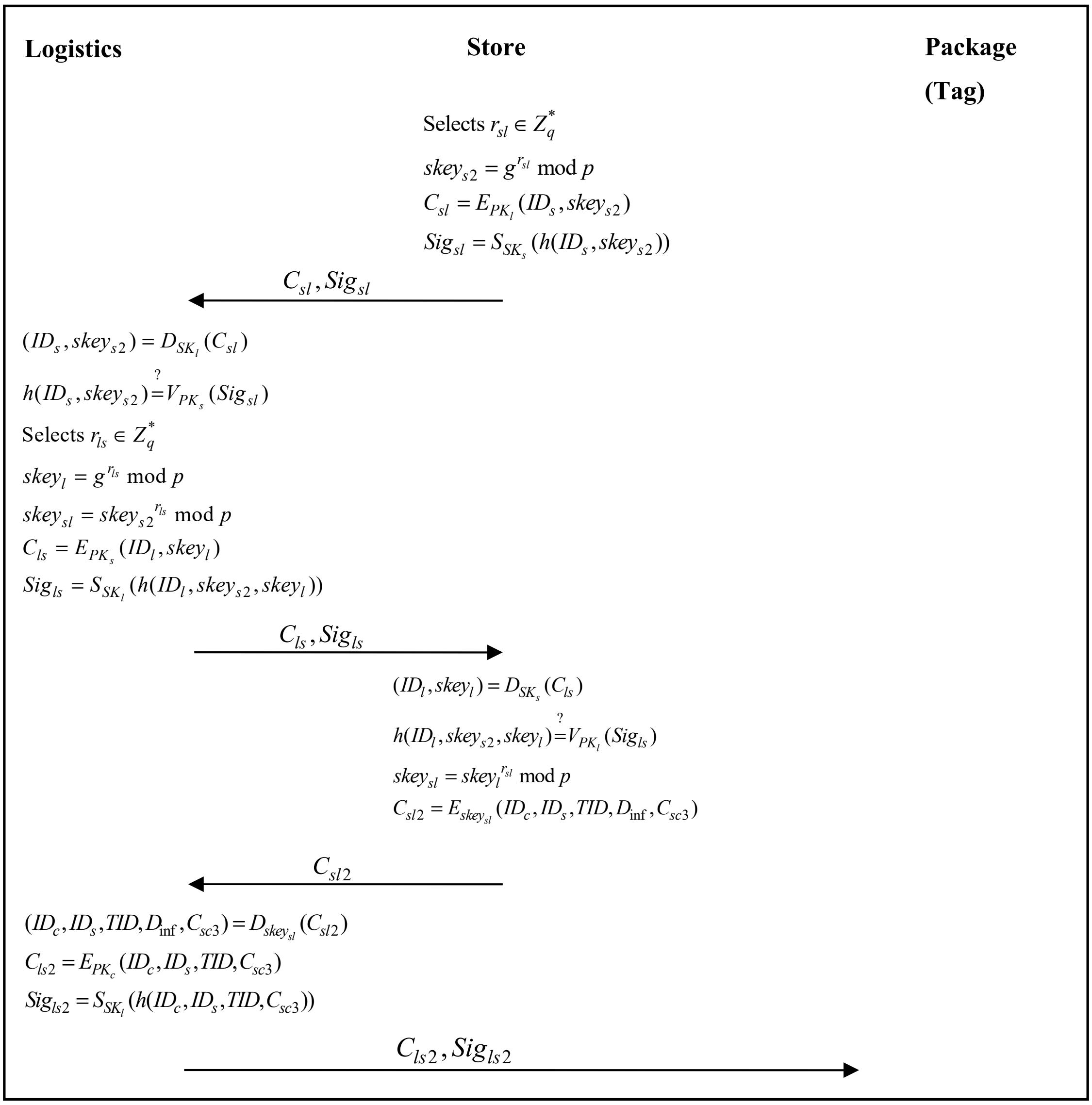

Figure 3. Package collection phase of the proposed scheme

Step 1: Thestoreselects $r_{sl} \in Z_q^*$, calculates

$$skey_{s2} = g^{r_{sl}} \bmod p, \tag{22}$$

$$C_{sl} = E_{PK_l}(ID_s, skey_{s2}), \tag{23}$$

$$Sig_{sl} = S_{SK_s}(h(ID_s, skey_{s2})), \tag{24}$$

and then sends (C_{sl}, Sig_{sl}) to the logistics.

Step 2: The logistics decrypts

$$(ID_s, skey_{s2}) = D_{SK_l}(C_{sl}), \tag{25}$$

and verifies

$$h(ID_s, skey_{s2}) \overset{?}{=} V_{PK_s}(Sig_{sl}). \tag{26}$$

If it passes the verification, then the logistics authenticates the legality of the store. The logistics selects $r_{ls} \in Z_q^*$, calculates

$$skey_l = g^{r_{ls}} \bmod p, \tag{27}$$

$$skey_{sl} = skey_{s2}^{r_{ls}} \bmod p, \tag{28}$$

$$C_{ls} = E_{PK_s}(ID_l, skey_l), \tag{29}$$

$$Sig_{ls} = S_{SK_l}(h(ID_l, skey_{s2}, skey_l)), \tag{30}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 January 2019 doi:10.20944/preprints201901.0052.v1

and then sends (C_{ls}, Sig_{ls}) to the store.

Step 3: Thestoredecrypts

$$(ID_l, skey_l) = D_{SK_s}(C_{ls}), \tag{31}$$

and verifies

$$h(ID_l, skey_{s2}, skey_l) \overset{?}{=} V_{PK_l}(Sig_{ls}). \tag{32}$$

If it passes the verification, then the store authenticates the legality of the logistics. The store calculates

$$skey_{sl} = skey_l^{r_{sl}} \bmod p \tag{33}$$

and

$$C_{sl2} = E_{skey_{sl}}(ID_c, ID_s, TID, D_{\inf}, C_{sc3}) \tag{34}$$

which includes the encrypted subliminal message C_{sc3}, then the store sends C_{sl2} to the logistics.

Step 4: The logistics decrypts the message

$$(ID_c, ID_s, TID, D_{\inf}, C_{sc3}) = D_{skey_{sl}}(C_{sl2}), \tag{35}$$

calculates

$$C_{ls2} = E_{PK_c}(ID_c, ID_s, TID, C_{sc3}), \tag{36}$$

$$Sig_{ls2} = S_{SK_l}(h(ID_c, ID_s, TID, C_{sc3})), \tag{37}$$

and then writes the message (C_{ls2}, Sig_{ls2}) to the tag which is attached outside the package.

3.5Package Dispatched Phase

The logistics and the deliverer must negotiate a secret key through a key agreement; they can then communicate with each other. The logistics also generates some information and writes it onto the sensor attached outside the package. The sensor can transfer some sensoring information to the backend logistics, like GPS location or temperature detection. The package dispatched phase of the proposed scheme is shown in Figure 4.

