JIBC

Journal of Internet Banking and Commerce

An open access Internet journal (http://www.icommercecentral.com)

Journal of Internet Banking and Commerce, April 2017, vol. 22, no. 1

EFFICIENT E-TICKETS FARE SCHEME FOR TIME-TYPED SERVICES

SATTAR J ABOUD

Department of Computer Science and Technology, Bedfordshire University, UK

Tel: +44 1234 400400;

Email: **m.AlFayoumi@psut.edu.jo**

MOUSTAFA AL-FAYOUMI

Department of Computer Science, Princess Summaya University for Technology, Jordan

MOHAMMAD AL-FAYOUMI

Department of Computer Science, Al-Isra University, Amman, Jordan

Abstract

In this scheme, we compute the fare that the passengers should pay based on the time of service for entry and exit of the scheme. The information and communication technologies let the use of e-tickets, which assists to decrease charges and enhance the control of the communications. But, these schemes should be secure anti-fraud and they should also protect passengers' privacy. Thus, we have considered the security specifications for the time-typed schemes and we have introduced the scheme for every of the e-tickets fare schemes. The schemes propose robust privacy for good passengers. It means that, the service issuer does not capable to reveal the information of its passenger and, also dissimilar trips of the same passenger are not linkable. Also, anonymity for passenger can be revoked when they behave badly. The scheme has been applied and its result has been gauged. The outcome observes that scheme is appropriate to be employed in e-tickets fare scheme while they provide the better result with the high-quality mobile phone.

Keywords: **Privacy; Mobile Applications; E-Commerce; Applied Cryptography**

INTRODUCTION

The integration of information and communication technologies in e-ticket fare schemes lets to decrease costs and enhances the control of the communications; some cases can be the real-time traffic density monitoring and the administration strategy of communications based on the passenger flows. E-ticket fare schemes are designed for huge-density public transport rather than setting the passenger destination, the charge can be considered in time-typed scheme. The advantages of using this scheme involve the removal of selling and cash machinery, passenger ease, quicker travel and decreased the office expense. But, to accomplish this, an efficient e-ticket fare scheme becomes an essential. Therefore, the secure administration of passenger check-in and check-out of a scheme is required, as they pay consistent with this use. When the scheme identifies the passenger, recognizing their entry and exit points. It means that where they travel and if a scheme can trace their travels. Using such movements it can generate passenger profiles. This is the considerable confidentiality threat. It means that, it breaches the passenger privacy. Therefore, such e-ticket fare scheme has to protect the passenger confidentiality to stop profiling and tracking. However, if the scheme provides non-revocable confidentiality, some illegal, for example terrorists can provide the transport scheme to flee from the security services. Therefore, we have two different characteristics. To satisfy both characteristics, the scheme can revoke anonymity of the fixed passenger by means of the court order. The additional concern is the high number of passenger in the e-ticket fare scheme, needing then the scheme to be very quick in both entry and exit operations. The work provides the secure administration for e-ticket fare scheme, with robust confidentiality for sincere passenger. But, when the passenger acts corruptly, the identity can be revealed to pick authorized events, as the scheme provides revocable anonymity. Also, passenger does not require getting the new credential each time that they join the e-ticket fare scheme. This characteristic enhanced the scheme usability, since in the preceding e-ticket fare scheme new credential detail is required for each new trip.

RELATED WORKS

In this paper, we consider the e-ticket fare scheme regarding the revocable anonymity of passenger. In such scheme, the issuer can connect dissimilar trips from the same passenger. In the linkable scheme, the revelation of an identity of the passenger in the trip produces the revelation of all the trips of the same passenger, vulnerable anonymity. Thus, the issuer knows where they travel, what time of the trips. The facts of passenger actions let the construction of passenger profiles. Such profiles are practical for the issuer since they are used generally to enhance the transport scheme or more solid to describe the business creation especially for one report. However, the construction of passenger profiles is the crucial breach of the confidentiality, and the e-ticket fare scheme should prevent the tracking of the passenger. In 2006, Heydt-Benjamin et al. [1] introduced a scheme of privacy for public transportation. But in their scheme the issuer cannot trace the trips, thus the new credential is required for each trip, this means that there is the important additional charge in such transport scheme, where the entries and exits of the scheme have to be as rapid as possible. The credential renewal needs more issuer construction that is costly, since it should manage the high number of credentials. However, the first scheme using the latest trends in the direction to utilize mobile phones is proposed in 2008 by Madlmayr et al. [2]. Therefore, we can state that the mobile phone is the passenger requirement in the e-ticket fare scheme. In this paper, we proposed scheme which gives revocable anonymity and intractability. Also, this scheme has been designed to employ the personal mobile phone of the passenger and the passenger do not want to get the new credential each time if he wants to make the trip, since the credential renewal means the additional cost.