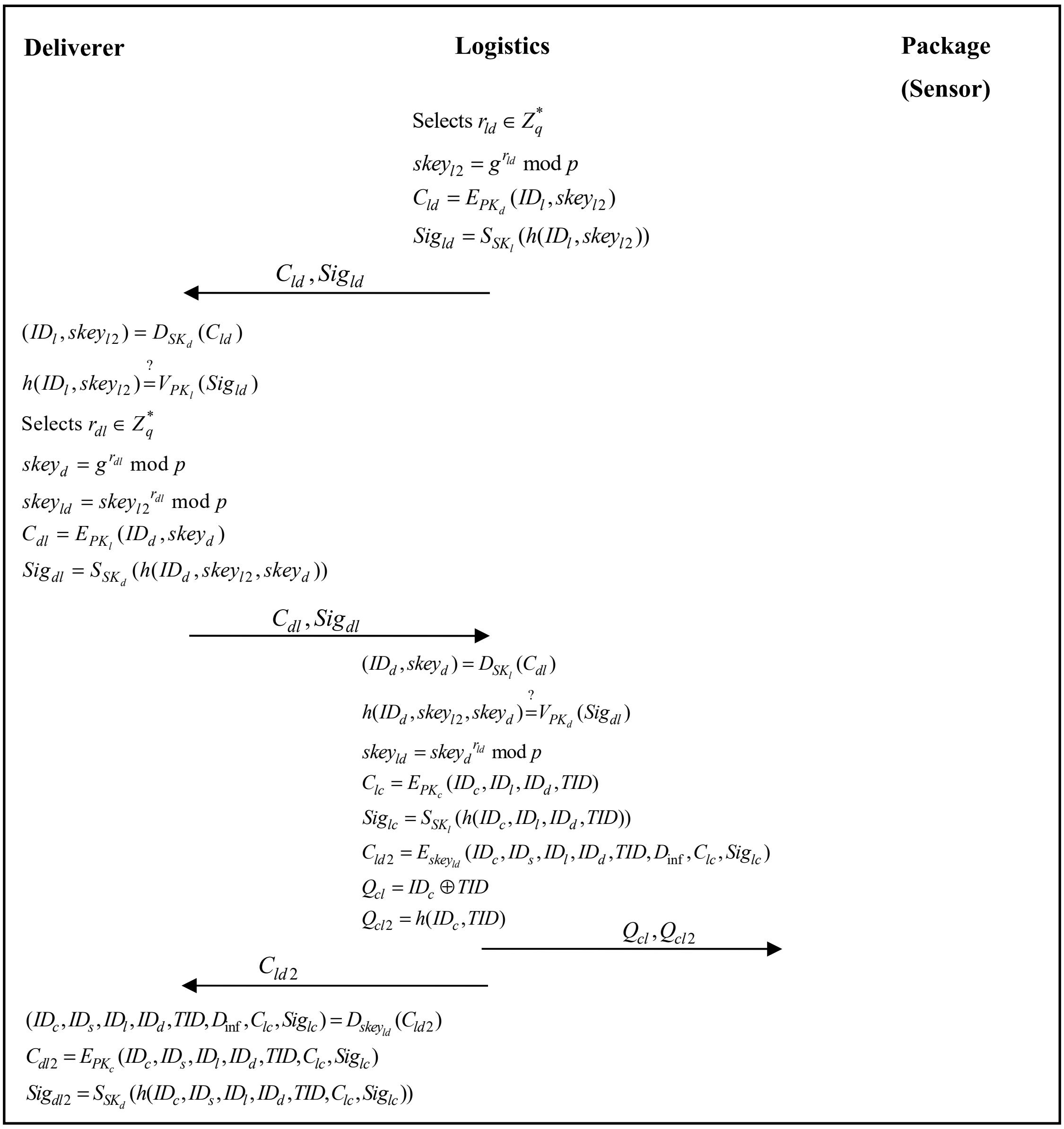

Figure 4. Package dispatched phase of the proposed scheme

Step 1: Thelogisticsselects $r_{ld} \in Z_q^*$, calculates

$$skey_{l2} = g^{r_{ld}} \bmod p, \tag{38}$$

$$C_{ld} = E_{PK_d}(ID_l, skey_{l2}), \tag{39}$$

$$Sig_{ld} = S_{SK_l}(h(ID_l, skey_{l2})), \tag{40}$$

and then sends (C_{ld}, Sig_{ld}) to the deliverer.

Step 2: The deliverer decrypts

$$(ID_l, skey_{l2}) = D_{SK_d}(C_{ld}), \tag{41}$$

and verifies

$$h(ID_l, skey_{l2}) \stackrel{?}{=} V_{PK_l}(Sig_{ld}). \tag{42}$$

If it passes the verification, then the deliverer authenticates the legality of the logistics. The deliverer selects $r_{dl} \in Z_q^*$, calculates

$$skey_d = g^{r_{dl}} \bmod p, \tag{43}$$

$$skey_{ld} = skey_{l2}{}^{r_{dl}} \bmod p, \tag{44}$$

$$C_{dl} = E_{PK_l}(ID_d, skey_d), \tag{45}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 January 2019 doi:10.20944/preprints201901.0052.v1

$$Sig_{dl} = S_{SK_d}(h(ID_d, skey_{l2}, skey_d)), \tag{46}$$

and then sends (C_{dl}, Sig_{dl}) to the logistics.

Step 3: Thelogisticsdecrypts

$$(ID_d, skey_d) = D_{SK_l}(C_{dl}), \tag{47}$$

and verifies

$$h(ID_d, skey_{l2}, skey_d) \stackrel{?}{=} V_{PK_d}(Sig_{dl}). \tag{48}$$

If it passes the verification, then the logistics authenticates the legality of the deliverer. The logistics calculates

$$skey_{ld} = skey_d^{r_{ld}} \bmod p, \tag{49}$$

$$C_{lc} = E_{PK_c}(ID_c, ID_l, ID_d, TID), \tag{50}$$

$$Sig_{lc} = S_{SK_l}(h(ID_c, ID_l, ID_d, TID)), \tag{51}$$

$$C_{ld2} = E_{skey_{ld}}(ID_c, ID_s, ID_l, ID_d, TID, D_{\inf}, C_{lc}, Sig_{lc}), \tag{52}$$

$$Q_{cl} = ID_c \oplus TID, \tag{53}$$

and

$$Q_{cl2} = h(ID_c, TID). \tag{54}$$

The logistics sends (Q_{cl}, Q_{cl2}) to the sensor attached outside the package; it also sends C_{ld2} to the deliverer.

Step 4: Thedelivererdecrypts

$$(ID_c, ID_s, ID_l, ID_d, TID, D_{\inf}, C_{lc}, Sig_{lc}) = D_{skey_{ld}}(C_{ld2}) \tag{55}$$

to get the delivery information, then calculates the messages

$$C_{dl2} = E_{PK_c}(ID_c, ID_s, ID_l, ID_d, TID, C_{lc}, Sig_{lc}) \tag{56}$$

and

$$Sig_{dl2} = S_{SK_d}(h(ID_c, ID_s, ID_l, ID_d, TID, C_{lc}, Sig_{lc})). \tag{57}$$

3.6Package Query Phase

In our proposed scheme, the client can query the delivery status of the package through the logistics anytime. After the logistics authenticates the legality of the client, the logistics sends the query request message to the sensor attached outside the package. The sensor responds the related sensoring messages likeGPS location or temperature to the client through the logistics. The package query phase of the proposed scheme is shown in Figure 5.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 January 2019 doi:10.20944/preprints201901.0052.v1

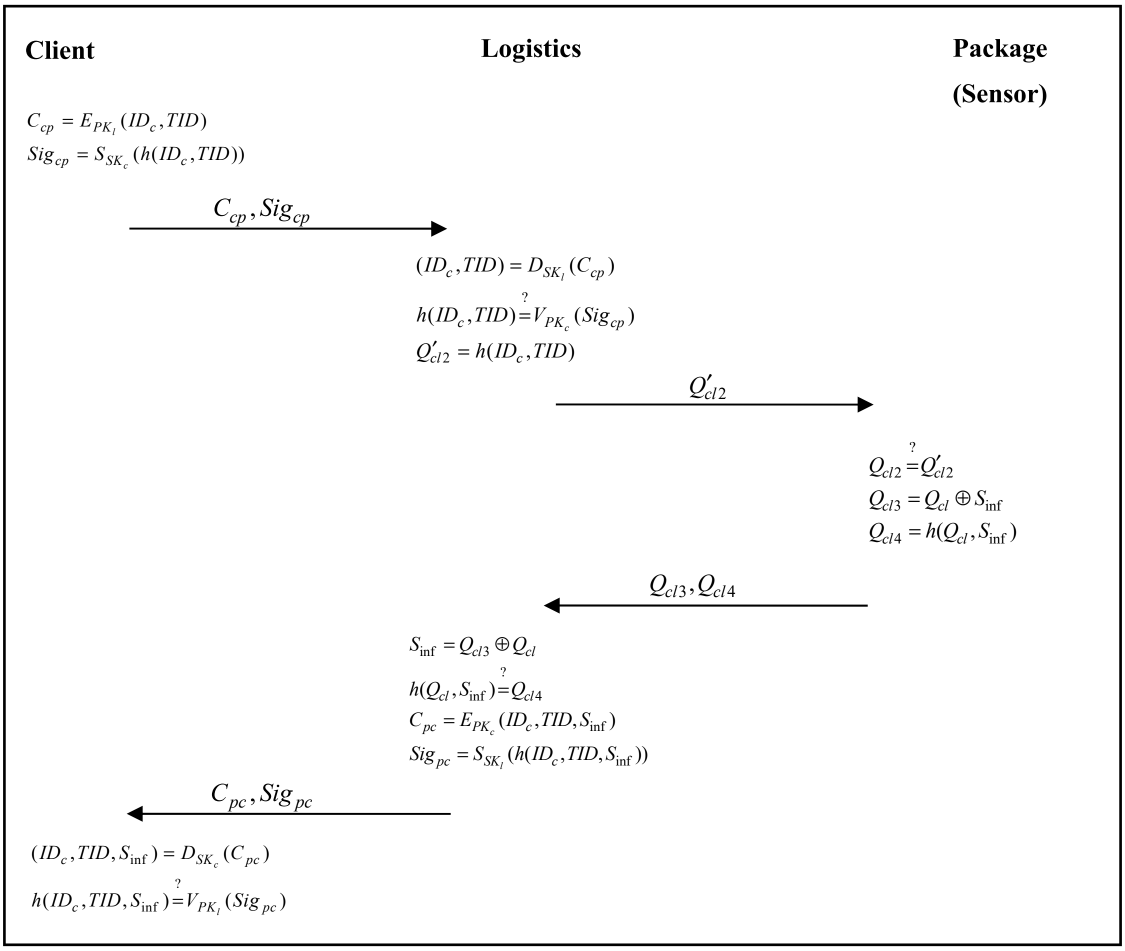

Figure 5. Package query phase of the proposed scheme

Step 1: When the client wants to query the delivery status of the package, he/she calculates

$$C_{cp} = E_{PK_l}(ID_c, TID), \tag{58}$$

$$Sig_{cp} = S_{SK_c}(h(ID_c, TID)), \tag{59}$$

and then sends (C_{cp}, Sig_{cp}) to the logistics.

Step 2: The logistics decrypts

$$(ID_c, TID) = D_{SK_l}(C_{cp}), \tag{60}$$

and verifies

$$h(ID_c, TID) \overset{?}{=} V_{PK_c}(Sig_{cp}). \tag{61}$$

If it passes the verification, then the logistics authenticates the legality of the client. The logistics calculates

$$Q'_{cl2} = h(ID_c, TID), \tag{62}$$

then sends Q'_{cl2} to the sensor attached outside the package.

Step 3: Thesensor attached outside the package verifies

$$Q_{cl2} \overset{?}{=} Q'_{cl2}. \tag{63}$$

If it passes the verification, then the sensor attached outside the package authenticates the legality of the logistics. The sensor attached outside the package calculates

$$Q_{cl3} = Q_{cl} \oplus S_{\inf}, \tag{64}$$

$$Q_{cl4} = h(Q_{cl}, S_{\inf}), \tag{65}$$

and then sends (Q_{cl3}, Q_{cl4}) to the logistics.

Step 4: The logistics decrypts

$$S_{\inf} = Q_{cl3} \oplus Q_{cl}, \tag{66}$$

 doi:10.20944/preprints201901.0052.v1

and verifies

$$h(Q_{cl}, S_{\inf}) \overset{?}{=} Q_{cl4} . \quad (67)$$

If it passes the verification, then the logistics authenticates the legality of the sensor attached outside the package. The logistics calculates

$$C_{pc} = E_{PK_c}(ID_c, TID, S_{\inf}) , \quad (68)$$

$$Sig_{pc} = S_{SK_l}(h(ID_c, TID, S_{\inf})) , \quad (69)$$

and then sends (C_{pc}, Sig_{pc}) to the client.

Step 5: Theclientdecrypts

$$(ID_c, TID, S_{\inf}) = D_{SK_c}(C_{pc}) , \quad (70)$$

and verifies

$$h(ID_c, TID, S_{\inf}) \overset{?}{=} V_{PK_l}(Sig_{pc}) . \quad (71)$$

If it passes the verification, then the client authenticates the legality of the logistics. The client also gets the GPS location or temperature $S_{\inf}$ from the sensor attached outside the package.

3.7Package Delivery Phase

When the deliverer delivers the package to the client, the client checks the legality and the transaction number. He/she also checks the transaction number and the subliminal message from the tag attached outside the package.The package delivery phase of the proposed scheme is shown in Figure 6.

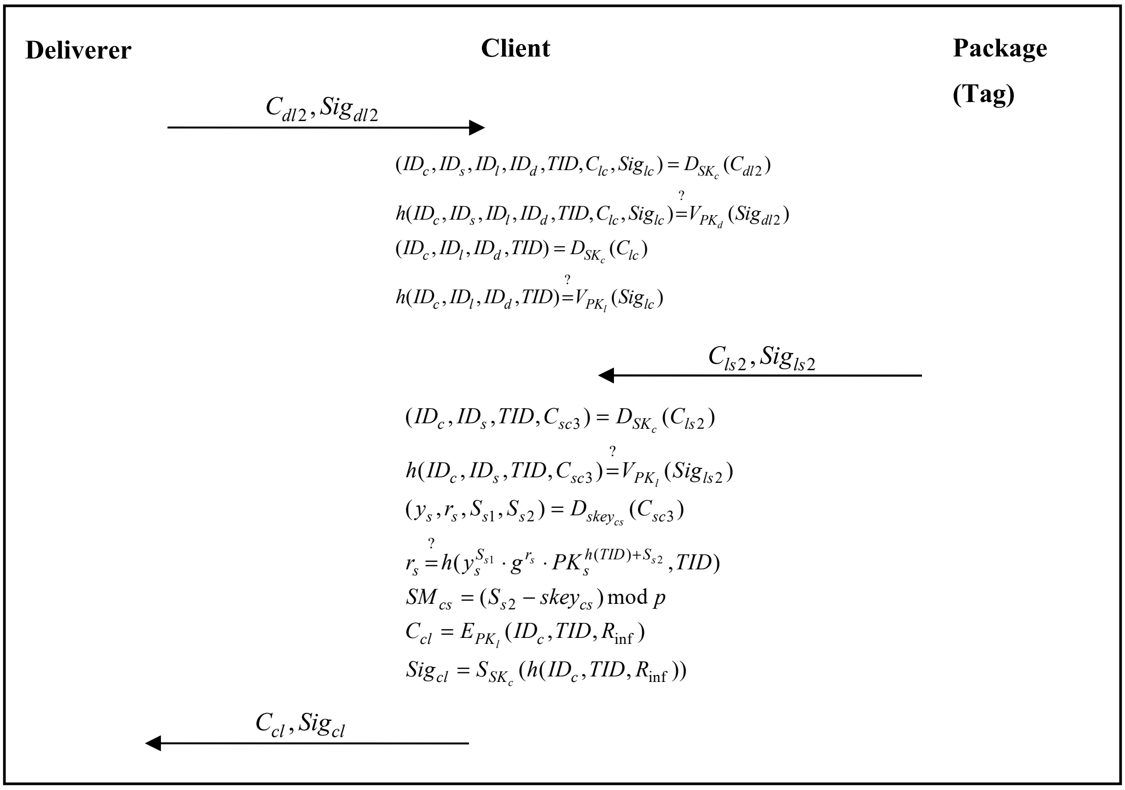

Figure 6. Package delivery phase of the proposed scheme

Step 1: When the deliverer delivers the package, he/she sends (C_{dl2}, Sig_{dl2}) to the client, the client decrypts

$$(ID_c, ID_s, ID_l, ID_d, TID, C_{lc}, Sig_{lc}) = D_{SK_c}(C_{dl2}) , \quad (72)$$

and verifies

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 January 2019 doi:10.20944/preprints201901.0052.v1

$$h(ID_c, ID_s, ID_l, ID_d, TID, C_{lc}, Sig_{lc}) \overset{?}{=} V_{PK_d}(Sig_{dl2}). \quad (73)$$

If it passes the verification, then the client authenticates the legality of the deliverer. After that, the client decrypts

$$(ID_c, ID_l, ID_d, TID) = D_{SK_c}(C_{lc}), \quad (74)$$

and verifies

$$h(ID_c, ID_l, ID_d, TID) \overset{?}{=} V_{PK_l}(Sig_{lc}). \quad (75)$$

If it passes the verification, then the client authenticates the legality of the logistics.

Step 2: The client also gets the message (C_{ls2}, Sig_{ls2}) from the tag attached outside the package.The client decrypts

$$(ID_c, ID_s, TID, C_{sc3}) = D_{SK_c}(C_{ls2}), \quad (76)$$

and verifies

$$h(ID_c, ID_s, TID, C_{sc3}) \overset{?}{=} V_{PK_l}(Sig_{ls2}). \quad (77)$$

If it passes the verification, then the client authenticates the legality of the logistics. After that, the client decrypts

$$(y_s, r_s, S_{s1}, S_{s2}) = D_{skey_{cs}}(C_{sc3}), \quad (78)$$

verifies

$$r_s \overset{?}{=} h(y_s^{S_{s1}} \cdot g^{r_s} \cdot PK_s^{h(TID)+S_{s2}}, TID), \quad (79)$$

and checks the subliminal message

$$SM_{cs} = (S_{s2} - skey_{cs}) \bmod p. \quad (80)$$

If it passes the verification, then the client authenticates the legality of the package. The clients calculates

$$C_{cl} = E_{PK_l}(ID_c, TID, R_{\inf}), \quad (81)$$

$$Sig_{cl} = S_{SK_c}(h(ID_c, TID, R_{\inf})), \quad (82)$$

and then sends (C_{cl}, Sig_{cl}) to the deliverer.