In 2010, Vives-Guasch et al. [3] introduced a fare collection scheme, in their scheme the passenger cannot able to alter the direction of the transfer without exiting the service. Also, in 2012, Andreu Pere Isern-Deya et al. [4] presented a Fare collection system for revocable anonymity for users which is not involving the requirements for the extensions. It means that, they should check out along with their direction. In 2014, Ghada Arfaoui et al. [5] introduced another scheme related to privacy-preserving of mobile for transport systems. Their scheme needed to put scheme exits separated by direction. Also, in 2016 Magdalena Payeras et al. [6] designed two schemes to get anonymity in transferable e-ticket. Their schemes also cannot modify the direction. In the proposed scheme, we extend the work to let time-typed scheme solve such problems.

The scheme applies the group signature system to check if the passenger is the proper member of the selected group of passenger. The group signature system used is illustrated in Section 4. Then, we consider the time-typed scheme in Section 5. Section 6 considers the security discussion of the scheme. Lastly, the conclusion is illustrated in Section 7.

Notations Used

The notations used are as follows:

p, q: prime numbers

pk: group public key

sk: group secret key

rt: group of revocations

P: passenger

eP: passenger pseudonym for payment

dP: inverse key of eP private

b: key base

ri: ith arbitrary number

si: key of ri

ci: ith challenge for P to prove authorship of eP

wi: challenge ci reply by P

sP: probabilistic encryption of eP

Ti: ith timestamp

v: verification key

hv: hash image of key v

$SE(c)$: digital signature of c generated by the entity E

ss: source service issuer identifier

t'_{in}: entry ticket, signed by ss

sb: serial number generated by ss for t_{in}

as: arrival station

t'_{out}: exit ticket, signed by as

cf: challenge and fare, signed by as for P

fc: fare computation function

fp: fare to be paid

ds: destination service issuer identifier

pe: probabilistic encryption of P

pn: probabilistic encryption of as

eg: entity generates passenger

pa: payment acceptance signed by eg

pr: payment rejection signed by eg

es: entry station ss identifier

τ_1: entry timestamp, time entry system

cs: commitment signed by P

$Ds(tin)$: digital signature content signed by es

$tin.sb$: serial number sent by P

ts: target station

τ_2: payment timestamp, it means time exit ticket

$Ds(t_{out})$: digital signature content signed by as

BACKGROUND

We utilize the short group signature [7] system to check that the passenger is the right member of the selected group of passenger. Observe that the notations in this part are explicit for the clarification of the used definitions.

The proposed scheme uses bilinear groups $G1$ and $G2$ with relevant generators $a1$ and $a2$. Assume that ($G1$, $G2$) are the Linear assumption. The scheme utilizes the bilinear map e: $G1 \times G2{=}GT$ and the secure hash function H: $\{0,1\}{=}Zp$. The public keys are a_1, z_1, z_1, $b \in G$, and a_2, $d \in G$. Hence, d=$a^u{}_2$ for private u ∈ Z. In the proposed scheme we use the following algorithms.

- *KeyGenG* (n). This algorithm has one input n. The steps of the algorithm are as follows:

    1. Choose an integer $b \in G1$;
    2. Select two integers $f1$, $f\,2 \in Z_P^*$;
    3. Choose two integers z_1, $z_2 \in G_1$ where $Z_1^{f_1} = Z_2^{f_2} = b$;
    4. Choose an integer $u \in Z_P^*$;
    5. Compute the integer $d{=}\,a_2^u$;
    6. Generate for every passenger Pi where $1 \le i \le n$ a key (w_i, y_i) as follows:
        1. Choose $y_i \in Z_P^*$;
        2. Compute $wi = a_1^{1/(u+y_i)}$;
    7. The key u is then a secret master key of a group key.

- *SignG (pk, sk[i],m)*.This algorithm takes the parameters, a group public key $pk{=}(a1, a2, b, z1, z2, d)$, the secret passenger key $sk[i]{=}(w_{i,}\ y_{i)}$ and the message $m \in \{0,1\}^*$.

Find the signature of information $\sigma{=}(A_1, A_2, A_3, c, sv_1, sv_2, sx, s\delta_1, s\delta_2)$. The steps of the algorithm are as follows:

Step 1

The descriptions of this step are as follows:

1. choose two integers v_1, $v_2 \in Z_p$;
2. find an encryption of A: (A_1, A_2, A_3)=$\left(Z_1^{v_1}, Z_2^{v_2}, Ab^{v_1+v_2}\right)$;
3. compute the number $\delta 1{=}x \cdot v_1$;
4. compute the value $\delta_2{=}x \cdot v_2$;

Step 2

The descriptions of this step are as follows:

1. Choose the integers $r_{v_1}, r_{v_2}, r_x, r_{\delta_1}, r_{\delta_2} \in Z_P$;
2. Find the numbers:

   $N_1 = Z_1^{r_{v_1}};$

   $N_2 = Z_2^{r_{v_2}}$

   $N_3 = e(A_3, a_2)^{r_x} .e(b,d)^{-r_{v_1} - r_{v_2}} .e(b,a_2)^{-r_{\delta_1} - r_{\delta_2}}$;

   $N_4 = A_1^{r_x}.Z_1^{-r_{\delta_1}};$

   $N_5 = A_2^{r_x}.Z_2^{-r_{\delta_2}};$

Step 3

The descriptions of this step are as follows:

1. find $c=H\ (m, A_1, A_2, A_3, N_1, N_2, N_3, N_4, N_5)$;

Step 4

The descriptions of this step are as follows:

1. Find the numbers:

$$S_{v_1} = r_{v_1} + cv_1;$$
$$S_{v_2} = r_{v_2} + cv_2;$$
$$S_x \leftarrow r_x + cx;$$
$$S_{\delta_1} \leftarrow r_{\delta_1} + c\delta_1;$$
$$S_{\delta_2} \leftarrow r_{\delta_2} + c\delta_2;$$

Step 5

The descriptions of this step are as follows:

1. The result is $\sigma = (A_1, A_2, A_3, c, S_{v_1}, S_{v_2}, S_x, S_{\delta_1}, S_{\delta_1});$

- Verify$_G(pk, m, \sigma)$. This algorithm provides a group public key

$gpk=(a_1,a_2,b,z_1,z_2,d)$ the message m and the group signature $\sigma=(A_1,A_2,A_3,c,S_{v_1},S_{v_2},S_x,S_{\delta_1},S_{\delta_1})$ check that σ is the valid signature of information.

1. Re-get *N₁, N 2, N₃, N₄, N₅:*
    1. $\tilde{N}_1 = z_1^{S_{v_1}} / A_1^c$;
    2. $\tilde{N}_2 = z_2^{S_{v_2}} / A_2^c$;
    3. $\tilde{N}_3' = e(A_3,a_2)^{S_x} .e(b,d)^{-S_{v_1}-S_{v_2}} .e(b,a_2)^{-S_{\delta_1}-S_{\delta_2}} .\left(e(A_3,d)/e(a_1,a_2)\right)^c$;
    4. $\tilde{N}_4 = A_1^{S_x} / z_1^{S_{\delta_1}}$;
    5. $\tilde{N}_5 = A_2^{S_x} / z_2^{S_{\delta_2}}$

2. verifies that: $c \equiv H(m,A_1,A_2,A_3,\tilde{N}_1,\tilde{N}_2,\tilde{N}_3,\tilde{N}_4,\tilde{N}_5)$;

- Open $_G(pk,msk,m,\sigma)$. This algorithm is employed to trace the signature inside the group. It is just on hand for the group director, as he is the owner of the *msk* master key, and gets all the pairs *(wi, yi)*. Suppose a group public key *pk=(a₁, a₂, b, z₁, z₂, d)* a group master secret key *msk=(f₁,f₂)* both with *m* and a signature $\sigma=(A_1,A_2,A_3,c,S_{v_1},S_{v_2},S_x,S_{\delta_1},S_{\delta_1})$. Then, retrieve a passenger *A* by $A=A_3/(A_1^{f_1},A_2^{f_2})$. If the group director is known the components w_i of the passenger secret keys, he can search for the passenger index similar to an identity *A* retrieved from the signature.
- SignLinkable $_G(pk,sk[i],m)$. This is the linkable signing algorithm to be applied in the scheme. Assume that the group public key *pk*, the secret customer key *sk[i]* and the message *m*. Find the signature of informationσ. To use such algorithm properly, do the following:

First: Employ standard Sign $_G(pk,sk[i],m)$:

Create the linear encryption of $A:(A_1,A_2,A_3)=(Z_1^{v_1},Z_2^{v_2},Ab^{v_1+v_2})$ for $v_1,v_2\in Z_P$; assume the message *m*, sign it and result the signature $\sigma=(A_1,A_2,A_3,c,S_{v_1},S_{v_2},S_x,S_{\delta_1},S_{\delta_1})$ where

$$c \equiv H(m,A_1,A_2,A_3,\tilde{N}_1,\tilde{N}_2,\tilde{N}_3,\tilde{N}_4,\tilde{N}_5) \in Z_P$$

Second: Use SignLinkable $_G(pk,sk[i],m)$:

Employ the same pair *(v₁, v₂)* creating the same linear encryption of *A* than in the first time: $\left(A_1, A_2, A_3\right) = \left(z_1^{v_1}, z_2^{v_2}, Ab^{v_1+v_2}\right)$

Determine the message m', sign it and yield the signature

$\sigma' = \left(A_1, A_2, A_3, c', s'_{v_1}, s'_{v_2}, s'_x, s'_{\delta_1}, s'_{\delta_2}\right)$ Where
$c' = H\left(m', A_1, A_2, A_3, N'_1, N'_2, N'_3, N'_4, N'_5\right) \in Z_P;$

Observe that it can provable some signatures that are created by the same passenger, as the knowledge *(A_1,A_2,A_3)* is public within the same signature. Also, the arbitrary values $\left(r_{v_1}, r_{v_2}, r_x, r_{\delta_1}, r_{\delta_1}\right)$ should be dissimilar to preceding instances, namely $\left(r'_{v_1} \neq r_{v_1}, r'_{v_2} \neq r_{v_2}, r'_x \neq r_x, r'_{\delta_1} \neq r_{\delta_1}, r'_{\delta_2} \neq r_{\delta_2}\right)$ to not disclose knowledge.