3.8Receipt Retention Phase

After the deliverer delivers the package to the client, the deliverer gets the receipt from the client. The deliverer sends the receipt to the logistics; the logistics keeps the receipt. The receipt retentionphase of the proposed scheme is shown in Figure 7.

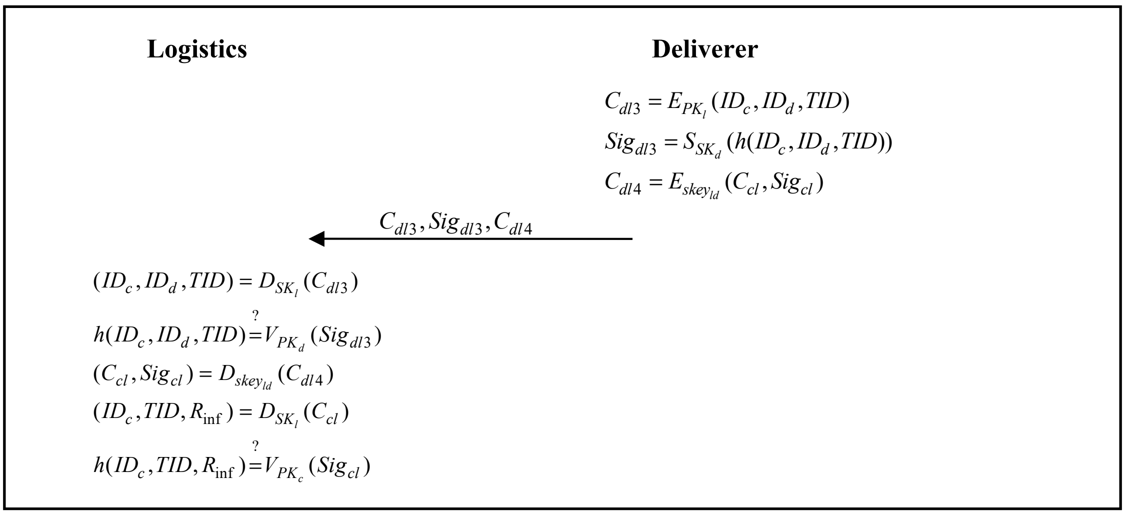

Figure 7. Receipt retention phase of the proposed scheme

Step 1: After the deliverer gets the signature message from the client, the deliverer calculates

$$C_{dl3} = E_{PK_l}(ID_c, ID_d, TID), \quad (83)$$

$$Sig_{dl3} = S_{SK_d}(h(ID_c, ID_d, TID)), \quad (84)$$

$$C_{dl4} = E_{skey_{ld}}(C_{cl}, Sig_{cl}), \quad (85)$$

and then sends $(C_{dl3}, Sig_{dl3}, C_{dl4})$ to the logistics.

Step 2: The logistics decrypts

$$(ID_c, ID_d, TID) = D_{SK_l}(C_{dl3}), \quad (86)$$

and verifies

$$h(ID_c, ID_d, TID) \overset{?}{=} V_{PK_d}(Sig_{dl3}). \quad (87)$$

If it passes the verification, then the logistics authenticates the legality of the deliverer. After that, the client decrypts

$$(C_{cl}, Sig_{cl}) = D_{skey_{ld}}(C_{dl4}), \quad (88)$$

$$(ID_c, TID, R_{\inf}) = D_{SK_l}(C_{cl}), \quad (89)$$

and then verifies

$$h(ID_c, TID, R_{\inf}) \overset{?}{=} V_{PK_c}(Sig_{cl}). \quad (90)$$

If it passes the verification, then the logistics authenticates the legality of the client.The logistics also gets the receipt $R_{\inf}$ from the client.

4. Security Analysis

4.1 Mutual Authentication

We use BAN logic to prove that our scheme achieves mutual authentication between different parties in each phase.

In the purchase phase of the proposed scheme, the main goal of the scheme is to authenticate the session key establishment between the clientC and the storeS.

$G1 \; : \; C \mid\equiv C \overset{skey_{cs}}{\leftrightarrow} S$

$G2 \; : \; C \mid\equiv S \mid\equiv C \overset{skey_{cs}}{\leftrightarrow} S$

$G3 \; : \; S \mid\equiv C \overset{skey_{cs}}{\leftrightarrow} S$

$G4 \; : S \mid\equiv C \mid\equiv C \overset{skey_{cs}}{\leftrightarrow} S$

$G5 \; : \; C \mid\equiv ID_s$

$G6 \; : \; C \mid\equiv S \mid\equiv ID_s$

$G7 \; : \; S \mid\equiv ID_c$

$G8 \; : \; S \mid\equiv C \mid\equiv ID_c$

According to the purchase phase, we use BAN logic to produce an idealized form as follows:

$M1 \; : \; (< ID_c, skey_c >_{PK_s}, < h(ID_c, skey_c) >_{SK_c})$

$M2 \; : \; (< ID_s, skey_s >_{PK_c}, < h(ID_s, skey_c, skey_s) >_{SK_s})$

To analyze our improved scheme, we make the following assumptions:

$A1 \; : \; C \mid\equiv \#(skey_c)$

$A2 \; : \; S \mid\equiv \#(skey_c)$

$A3 \; : \; C \mid\equiv \#(skey_s)$

$A4 \; : \; S \mid\equiv \#(skey_s)$

$A5 \; : \; C \mid\equiv S \mid\Rightarrow C \overset{skey_{cs}}{\leftrightarrow} S$

$A6 \; : \; S \mid\equiv C \mid\Rightarrow C \overset{skey_{cs}}{\leftrightarrow} S$

A7 : $C \mid\equiv S \mid\Rightarrow ID_s$

A8 : $S \mid\equiv C \mid\Rightarrow ID_c$

According to those assumptions and the rules of BAN logic, we show the main proof of the purchase phase as follows:

a. Store*S* authenticates client*C*.

By *M1* and the *seeing rule*, we can derive:

$S \triangleleft (<ID_c, skey_c>_{PK_s}, <h(ID_c, skey_c)>_{SK_c})$ (*Statement 1*)

By *A2* and the *freshness rule*, we can derive:

$S \mid\equiv \#(<ID_c, skey_c>_{PK_s}, <h(ID_c, skey_c)>_{SK_c})$ (*Statement 2*)

By (*Statement 1*), *A4* and the *message meaning rule*, we can derive:

$S \mid\equiv C \mid\sim (<ID_c, skey_c>_{PK_s}, <h(ID_c, skey_c)>_{SK_c})$ (*Statement 3*)

By (*Statement 2*), (*Statement 3*), and the *nonce verification rule*, we can derive:

$S \mid\equiv C \mid\equiv (<ID_c, skey_c>_{PK_s}, <h(ID_c, skey_c)>_{SK_c})$ (*Statement 4*)

By (*Statement 4*) and the *belief rule*, we can derive:

$S \mid\equiv C \mid\equiv C \overset{skey_{cs}}{\leftrightarrow} S$ (*Statement 5*)

By (*Statement 5*), *A6* and the *jurisdiction rule*, we can derive:

$S \mid\equiv C \overset{skey_{cs}}{\leftrightarrow} S$ (*Statement 6*)

By (*Statement 6*) and the *belief rule*, we can derive:

$S \mid\equiv C \mid\equiv ID_c$ (*Statement 7*)

By (*Statement 7*), *A8* and the *jurisdiction rule*, we can derive:

$S \mid\equiv ID_c$ (*Statement 8*)

b. Client*C* authenticates store*S*.