- VerifyLinkable $_G(\sigma, \sigma')$. The algorithm requires two signatures as input

$\sigma = \left(A_1, A_2, A_3, c, s_{v_1}, s_{v_2}, s_x, s_{\delta_1}, s_{\delta_2}\right)$ and $\sigma' = \left(A'_1, A'_2, A'_3, c', s'_{v_1}, s'_{v_2}, s'_x, s'_{\delta_1}, s'_{\delta_2}\right)$ and result true or false based on the signatures have created by a same signer false name
$\left(A_1, A_2, A_3\right) : \left(A_1 \equiv A'_1, A_2 \equiv A'_2, A_3 \equiv A'_3\right)$.

TIME-TYPED-TICKET FARE SCHEME

First, we start to describe the requirements of the e-ticket fare scheme

Requirements of Time-typed Scheme

The subsequent security requirements have to be certain in any proposed scheme:

1. Authenticity: each ticket should be produced by its authorized provider.
2. Non-repudiation: a passenger cannot repudiate the issue of one of its tickets.
3. Integrity: after the ticket is produced, cannot be adjusted.
4. Validity period: each ticket has a validity period item to verify if it is in use or not. Every used ticket will saved in the file until its validity period is expired.
5. Non-double-spending: The validity time of each ticket is verified. If the verification is true, the scheme says that a ticket is not in the file of used tickets based on its serial number. Such verification guarantees that the ticket does not employs more than one time.
6. Revocable anonymity: the scheme should promise the customer anonymity to receive approval of the passenger community, but the scheme and the public authorities favor non-anonymity because of control and security reasons. So, the midway solution is revocable anonymity for passenger. If the passenger behaves badly, his anonymity is called.
7. Non-traceability: the supplier can only trace the entry of the passenger with its related exit, but in no way can trace diverse trips of the same passenger.

The common time-typed fare is the daily, weekly or monthly employed by passengers to use the public transport, generating the single ticket which lets the passenger to use it. However, we will denote to the time-typed fare scheme if the money to be paid by the passenger based on the time period does employ. Therefore, in this case, the suitable timestamp should be created if the passenger becomes inward and outward movement of the scheme. The dissimilarity between the current time and an initial timestamp will determine a fare which should be paid to the service issuer.

Time-typed fares are most suitable in locations where the most related parameter of the service provided the time. For instance, bus services, taxi services, tube services and parking places services. Therefore, time-typed costing methods will need time accounts instead of pay per boarding trip. Thus, in this example the scheme has to:

1. Generate the appropriate timestamp if the new ticket is released.
2. The timestamp generates the time-window if a customer has the right to employ the service fare.
3. The time-window has the start-date and the expiry-date that writes the ceiling-time of the service fare.
4. The price to be paid is relative to the time-period that a customer has employed the fare-service. The longer is the time the costly is a ticket.
5. The timestamp should be verified the scheme exit to calculate the service cost.

Now, we explain the proposed time-typed e-ticket fare scheme that gives anonymity to the passenger by the application of group signatures [8] for group-transport services. We explain the participants included in the scheme, the security requirements to be certain, the details which is involved into the entry and exit tickets, and finally the phases by which the scheme contains.

Scheme Participants

The subsequent players are included in the proposed scheme:

1. Passenger P. Entrances to a transport system then pay for a service at an exit. Passenger P does these services by means of his mobile phone.
2. Issuers (ss departure station, as arrival station): checkpoint that runs the tickets used by passenger P. The price to be paid by P is calculated by as in proportion to parameters determined, time-typed fares.
3. Payment $TA\ eg$: runs passenger payments if they exit from a scheme.
4. Group $TA\ ed$: runs a revocation list and group keys. It can call passenger anonymity in case of badly behaved.

Scheme Description

In the scheme, there are four protocols which are as follows:

1. **Initialization Protocol**

   The *ed* creates the group keys and revocation list. This setup is performed once at first. *ed* runs $KeyGen_G(n)$ that generates the group of fixed length n, yields $\left(pk, sk[i], rt[i], a, p, q\right)$, such that *pk* is a group public key, *sk[i]* is a secret key for every passenger P_i, *rt[i]* is a revocation list, *(a, p, q)* are public keys, with *a* is a public key, and *(p,q)* prime numbers such that $p=2q+1$, where $p,q \in Z_p, Z_q$ respectively. Also, every service issuer creates its key pair and illustrates its public key. The secret group key *sk[i]* is released if passenger are listed in the group.

2. **Passenger Registration Protocol**

   The passenger *P* also registers at *eg* by the pseudonym that is used just for payments, he receives the group key pair. In the proposed scheme, *eg* is the entity that generates passenger and service issuer accounts. Such entity deals with the payment related messages and promises the payment for official transactions consistent with the scheme requirements.

   The passenger *P* registers in the group *TA ed* and gets the group key pair *(pk, sk[i])*. Now, the passenger consent that their identity are revealed when they are not truthful, or when the judge needs to cancel their anonymity. Then, *P* also registers anonymously to the payment *TA eg* by an authorization of *ed*; a passenger owns the pseudonym *eP* that is the exponentiation of the arbitrary integer $d_P \in Zq$, with $e_P = a^{d_P}$ mod p; the *eP* is proved to *eg* and authenticated by Schnorr zero-knowledge proof [8] proving of d *P* without revealing that private. Therefore, confidentiality is sealed for passenger, but this anonymity can be called by *ed* when needed. The passenger registration protocol is described as follows:

Generate pseudonym: The passenger *P* should do the following:

1. select the pseudonym as the random integer $d_P \in Zq$;
2. find the value $e_P = a^{d_P}$ mod p;
3. pass the identity *Pi* to the group *TA ed*;
4. pass the certificate *CertPi* to the group *TA ed*;
5. pass the signed message $Sign_P(eP)$ to the group *TA ed*;

Key issue: *ed* should do the following

1. pass the group key pair *(pk, sk[i])* to a passenger *P*;
2. pass the public parameters *(a, p, q)* to a passenger *P*;
3. pass the signature $Sign_{ed}(e_P)$ to the passenger *P*;

Starting *ZKP: P* should do the following

1. Select an arbitrary integer $g_0 \in Z_q$
2. Find $g_1 = a^{g_0}$ mod p;
3. Pass $\left(e_p, g_1, Sig_{ed}\left(e_p\right)\right)$ to the payment $TA\ ed$;

Challenge generation: eg should do the following

1. Select the integer $g_2 \in Z_q$;
2. Pass g_2 to P ;

Proof generation: P should do the following

1. Find the Schnorr ZKP;
2. Compute $g_3 = g_0 + g_2.d_p \bmod_q$;
3. Pass g_3 to eg;

Check pseudonym: eg should do the following

1. Check that $a^{g_3} \equiv g_1.\left(e_p\right)^{g_2}$;

Scheme Entry

Scheme entry: the passenger joins in the departure station and creates the group signature that confirms he is the valid scheme group member, while his identity is not revealed. If such signature is passed to the service issuer ss, he receives the entry ticket from ss that will be illustrated in the departure station.

If P has properly keyed the scheme, the entry ticket t_{in} is then received. The t_{in} will be later employed to authorize a passenger to pay the considered fee. The scheme entry is described as follows:

Obtain service: The passenger P should do the following

1. select a random integer $L_1 \in Z_q$;
2. find $L_2 = a^{L_1}$ mod p;
3. find $\delta_p = PK_{eg}\left(e_p\right)$;
4. select a random integer $L_3 \in Z_q$;
5. find a hash function of: $h_{L_3} = hash\left(L_3\right)$;
6. determine $\sigma = \left(L_2, \delta_P, k_{L_3}\right)$ and signs it with $sk[i]$;

7. passenger secret group key is $\sigma^{*} = \left(\sigma, \bar{\sigma} = Sign_{G}\left(pk, sk\left[i\right], \sigma\right)\right)$;
8. pass σ^{*} to ss;

Generate ticket: The source service issuer ss should do the following

1. Checks a signature of σ^{*}. If a signer is a valid member as Verify$_G$ (pk,σ,$\bar{\sigma}$);
2. Select the timestamp τ_1;
3. Compute an entry ticket $t_{in}=(S_n, ss, \tau_1, \sigma^{*})$
4. Sign it $t_{in}^{*} = \left(t_{in}, Sign_{ss}\left(t_{in}\right)\right)$
5. Pass t_{in}^{*} to the passenger P;

Check entry: passenger P should do the following

1. Checks a signature of t_{in}^{*};

Scheme Exit

The passenger does the weak authentication to an arrival checkpoint as and proves an entry ticket. as then computes the charge to be paid. The passenger has to accept the price and passes this knowledge safely to eg within his payment pseudonym authentication, just eg has information of such pseudonym, as can not reveal that knowledge. Then, eg costs to P account. When the entire process is right, the passenger receives the exit ticket, which is the evidence shows that the passenger has followed the scheme properly. If the passenger exits the scheme, then passes the ticket entry tin to the arrival service supplier as, and the charge to be paid is computed. If P acts properly, the exit ticket t_{out} is received, and can be later presented as the proof of payment, involving that the scheme had been followed properly. The scheme exits and describe as follows:

Prove ticket: passenger P should do the following

1. encrypt L_3
2. pass (t_{in}^{*}, $PK_{as}\, L_3$)) to as;

Check ticket: The service issuer as should do the following:

1. Check a signature of t_{in}^{*} which is calculated by ss;
2. Check that $\sigma.h_{L_3} \equiv hash\left(l_3\right)$, shows that P is a correct owner of the ticket tin;
3. Check that $t_{in}\, .S_n$ had not been used before;
4. Select the timestamp τ2 where $\tau_{2\,\leq}\,\tau_2$;
5. Compute the charge to be paid based on the elapsed time between related time

stamps $\tau_1, \tau_2 : a = f_t\left(t_{in}.ss, as, t_{in}.\tau_1, \tau_2\right)$; thus, in this example, f_t *()* is the function designed to compute the charge between two stations on the time-typed fare scheme.