By *M2* and the *seeing rule*, we can derive:

$C \triangleleft (<ID_s, skey_s>_{PK_c}, <h(ID_s, skey_c, skey_s)>_{SK_s})$ (*Statement 9*)

By *A1* and the *freshness rule*, we can derive:

$C \mid\equiv \#(<ID_s, skey_s>_{PK_c}, <h(ID_s, skey_c, skey_s)>_{SK_s})$ (*Statement 10*)

By (*Statement 9*), *A3* and the *message meaning rule*, we can derive:

$C \mid\equiv S \mid\sim (<ID_s, skey_s>_{PK_c}, <h(ID_s, skey_c, skey_s)>_{SK_s})$ (*Statement 11*)

By (*Statement 10*), (*Statement 11*), and the *nonce verification rule*, we can derive:

$C \mid\equiv S \mid\equiv (<ID_s, skey_s>_{PK_c}, <h(ID_s, skey_c, skey_s)>_{SK_s})$ (*Statement 12*)

By (*Statement 12*) and the *belief rule*, we can derive:

$C \mid\equiv S \mid\equiv C \overset{skey_{cs}}{\leftrightarrow} S$ (*Statement 13*)

By (*Statement 13*), *A5* and the *jurisdiction rule*, we can derive:

$C \mid\equiv C \overset{skey_{cs}}{\leftrightarrow} S$ (*Statement 14*)

By (*Statement 14*) and the *belief rule*, we can derive:

$C \mid\equiv S \mid\equiv ID_s$ (*Statement 15*)

By (*Statement 15*), *A7* and the *jurisdiction rule*, we can derive:

$C \mid\equiv ID_s$ (*Statement 16*)

By (*Statement 6*), (*Statement 8*), (*Statement 14*), and (*Statement 16*), we can provethe proposed scheme such that client*C* and store*S* authenticate each other. Moreover, we are also able to prove that the proposed scheme can establish a session key between client*C* and store*S*.

In the proposed scheme, the store authenticates the client by

$$h(ID_c, skey_c) \overset{?}{=} V_{PK_c}(Sig_{cs}) . \quad (5)$$

If it passes the verification, the store authenticates the legality of the client. Then, the client authenticates the store by

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 January 2019 doi:10.20944/preprints201901.0052.v1

$$h(ID_s, skey_c, skey_s) \overset{?}{=} V_{PK_s}(Sig_{sc}) . \quad (11)$$

If it passes the verification, the client authenticates the legality of the store. Hence, mutual authentication is achieved in the purchase phase between the store and client.

In package collection phase of the proposed scheme, the main goal of the scheme is to authenticate the session key establishment between logistics$L$ and store$S$.

$G9 \ : \ L |\equiv L \overset{skey_{sl}}{\leftrightarrow} S$

$G10 : \ L |\equiv S |\equiv L \overset{skey_{sl}}{\leftrightarrow} S$

$G11 : \ S |\equiv L \overset{skey_{sl}}{\leftrightarrow} S$

$G12 : S |\equiv L |\equiv L \overset{skey_{sl}}{\leftrightarrow} S$

$G13 : \ L |\equiv ID_s$

$G14 : \ L |\equiv S |\equiv ID_s$

$G15 : \ S |\equiv ID_l$

$G16 : \ S |\equiv L |\equiv ID_l$

According to the package collection phase, we use BAN logic to produce an idealized form as follows:

$M3 \ : \ (< ID_l, skey_l >_{PK_s}, < h(ID_l, skey_{s2}, skey_l) >_{SK_l})$

$M4 \ : \ (< ID_s, skey_{s2} >_{PK_l}, < h(ID_s, skey_{s2}) >_{SK_s})$

To analyze our improved scheme, we make the following assumptions:

$A9 \ : \ L |\equiv \#(skey_l)$

$A10 : \ S |\equiv \#(skey_l)$

$A11 : \ L |\equiv \#(skey_{s2})$

$A12 : \ S |\equiv \#(skey_{s2})$

$A13 : \ L |\equiv S |\Rightarrow L \overset{skey_{sl}}{\leftrightarrow} S$

$A14 : \ S |\equiv L |\Rightarrow L \overset{skey_{sl}}{\leftrightarrow} S$

$A15 : \ L |\equiv S |\Rightarrow ID_s$

$A16 : \ S |\equiv L |\Rightarrow ID_l$

According to those assumptions and the rules of BAN logic, we show the main proof of the package collectionphase as follows:

c. Store$S$ authenticates logistics$L$.

By $M3$ and the *seeing rule*, we can derive:

$S \triangleleft (< ID_l, skey_l >_{PK_s}, < h(ID_l, skey_{s2}, skey_l) >_{SK_l})$ (*Statement 17*)

By $A10$ and the *freshness rule*, we can derive:

$S |\equiv \#(< ID_l, skey_l >_{PK_s}, < h(ID_l, skey_{s2}, skey_l) >_{SK_l})$ (*Statement 18*)

By (*Statement 17*), $A12$ and the *message meaning rule*, we can derive:

$S |\equiv L |\sim (< ID_l, skey_l >_{PK_s}, < h(ID_l, skey_{s2}, skey_l) >_{SK_l})$ (*Statement 19*)

By (*Statement 18*), (*Statement 19*), and the *nonce verification rule*, we can derive:

$S |\equiv L |\equiv (< ID_l, skey_l >_{PK_s}, < h(ID_l, skey_{s2}, skey_l) >_{SK_l})$ (*Statement 20*)

By (*Statement 20*) and the *belief rule*, we can derive:

$S |\equiv L |\equiv L \overset{skey_{sl}}{\leftrightarrow} S$ (*Statement 21*)

By (*Statement 21*), $A14$ and the *jurisdiction rule*, we can derive:

$S |\equiv L \overset{skey_{sl}}{\leftrightarrow} S$ (*Statement 22*)

By (*Statement 22*) and the *belief rule*, we can derive:

$S \mid\equiv L \mid\equiv ID_l$ (*Statement 23*)

By (*Statement 23*), *A16* and the *jurisdiction rule*, we can derive:

$S \mid\equiv ID_l$ (*Statement 24*)

d. Logistics$L$ authenticates store$S$.

By *M4* and the *seeing rule*, we can derive:

$L \triangleleft (<ID_s, skey_{s2}>_{PK_l}, <h(ID_s, skey_{s2})>_{SK_s})$ (*Statement 25*)

By *A9* and the *freshness rule*, we can derive:

$L \mid\equiv \#(<ID_s, skey_{s2}>_{PK_l}, <h(ID_s, skey_{s2})>_{SK_s})$ (*Statement 26*)

By (*Statement 25*), *A11* and the *message meaning rule*, we can derive:

$L \mid\equiv S \mid\sim (<ID_s, skey_{s2}>_{PK_l}, <h(ID_s, skey_{s2})>_{SK_s})$ (*Statement 27*)

By (*Statement 26*), (*Statement 27*), and the *nonce verification rule*, we can derive:

$L \mid\equiv S \mid\equiv (<ID_s, skey_{s2}>_{PK_l}, <h(ID_s, skey_{s2})>_{SK_s})$ (*Statement 28*)

By (*Statement 28*) and the *belief rule*, we can derive:

$L \mid\equiv S \mid\equiv L \overset{skey_{sl}}{\leftrightarrow} S$ (*Statement 29*)

By (*Statement 29*), *A13* and the *jurisdiction rule*, we can derive:

$L \mid\equiv L \overset{skey_{sl}}{\leftrightarrow} S$ (*Statement 30*)

By (*Statement 30*) and the *belief rule*, we can derive:

$L \mid\equiv S \mid\equiv ID_s$ (*Statement 31*)

By (*Statement 31*), *A15* and the *jurisdiction rule*, we can derive:

$L \mid\equiv ID_s$ (*Statement 32*)

By (*Statement 22*), (*Statement 24*), (*Statement 30*), and (*Statement 32*), we can provethe proposed scheme such that logistics$L$ and store$S$ authenticate each other. Moreover, we are also able to prove that the proposed scheme can establish a session key between logistics$L$ and store$S$.

In the proposed scheme, the logistics authenticates the store by

$$h(ID_s, skey_{s2}) \overset{?}{=} V_{PK_s}(Sig_{sl}). \quad (26)$$

If it passes the verification, the logistics authenticates the legality of the store. Then, the store authenticates the logistics by

$$h(ID_l, skey_{s2}, skey_l) \overset{?}{=} V_{PK_l}(Sig_{ls}). \quad (32)$$

If it passes the verification, the store authenticates the legality of the logistics. Hence, mutual authentication is achieved in the package collection phase between the logistics and store.

In the package dispatched phase of the proposed scheme, the main goal of the scheme is to authenticate the session key establishment between logistics$L$ and deliverer$D$.