6. Select the challenge $L_4 \in Z_q$;
7. Compute $\lambda = \left(t_{in}^{*}, L_3, a, L_4, \tau_2, P_d\right)$;
8. Sign it λ^*=(λ, Sign$_{as}$(λ))
9. Pass λ^* to P, in case of challenge λ is employed by P as the evidence to show that he has exit at τ_2;
10. Compute $y_{as}=(\lambda.z,t_{in}.S_n,t_{in}.\sigma,L_4)$;

Set payment: passenger P should do the following:

1. Check a signature of λ^* which is calculated by as;
2. Find $L_5=L_1 + L_4 . d_P$ mod q;
3. Encrypt $e_P=PK_{eg}(L_5,t_{in}.S_n,\lambda.a)$;
4. Pass e_P to as;

Passing payment information: The service supplier as should do the following:

1. Repost e_P and y_{as} to the payment TA eg;

Check payment: eg should do the following:

1. Recover e_P to get the Schnorr proof L_5;
2. Recover $t_{in}.\delta_P$ to get the pseudonym e_P;
3. Charge the bill to the related passenger account;
4. Check an identity of P by Schnorr ZKP by a $a^{L_5} \equiv L_2.\left(e_P\right)^{L_4}$;
5. If true, the price a is charged from the passenger account that owns e_P and a protocol resumes. If not compute the payment refusal ko=(authentication error, e_P),
6. Sign $ko^*=(ko, Sign_{eg}(ko))$;
7. Pass it to as and stops the protocol;
8. Compute $ok=(t_{in}.S_n,\lambda.a)$;
9. Sign $ok^*=(ok, Sign_{eg}(ok))$;
10. Pass ok* to as;

Set exit: The service issuer as should do the following:

1. Compute $t_{out}=(t_{in},S_n,P_d,\lambda.a)$
2. Sign $t_{out}^{*} = \left(t_{out}, Sign_{as}\left(t_{out}\right)\right)$;
3. Pass t_{out}^{*} to P and lets him to exit the scheme successfully;

Verify ticket: passenger P should do the following:

1. Check a signature of t_{out}^{*};

Passenger Assumptions

Through the scheme exit protocol, as cannot follow the protocol because of various causes. For example *as* may fail, produce errors, or entrust corrupt activities. Due to that, the sincere passenger will receive the illegal service. To solve such problem, the protocol could face two passenger assumptions.

1. **Assumption 1: Wrong λ* is received**

Through the scheme exit protocol, customer *P* can pass the validation data (t_{in},k), but as could behave badly and passes the incorrect λ. For example, the message has the inexact τ_2 to *P* or, *as* is not passed it. Then, such passenger can claim to receive the valid λ* to payment *AT eg* by the subsequent steps:

Step 1 request: The passenger *P* should do the following:

1. pass (t_{in}^{*}, k)
2. send wrong λ* to *eg*;

Step 2 reply: The payment *TA eg* should do the following:

1. Check the signature of t_{in}^{*} which is calculated by *ss*;
2. Check that $\sigma.h_{L_3} \equiv hash(L_3)$, show that *P* is the true owner of the ticket t_{in};
3. In case of a wrong (λ^*, eg) check that the variables $B.\tau_2$ or $\lambda.\ a$ are not correct. For instance$\lambda.\tau_2$ is greater than the present time;
4. Select a new timestamp τ_2. *eg* can do that to compensate the user because of the time overhead created by the current transaction in relation to the time if the scheme exit sub-protocol was performed;
5. Compute the charge to be paid based on an elapsed time between related timestamps τ_1, τ_2 by $a=f_t(as,t_{in}.ss,t_{in}.\tau_1,\tau_2)$;
6. Select the integer $L_4 \in Z_q$;
7. Compute $\lambda=(t_{in}^{*},a,L_4,\tau_2,P_d)$;
8. Sign $\lambda^*=(B,Sign_{eg}\ (B))$;
9. pass λ^* to *P*;

Step 3 resume: The scheme does the following:

1. The scheme exit, protocol keeps on as normal.

1. Assumption 2: Wrong t^*_{out} is received

Through the scheme exit protocol, P can pass the validation knowledge (t^*_{in},L_3,e_p), but as can behave badly and passes the wrong t^*_{out} to P or just denies to pass it. Then, the passenger can communicate with a payment TA eg and he can claim to receive the valid t^*_{out} by the subsequent steps:

Step 1 request: The passenger P should do the following:

1. pass $(t^*_{in},L_3,\lambda^*,e_p)$ to eg;

Step 2 reply: The payment TA eg should do the following:

1. Check a signature of t^*_{in} which is calculated by ss;
2. Check an identity of P by Schnorr ZKP by $a^{L_5} = L_2.(e_P)^{L_4}$;
3. Check that $\sigma.h_{L_3} \equiv hash(L_3)$, shows that P is a correct owner of the ticket t_{in};
4. Compute the ticket cost to be paid based on the elapsed time between related timestamps (τ_1,τ_2) by $a=f_t(t_{in}.ss,\lambda.as,t_{in}.\tau_1,\lambda.\tau2)$;
5. Check that the computed value a is equivalent to $\lambda.a$. In case of the non-positive verification, the passenger is addressed to perform the protocol at assumption 1;
6. Find $t_{out}=(t_{in}.S_n,\lambda.a))$;
7. Sign $t^*_{out}=(t_{out},Sign_{eg}(t_{out}))$;
8. Pass t^*_{out} to passenger P ;

Step 3 resume: The scheme does the following:

1. The scheme exit, protocol keeps on as normal.

Remarks

In both assumptions, the payment TA eg has to:

1. Inform as of its bad behavior or message problems with passenger.
2. Notify as of possible more actions if such problem continues.

Issuer Assumptions

Through the scheme exit protocol, P cannot follow the protocol because of various causes. For example, P may be unsuccessful, make errors, entrust corrupt actives. Due to that, the supplier will receive the illegal service. To solve such problem, the proposed protocol can face two supplier assumptions.

1. Assumption 1: Wrong (t_{in}^{*},L_3) is received

Through the scheme exit protocol, *as* receives the first step of a checking message (t_{in}^{*},L_3), but this message cannot be true. Then, the service supplier can claim to reveal customer identity by the subsequent steps:

Step 1 request: The destination service issuer as should do the following:

1. Pass (t_{in}^{*},L_3) to *ed*;

Step 2 request passenger: The passenger *P* should do the following:

1. Pass also (t_{in}^{*}, L_3) to *ed*, to evade false complaints;

Step 3 reply: The group *TA ed* should do the following when *P* is not passed the needed items:

1. Check a signature of (t_{in}^{*}, L_3) which is created by *ss*;
2. Check the connection with the secure hash value $t_{in}.\sigma.h_{L_3} \equiv hash(L_3)$ when a connection is not checked, *ed* terminates the claim;
3. Check the group signature of $t_{in}.\sigma^{*}$ which is created by *P*;
4. Revealing who is a signer inside the group;
5. Pass the passenger identification *Pi* to *as*;
6. Send e_P to *eg*;
7. add P_i to the revocated list;

1. Assumption 1: Wrong e_P is received

Through the scheme exit protocol, *as* and *eg* gets the last step of the checking message e_P, but this message cannot be true. Thus, the service issuer can claim to reveal passenger identity by the subsequent steps:

Step 1 request: The payment *TA eg* should do the following:

1. Compute the payment rejection ko=('verification information error', e_P);
2. Sign $ko^{*}=(ko, Sign_{eg}(ko))$;
3. Pass ko^{*} to *as* ;
4. Pass $(skas\ (e_P),y_{as})$ to *ed*
5. End the protocol.

Step 2 Issuer information: The destination service issuer *as* should do the following:

1. Pass (t_{in}^*,L_3) to *ed*

Step 3 request passenger: passenger P should do the following:

1. pass (t_{in}^*,L_3,e_p) to *ed*, to evade false complaints;

Step 4 reply: The group *TA ed* should do the following:

1. Check when the decrypted message of e_P, y_{as} and (t_{in}^*,L_3) connect;
2. Check the group signature of $t_{in}.\sigma^*$ which is generated by P;
3. Revealing who is the signer inside the group;
4. Pass the passenger identification P_i to *as*;
5. Pass e_P to *eg*;
6. Add P_i to the revocated list;

SECURITY ANALYSIS

The proposed scheme achieves the security requirements described in section 4. The achievements are as follows:

The Authenticity

The formation of fake ticket is totally not practical these days. Since, the tickets are signed $t_{in}^* = \left(Sign_{ss}\left(t_{in}\right)\right)$ and $t_{out}^* = \left(t_{out}, Sign_{as}\left(t_{out}\right)\right)$, also the posted information previous to a payment $\lambda^*=(\lambda, Sign_{as}(\lambda))$. When the illegal passenger can generate the valid ticket (entry or exit) without information of the secret keys neither of *ss* nor *as*, it can create digital signature while pretend to be such issuers. Assume that we use the digital signature scheme, this process is not practical. Conversely, the passenger passes the verification message signed with his group secret key $\sigma^*=(\sigma, Sign_G(\sigma))$. Such signature ensures that a message is real and is issued by the valid passenger.

Non-repudiation

The issuer of the ticket cannot repudiate the release of such ticket. The ticket is signed by its official provider and, by allowing for that the applied signature scheme is safe, such operation can be only done by these issuers. Therefore, the issuer identity is connected to the ticket and, for the characteristics of the e-signature scheme, that issuer cannot repudiate its compilation. The same happens with a group signature scheme, when an identity is revealed, a message compilation can be checked.