$G17: \ L \mid\equiv L \overset{skey_{ld}}{\leftrightarrow} D$

$G18: \ L \mid\equiv D \mid\equiv L \overset{skey_{ld}}{\leftrightarrow} D$

$G19: \ D \mid\equiv L \overset{skey_{ld}}{\leftrightarrow} D$

$G20: D \mid\equiv L \mid\equiv L \overset{skey_{ld}}{\leftrightarrow} D$

$G21: \ L \mid\equiv ID_d$

$G22: \ L \mid\equiv D \mid\equiv ID_d$

$G23: \ D \mid\equiv ID_l$

$G24: \ D \mid\equiv L \mid\equiv ID_l$

According to the package dispatched phase, we use BAN logic to produce an idealized form as follows:

$M5 \ : \ (<ID_l, skey_{l2}>_{PK_d}, <h(ID_l, skey_{l2})>_{SK_l})$

$M6\ :\ (<ID_d, skey_d>_{PK_l}, <h(ID_d, skey_{l2}, skey_d)>_{SK_d})$

To analyze our improved scheme, we make the following assumptions:

$A17\ :\ L \mid\equiv \#(skey_{l2})$

$A18\ :\ D \mid\equiv \#(skey_{l2})$

$A19\ :\ L \mid\equiv \#(skey_d)$

$A20\ :\ D \mid\equiv \#(skey_d)$

$A21\ :\ L \mid\equiv D \mid\Rightarrow L \overset{skey_{ld}}{\leftrightarrow} D$

$A22\ :\ D \mid\equiv L \mid\Rightarrow L \overset{skey_{ld}}{\leftrightarrow} D$

$A23\ :\ L \mid\equiv D \mid\Rightarrow ID_d$

$A24\ :\ D \mid\equiv L \mid\Rightarrow ID_l$

According to those assumptions and the rules of BAN logic, we show the main proof of the package dispatchedphase as follows:

e. Deliverer*D* authenticates logistics*L*.

By *M5* and the *seeing rule*, we can derive:

$D \triangleleft (<ID_l, skey_{l2}>_{PK_d}, <h(ID_l, skey_{l2})>_{SK_l})$ (*Statement 33*)

By *A18* and the *freshness rule*, we can derive:

$D \mid\equiv \#(<ID_l, skey_{l2}>_{PK_d}, <h(ID_l, skey_{l2})>_{SK_l})$ (*Statement 34*)

By (*Statement 33*), *A20* and the *message meaning rule*, we can derive:

$D \mid\equiv L \mid\sim (<ID_l, skey_{l2}>_{PK_d}, <h(ID_l, skey_{l2})>_{SK_l})$ (*Statement 35*)

By (*Statement 34*), (*Statement 35*), and the *nonce verification rule*, we can derive:

$D \mid\equiv L \mid\equiv (<ID_l, skey_{l2}>_{PK_d}, <h(ID_l, skey_{l2})>_{SK_l})$ (*Statement 36*)

By (*Statement 36*) and the *belief rule*, we can derive:

$D \mid\equiv L \mid\equiv L \overset{skey_{ld}}{\leftrightarrow} D$ (*Statement 37*)

By (*Statement 37*), *A22* and the *jurisdiction rule*, we can derive:

$D \mid\equiv L \overset{skey_{ld}}{\leftrightarrow} D$ (*Statement 38*)

By (*Statement 38*) and the *belief rule*, we can derive:

$D \mid\equiv L \mid\equiv ID_l$ (*Statement 39*)

By (*Statement 39*), *A24* and the *jurisdiction rule*, we can derive:

$D \mid\equiv ID_l$ (*Statement 40*)

f. Logistics*L* authenticates deliverer*D*.

By *M6* and the *seeing rule*, we can derive:

$L \triangleleft (<ID_d, skey_d>_{PK_l}, <h(ID_d, skey_{l2}, skey_d)>_{SK_d})$ (*Statement 41*)

By *A17* and the *freshness rule*, we can derive:

$L \mid\equiv \#(<ID_d, skey_d>_{PK_l}, <h(ID_d, skey_{l2}, skey_d)>_{SK_d})$ (*Statement 42*)

By (*Statement 41*), *A19* and the *message meaning rule*, we can derive:

$L \mid\equiv D \mid\sim (<ID_d, skey_d>_{PK_l}, <h(ID_d, skey_{l2}, skey_d)>_{SK_d})$

(*Statement 43*)

By (*Statement 42*), (*Statement 43*), and the *nonce verification rule*, we can derive:

$L \mid\equiv D \mid\equiv (<ID_d, skey_d>_{PK_l}, <h(ID_d, skey_{l2}, skey_d)>_{SK_d})$ (*Statement 44*)

By (*Statement 44*) and the *belief rule*, we can derive:

$L \mid\equiv D \mid\equiv L \overset{skey_{ld}}{\leftrightarrow} D$ (*Statement 45*)

By (*Statement 45*), *A21* and the *jurisdiction rule*, we can derive:

$L \mid\equiv L \overset{skey_{ld}}{\leftrightarrow} D$ (*Statement 46*)

By (*Statement 46*) and the *belief rule*, we can derive:

$L \mid\equiv D \mid\equiv ID_d$ (*Statement 47*)

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 January 2019 doi:10.20944/preprints201901.0052.v1

By (*Statement 47*), *A23* and the *jurisdiction rule*, we can derive:

$L \mid\equiv ID_d$ (*Statement 48*)

By (*Statement 38*), (*Statement 40*), (*Statement 46*), and (*Statement 48*), we can provethe proposed scheme such that logistics$L$ and deliverer$D$ authenticate each other. Moreover, we are also able to prove that the proposed scheme can establish a session key between logistics$L$ and deliverer$D$.

In the proposed scheme, the deliverer authenticates the logistics by

$$h(ID_l, skey_{l2}) \stackrel{?}{=} V_{PK_l}(Sig_{ld}) \cdot \tag{42}$$

If it passes the verification, the deliverer authenticates the legality of the logistics. Then, the logistics authenticates the deliverer by

$$h(ID_d, skey_{l2}, skey_d) \stackrel{?}{=} V_{PK_d}(Sig_{dl}) \cdot \tag{48}$$

If it passes the verification, the logistics authenticates the legality of the deliverer. Hence, mutual authentication is achieved in the package dispatched phase between the logistics and deliverer.

Scenario: A malicious attacker pretends to be the legal client to get the delivery package from the deliverer.

Analysis: The attacker will not succeed because the delivery message from the deliverer is encrypted by the public key of the legal client. Only the legal client can use his/her private key to decrypt the package. Since the illegal client has a different private key, he/she can't decrypt the delivery message from the deliverer. In the proposed scheme, the attacker cannot achieve his/her purpose by pretending to be the legal client. In the similar scenario, the proposed scheme can also defend against a malicious attack pretending to be the legal deliverer to deliver a dangerous package to the client. The client checks the signature of the delivery message by using the public key of the deliverer. Since the illegal deliverer can't sign the correct delivery message, the client rejects the package. In the proposed scheme, the attacker will fail in pretending to be the legal deliverer.

4.2 Data Integrity

To ensure the integrity of transaction data, this study uses the Diffie-Hellman key exchange algorithm to calculate the session key between both parties, as well as to ensure data integrity. The malicious attacker only knows the partial message of the session key, so he/she can't use the message to calculate the correct session key. Only the correct session key will allow successful communication. Thus attackers can't modify the transmitted message; therefore, the proposed scheme achieves data integrity.

Scenario: A malicious attacker intercepts the transmitted message from the client to the store, and sends a modified message to the store.

Analysis: The attacker will not succeed because the legal store will use

$$(ID_c, M_{\inf}, D_{\inf}, SM_{cs}) = D_{skey_{cs}}(C_{cs2}) \tag{14}$$

to decrypt the received message. The attacker cannot calculate the correct session key $skey_{cs}$. Thus, the attack will fail when the legal storedecrypts the received message. In the proposed scheme, the attacker can't achieve his/her purpose by sending a modified message to the store. For the same reason, the attack will fail because he/she can't use the correct session key $skey_{cs}$ to decrypt the received messagevia

$$(ID_s, ID_c, M_{\inf}, TID, SM_{cs}) = D_{skey_{cs}}(C_{sc2}) \cdot \tag{21}$$

Therefore, attackers cannot achieve their purpose by sending a modified message to the client.