Integrity

Once the ticket is generated cannot be changed. Assume that a hash function is secure and its inverse function is totally impossible these days. If ticket content is changed, the checking of the signature will be wrong. To exceed the checking, the signature will be required to be recreated from the new ticket content. Such operation is totally impossible these days in the most present machines.

Validity Period

The ticket is not more valid when its validity time T_v is expired. The target station as extradites a ticket from the passenger to be checked. In this verification, the present time is compared with a validity time T_v of an entry ticket t_{in}^* which is signed by ss. The information regarding a passenger identity is encrypted by a payment TA public key. The authorized issuers (ss and as) cannot get access to such information since they require the secret key of the TA. In the proposed scheme, passengers calculate the group signature $(t_{in}.\sigma^*=(\sigma,Sign_G(\sigma)))$ which verify a signer is the valid group member. When we consider the characteristics of a group signature scheme, an issuer cannot reveal an identity of a signature generator. In case of debatable circumstances, an identity of a passenger which signed the content might be revealed during the verification of both payment $TA\ eg$ and the group $TA\ ed$.

Revocable Anonymity

The ticket is anonymous. The passenger is anonymous by an authorized issuer through a payment protocol. The content regarding a payment is encrypted and just a payment TA can get access to it. The authorized issuer is outside to the payment, and just receives the payment verification from the payment $TA\ eg$. So, eg has information concerning e_P from the pair (d_P, e_P) such that $e_p = a^{d_p}$ mod p, which identifies him as the valid passenger. Then, the passenger authenticates by showing information of d_p by Schnorr ZKP.

Non-traceability

The group signatures done by the same passenger should be untraceable by the authorized issuers or other bodies outside to the scheme. The group signature in ref. [7] by Boneh, et al. [8] applies the probabilistic signature scheme. It is not likely to guess the encrypted message given the certain message. This lets difficultly between various group signatures done by the same passenger.

Non-double-spending

The scheme prevents ticket double-spending. When the passenger attempts to double-spend an entry ticket, the serial number is signed as already used. When such passenger bad behavior is showed, the group $TA\ ed$ can add in such passenger to a revocation list.

Conspiring Attack

The time-typed fare collection scheme illustrated in section 5 cannot be attacked by conspired passengers. The conspiring attack illustrated in 6.2 using the swap of entry tickets is not applicable to time-typed because the passengers do not get any gain of the exchange. The fare is computed using the entry timestamp thus when the passengers swap their tickets the charges are the same and one of the passengers will pay more than her actual ticket. Therefore passengers are discouraged to swap tickets.

CONCLUSIONS

We have introduced a secure e-ticket fare scheme which is tailored for huge passengers transport. We have accomplished the scheme that can be tailored to time-typed or distance-typed charge with somewhat modifications. The utilize of group signatures schemes lets the passenger authentication whereas it is preserved his privacy. But, the identity of passengers can be reveal in case of the passenger bad behavior. The proposed scheme does not need to get the new credential each time the passenger links in the scheme to get intractability and to avoid tracking and profiling. Thus, the proposed scheme resistant from attacks of conspired passenger.

The future work leaves to the direction and extend the new communication tools more appropriate for e-commerce systems such area of communication, which is planned mainly for use in mobile phones.

REFERENCES

1. Heydt-Benjamin T, Chae H, Defend B, Fu K (2006) Privacy for public transportation, 6th Workshop on Privacy Enhancing Technologies (PET 2006), pp: 1-19.
2. Madlmayr G, Kleebauer P, Langer J, Scharinger J (2008) Secure communication between web browsers and NFC targets by the example of an e-ticketing system. EC-Web08: Proceedings of the 9th international conference on E-Commerce and Web Technologies, Berlin, Heidelberg, Springer-Verlag. pp: 1-10.
3. Vives-Guasch A, Castella-Roca J, Payeras-Capella M, Mut M (2010) An electronic and secure automatic fare collection system with revocable anonymity for users. 8th International Conference on Advances in Mobile Computing and Multimedia (MoMM).

4. Isern-Deyà AP, Vives-Guasch A, Mut-Puigserver M, Payeras-Capellà M, Castellà-Roca J (2012) A Secure Automatic Fare Collection System for Time-Based or Distance-Based Services with Revocable Anonymity for Users. The Computer Journal.
5. Arfaoui G, Dabosville G, Gambs S, Lacharme P, Lalande JF (2014) A Privacy-Preserving NFC Mobile Pass for Transport Systems. EAI Endorsed Transactions on Mobile Communications and Applications, pp: 09-12.
6. Magdalena Payeras M, Mut-Puigserver M, Castellà Roca J, Bondia Barceló J (2016) Design and Performance Evaluation of Two Approaches to Obtain Anonymity in Transferable Electronic Ticketing Schemes. Mobile Networks and Applications pp: 1-20.
7. Schnorr C (1991) Efficient signature generation by smart cards. The Computer Journal 4: 161-174.
8. Boneh D, Boyen X, Shacham H (2004) Short group signatures. CRYPTO, Lecture Notes in Computer Science 3152: 41-55.