4.3 Anti-Switch Package

Another form of logistics attack involves attempting to switch the original package from the store to the client; thus, the package received by the client isn't the original one sent by the store. The high

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 January 2019 doi:10.20944/preprints201901.0052.v1

value package may be changed to a lower value package. In the proposed scheme, we use the subliminal channel to avoid such condition. When the client purchases merchandise from the store, they negotiate a subliminal message SM_{cs}. The store writes the subliminal message onto the tag attached outside the package. Even if the attacker switches the package from the original one, he/she can't write the correct subliminal message onto the tag attached outside the package.When the deliverer delivers the package, the client checks the correctness of the received message. The process for the client checking the correctness of the signature is as follows:

$$\begin{aligned}
&h(y_s^{S_{s1}} \cdot g^{r_s} \cdot PK_s^{h(TID)+S_{s2}}, TID) \\
&= h((g^k)^{S_{s1}} \cdot g^{r_s} \cdot (g^{SK_s})^{h(TID)+S_{s2}}, TID) \\
&= h(g^{k \cdot S_{s1} + r_s + SK_s(h(TID)+S_{s2})}, TID) \\
&= h(g^{k(k-k^{-1}(r_s + SK_s \cdot h(TID))) + r_s + SK_s(h(TID)+S_{s2})}, TID) \\
&= h(g^{k^2 - r_s - SK_s \cdot h(TID) + r_s + SK_s \cdot h(TID) + SK_s \cdot S_{s2}}, TID) \\
&= h(g^{k^2 + SK_s \cdot S_{s2}}, TID) \\
&= h(g^{k^2 + SK_s(SM_{cs} + skey_{cs})}, TID) \\
&= h((g^k)^k \cdot (g^{SK_s})^{(SM_{cs} + skey_{cs})}, TID) \\
&= h({y_s}^k \cdot {PK_s}^{(SM_{cs} + skey_{cs})}, TID) \\
&= r_s
\end{aligned} \tag{91}$$

After the client checks the correctness of the subliminal signature, the client then decrypts the subliminal message. The process for restoring the subliminal message by the client is as follows:

$$\begin{aligned}
&S_{s2} = SM_{cs} + skey_{cs} \bmod p \\
&SM_{cs} = (S_{s2} - skey_{cs}) \bmod p
\end{aligned} \tag{92}$$

Thus, in the proposed scheme, the anti-switch package is achieved.

4.4 Intelligent and Secure Package Tracing

When the client purchases merchandise from the store, he/she may want to know the delivery status of his/her purchased merchandise. In the proposed scheme, the client can get the delivery status through the logistics. After the logistics verifies the legality of the client, the logistics asks the sensorattached outside the packageto report the GPS location, the temperature and humidity sensing data. Even in some high-price goods or fresh food delivery services, the sensorattached outside the packagecan report the temperature and humidity to the client. In the proposed scheme, the client can trace the GPS location, the temperature and humiditysensing data $S_{\inf}$ of the merchandise via

$$(ID_c, TID, S_{\inf}) = D_{SK_c}(C_{pc}), \tag{70}$$

and enjoy better control over the merchandise that he/she bought from the store.

4.5 Resisting Replay Attack

Attackers may also intercept the message transmitted between two parties, like the client and the store, or the deliverer and the client. They can attempt to impersonate a legal client, store or deliverer, and then send the same message again to the intended receiver for a replay attack. Because the transmitted messages are protected by the session key $skey_{xy}$, and the session key $skey_{xy}$ is changed every round in the proposed scheme, the same message can't be sent twice; thus, the replay attack can't succeed.

4.6 Forward and Backward Secrecy

doi:10.20944/preprints201901.0052.v1

Even if the session key between two parties is compromised at any point by an attacker, the system still satisfies forward and backward secrecy. An attacker may use the session key for future communication, or use it to obtain previous messages. However, in the proposed scheme, the session key $skey_{xy}$ is established by each of the two parties and is changed every round. The attacker cannot use the same session key for future communication, or to obtain previous messages. Thus, the proposed scheme achieves forward and backward secrecy.

4.7Non-Repudiation

In the proposed scheme, we use digital signature to achieve non-repudiation between the parties in each phase. The sender uses his/her private key to sign the transmitted message; after the receiver verifies the received message, the receiver uses his/her private key to sign the response message. Thus, the proposed scheme achieves the non-repudiation issue. Table 1 shows the non-repudiation of the proposed scheme.

Table 1. Non-repudiation of the proposed scheme

Item / Phase	Proof	Issuer	Holder	Verification
Purchase Phase	(C_{cs}, Sig_{cs})	Client	Store	$h(ID_c, skey_c) \stackrel{?}{=} V_{PK_c}(Sig_{cs})$
	(C_{sc}, Sig_{sc})	Store	Client	$h(ID_s, skey_c, skey_s) \stackrel{?}{=} V_{PK_s}(Sig_{sc})$
Package Collection Phase	(C_{sl}, Sig_{sl})	Store	Logistics	$h(ID_s, skey_{s2}) \stackrel{?}{=} V_{PK_s}(Sig_{sl})$
	(C_{ls}, Sig_{ls})	Logistics	Store	$h(ID_l, skey_{s2}, skey_l) \stackrel{?}{=} V_{PK_l}(Sig_{ls})$
Package Dispatched Phase	(C_{ld}, Sig_{ld})	Logistics	Deliverer	$h(ID_l, skey_{l2}) \stackrel{?}{=} V_{PK_l}(Sig_{ld})$
	(C_{dl}, Sig_{dl})	Deliverer	Logistics	$h(ID_d, skey_{l2}, skey_d) \stackrel{?}{=} V_{PK_d}(Sig_{dl})$
Package Query Phase	(C_{cp}, Sig_{cp})	Client	Logistics	$h(ID_c, TID) \stackrel{?}{=} V_{PK_c}(Sig_{cp})$
	(C_{pc}, Sig_{pc})	Logistics	Client	$h(ID_c, TID, S_{\inf}) \stackrel{?}{=} V_{PK_l}(Sig_{pc})$
Package Delivery Phase	(C_{dl2}, Sig_{dl2})	Deliverer	Client	$h(ID_c, ID_s, ID_l, ID_d, TID, C_{lc}, Sig_{lc}) \stackrel{?}{=} V_{PK_d}(Sig_{dl2})$
	(C_{ls2}, Sig_{ls2})	Logistics	Client	$h(ID_c, ID_s, TID, C_{sc3}) \stackrel{?}{=} V_{PK_l}(Sig_{ls2})$
Receipt Retention Phase	$(C_{dl3}, Sig_{dl3}, C_{dl4})$	Deliverer	Logistics	$h(ID_c, ID_d, TID) \stackrel{?}{=} V_{PK_d}(Sig_{dl3})$

doi:10.20944/preprints201901.0052.v1

4.8 Computation Cost

Table 2 shows the computation costs of the proposed scheme.

Table 2. Computation cost of the proposed scheme

Phase \ Party	Client	Store	Logistics	Deliverer
Purchase Phase	$2T_{Exp}+2T_H$ $+1T_{Cmp}+6T_{Enc}$	$5T_{Exp}+3T_{Mul}$ $+4T_H+1T_{Cmp}$ $+7T_{Enc}$	N/A	N/A
Package Collection Phase	N/A	$2T_{Exp}+2T_H$ $+1T_{Cmp}+5T_{Enc}$	$2T_{Exp}+3T_H$ $+1T_{Cmp}+7T_{Enc}$	N/A
Package Dispatched Phase	N/A	N/A	$2T_{Exp}+4T_H$ $+1T_{Cmp}+7T_{Enc}$ $+1T_{Xor}$	$2T_{Exp}+3T_H$ $+1T_{Cmp}+7T_{Enc}$
Package Query Phase	$2T_H+1T_{Cmp}$ $+4T_{Enc}$	N/A	$4T_H+2T_{Cmp}$ $+4T_{Enc}+1T_{Xor}$	N/A
Package Delivery Phase	$3T_{Exp}+2T_{Mul}$ $+5T_H+4T_{Cmp}$ $+9T_{Enc}$	N/A	N/A	N/A
Receipt Retention Phase	N/A	N/A	$2T_H+2T_{Cmp}$ $+5T_{Enc}$	$1T_H+3T_{Enc}$

T_{Exp} : Exponential operation
T_{Mul} : Multiplication operation
T_H : Hash function operation
T_{Cmp} : Comparison operation
T_{Enc} : Encryption operation
T_{Xor} : Exclusive-or operation

From Table 2, the proposed scheme's computation costs for the client, store, logistics and deliverer in each phase are analyzed. For the highest computation cost in the purchase phase, a client needs two exponential operations, two hash function operations, one comparison operation and six encryption operations. A store needs fiveexponential operations, three multiplication operations, four hash function operations, one comparison operation and seven encryption operations. The computation cost and complexity are acceptable.

4.7 Communication Performance

The communication cost of the proposed scheme is shown in Table 3.

 doi:10.20944/preprints201901.0052.v1

Table 3. Communication cost of the proposed scheme

Item / Phase	Message Length	Round	3.5G (14 Mbps)	4G (100 Mbps)
Purchase Phase	4608 bits	4	0.329 ms	0.046 ms
Package Collection Phase	6400 bits	4	0.457 ms	0.064 ms
Package Dispatched Phase	4592 bits	4	0.328 ms	0.046 ms
Package Query Phase	4466 bits	4	0.319 ms	0.045 ms
Package Delivery Phase	6144 bits	3	0.439 ms	0.061 ms
Receipt Retention Phase	2304 bits	1	0.165 ms	0.023 ms

The communication efficiency of the proposed scheme during the transaction process of each phase was also analyzed. It was assumed that anRSA operation requires 1024 bits, an AES operation requires256 bits, and a hash function operation requires 160 bits, while other messages with exclusive-or operation require 80 bits. For example, the package collection phase of the proposed scheme requiressix RSA messages and one AES message. It thus requires1024*6+256*1 = 6400 bits. In a 3.5 G environment, the maximum transmission speed is 14 Mbps, which only takes 0.457 ms to transfer all messages. In a 4 G environment, the maximum transmission speed is 100 Mbps, and the transmission time is reduced to 0.064 ms (ITU 2016).

5. Conclusions

In recent years, with the rapid development of the Internet, e-commerce services have flourished. After the client shops in the store, an important issue is the safety of recent merchandise delivery. In this paper, we have proposed an intelligent and secure package sensoring logistics system based on a subliminal channel. The scheme can solve the switched package issue effectively, and the client can grasp the delivery status of the goods at any time.

In the part of avoiding the switched package issue, we adopted the subliminal channel technology. When the client shops in the store, they negotiate the subliminal message in advance. The subliminal message will be hidden in the signature by the store.When the client receives the goods, he/she will first check the subliminal message hidden in the signature to confirm whether the goods have been switched. In addition, after the store passes the package to the logistics, the sensor will be attached to the package by the logistics. The client can check the GPS location, the temperature and humidity sensing data of the package any time during the delivery process, and the intelligent logistics can be achieved.

To sum up, the research proposes a complete intelligent and secure architecture for the logistics environment. The proposed scheme achieves the following goals.First, we apply the BAN logic to prove that our scheme achieves mutual authentication.Second, we use the subliminal channel technology to avoid the switched package issue. Third, the sensor is attached onto the package so the client can check the package delivery status at any time. Fourth, the proposed scheme also achieves data integrity, resisting replay attack, forward and backward secrecy, and non-repudiation.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 January 2019 doi:10.20944/preprints201901.0052.v1

Funding: This work is supported by the National Natural Science Foundation of China (No. 61672442), the Science and Technology Planning Project of Fujian Province(No.2016Y0079).

Author Contributions: Yong-Yuan Deng proposed the original idea and design protocol. Chin-Ling Chen designed the protocol and analyzed the security property. Chun-Ta Li analyzed the security property and comparison analysis. Shunzhi Zhu surveyed related works and delivering process.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. A. Whitmore, A. Agarwal, and L. Da Xu, "The internet of things: a survey of topics and trends," *Information Systems Frontiers*, vol. 17, no. 2, 2015, pp. 261-274.
2. B. R. Ray, J. Abawajy, M. Chowdhury, and A. Alelaiwi, "Universal and secure object ownership transfer protocol for the Internet of Things," *Future Generation Computer Systems*, in Press, 2017.
3. K. Liang, and W. Susilo, "Searchable attribute-based mechanism with efficient data sharing for secure cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, 2015, pp. 1981-1992.
4. X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the internet of things," *Future Generation Computer Systems*, vol. 49, 2015, pp. 104-112.
5. K. Liang, and W. Susilo, "Searchable attribute-based mechanism with efficient data sharing for secure cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, 2015, pp. 1981-1992.
6. J. Han, W. Susilo, and Y. Mu, "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption," *IEEE Transactions on Information Forensics and Security*, vol. 10, 2015, pp. 665-678.
7. S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 2, 2012, pp. 380–400.
8. Z. Zhou, D. Huang, and Z. Wang, "Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption," *IEEE Transactions on Computers*, vol. 64, no. 1, Jan. 2015, pp. 126-138.
9. H. Kim, C. H. Kim, and J. M. Chung, "A novel elliptical curve ID cryptography protocol for multi-hop ZigBee sensor networks," *Wireless Communications and Mobile Computing*, vol. 12, no. 2, 2012, pp. 145-157.
10. C. L. Chen, and J. J. Liao, "A fair online payment system for digital content via subliminal channel," *Electronic Commerce Research and Application*, vol. 10, 2011, pp. 279-287.
11. C. L. Chen, and M. H. Liu, "A traceable E-cash transfer system against blackmail via subliminal channel," *Electronic Commerce Research and Application*, vol. 8, 2009, pp. 327-333.
12. C. L. Chen, K. H. Wang, W. J. Tsaur, J. H. Chen, and C. H. Chen, "An electronic public engineering project bidding protocol via a subliminal channel," *Journal of Information Technology*, vol. 46, 2017, pp. 470-483.
13. M. A. S. Jr., M. V. M. Silva, R. C. A. Alves, and T. K. C. Shibata, "Lightweight and escrow-less authenticated key agreement for the Internet of Things," *Computer Communications*, vol. 98, 2017, pp. 43–51.
14. M. Simplicio, B. Oliveira, P. Barreto, C. Margi, T. Carvalho, and M. Naslund, "Comparison of authenticated-encryption schemes in wireless sensor networks," *in: Proceedings of the 36th IEEE Conference on Local Computer Networks (LCN)*, 2011, pp. 454-461.
15. D. He, C. Chen, S. Chan, and J. Bu, "SDRP: A secure and distributed reprogramming protocol for wireless sensor networks," *IEEE Transactions on Industrial Electronics*, vol. 59, no. 11, Nov. 2012, pp. 4155–4163.
16. Z. Dakhli, and Z. Lafhaj, "Efficient logistics enabled by smart solutions in tunneling," *Underground Space*, vol. 2, 2017, pp. 227-233.
17. J. M. Danielsen, P. Engelseth, and H. Wang, "Large scale integration of wireless sensor network technologies for air quality monitoring at a logistics shipping base," *Journal of Industrial Information Integration*, 2018.
18. H. Luo, K. Wang, X. T. R. Kong, S. Lu, and T. Qu, "Synchronized production and logistics via ubiquitous computing technology," *Robotics and Computer-Integrated Manufacturing*, vol. 45, 2017, pp. 99-115.
19. M. Burrows, M. Abadi, R. Needham, "A logic of authentication,"*ACM Transactions on Computer Systems*, vol. 8, 1990, pp. 18-36.

20. W. Han, and Z. Zhu, "An ID-based mutual authentication with key agreement protocol for multiserver environment on elliptic curve cryptosystem," *International Journal of Communication Systems*, vol. 27, no. 8, 2014, pp. 1173-1185.
21. G. J. Simmons, "The subliminal channel and digital signatures," *In Proceedings of theEurocrypt '84 workshop on Advances in Cryptology*, 1984, pp. 364-378.
22. G. J. Simmons, "Subliminal communication is easy using the DSA," *In Proceedings of Eurocrypt '93*, 1993, pp. 218-232.
23. G. J. Simmons, "The history of subliminal channels," *IEEE Journal on Selected Areas in Communications*, vol. 16, 1998, pp. 452-462.
24. C. T. Li, T. Y. Wu, C. L. Chen, C. C. Lee, and C. M. Chen, "An Efficient User Authentication and User Anonymity Scheme with Provably Security for IoT-Based Medical Care System," *Sensors*, 2017,doi:10.3390/s17071482.
25. A.K. Das, A. Goswami, "A robust anonymous biometric-based remote user authentication scheme using smart cards,"*Journal of King Saud University – Computer and Information Sciences*, vol. 27, 2015,pp. 193-210.
26. M. G. Speranza, "Trends in transportation and logistics," *European Journal of Operational Research*, vol. 264, 2018, pp. 830-836.
27. V. Odelu, A.K. Das, A. Goswami, "An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card,"*Journal of Information Security and Applications*, vol. 21, 2015, pp. 1-19.
28. D. Mishra, A. Chaturvedi, S. Mukhopadhyay, "Design of a lightweight two-factor authentication scheme with smart card revocation,"*Journal of Information Security and Applications*, vol. 23, 2015, pp. 44-53.
29. A. Chaturvedi, A.K. Das, D. Mishra, S. Mukhopadhyay, "Design of a secure smart card-based multi-server authentication scheme,"*Journal of Information Security and Applications*, vol. 30, 2016, pp. 64-80.
30. R. Madhusudhan, M. Hegde, "Security bound enhancement of remote user authentication using smart card,"*Journal of Information Security and Applications*, vol. 36, 2017, pp. 59-68.