2PLoc: Preserving Privacy in Location-Based Services

Amir Salar Amoli
Department of Information Technology
Qom University, Qom, Iran
and
Sharif Network Security Center
Sharif University of Technology, Tehran, Iran
salar@cert.sharif.edu

Mehdi Kharrazi
Sharif Network Security Center
Department of Computer Engineering
Sharif University of Technology
Tehran, Iran
kharrazi@sharif.edu

Rasool Jalili
Sharif Network Security Center
Department of Computer Engineering
Sharif University of Technology
Tehran, Iran
jalili@sharif.edu

***Abstract*—Location-based services are becoming popular for mobile users. The mobile users' location plays a key role to provide the service from one side, but it can be considered as a dimension of their privacy and so necessary to keep it anonymous to the other parties. Since one important issue is to achieve an accurate service, it is important to use the mobile's accurate location. Using the location accurately raises some concerns on behalf of the user's privacy. One solution for meeting this requirement is using tickets by the means of a third party. The tickets should have some properties for not letting a mobile user to cheat and use the ticket more than one time.**

This paper proposes a protocol to preserve Preserve Privacy in Location based services, in short 2PLoc, aimed to provide anonymity of location, for location based services, based on one-time tickets regardless of the existence of any trusted third party. The protocol satisfies the requirement of accurate location use, as well as the ability of revoking anonymity on the ticket double spending. The user, location-based service provider, and the ticket issuer are the three untrusted parties in 2PLoc. 2PLoc is based on a special designed ticket that disconnects the relation between the location of the mobile user and its identity. The ticket is designed based on the blind signature and the concept of elliptic curves discrete logarithm.

***Index Terms*—Privacy; Location-Based Services; Location Privacy; Mobile-Commerce;**

I. Introduction

With the wide availability of online services, and ease of connectivity, E-commerce has gained a significant portion of the consumer market in the past few year. Morover with the wide availability of portable devices (i.e. mobile handsets, PDAs, etc.), another form of commerce, named Mobile-Commerce is gaining ground. This is specially true, given the current mobile technology, where users can access the Internet, virtually from any location, be it in office, at home, or on the road. Nevertheless M-Commerce services are faced' with a number of challenges, inherent to the mobile devices. These include low computation power, limited bandwidth, and storage space.

One of the main services provided in M-Commerce is location based services in short LBS. As the name suggests, such services are dependent on the location of the user. Where the location of the service requester is calculated with the help of technologies such as GPS, and then passed with the user's service request to the service provider. The service provider then responds to the user taking into account the mobile user's location. For example, tourist guides, navigational information, location sensitive billing, and etc.

One of the most important issues in M-commerce is the privacy of the users' information. As the location of the user should be transmitted with the user request, the most important issue for a user is location privacy. Hence an important aspect of LBS algorithms is to preserve location privacy for the user. To give a few examples, suppose that the system finds out that the user goes to a center for cancer treatment, it can then infer that he/she is diagnosed with cancer. By finding out this piece of information, very private information is revealed. As another example, the system recognizes that a user has been in a specific shopping center that provides some specific sporting goods, it may then annoy the user by sending targetted advertisements to the user. Duckham and Kulik [1] mentioned these impacts in three categories: Location-based spam, Personal safety, Intrusive inferences.

As an example of the usability of such protocols, consider the following example. Assume a service agency provides a subscription service and arranges taxis to pickup the customer when they request transport, so that every customer is allowed a limited number of taxi services for a fixed monthly amount. For such a system to work, the customer should first provide his/her subscription information to the agency as well as his/her location. But there are a number of important issues which would arise:

The customer would like to preserve his/her location privacy, hence non of his/her requests should tie to a subscription id, and the service should be requestable through a mobile handset. On the otherhand and from the service provider perspective, the customer should not be able to cheat the system, either by forging subscription information, or double-spending. Furthermore, the agency would like to be able to revoke the anonymity of the customer, if there is any double spending.

Given the above requirements, in this paper, we propose a protocol to **P**reserve **P**rivacy in **Loc**ation based services, in short **2PLoc**, where the proposed protocol provides the

following features:

- User and location are unlinkable
- Low-cost computation
- Non-forgeable
- Double-spending resistant
- Revocation of the user id, in the event of double spending

The structure for the rest of the paper is as follows, in Section II we survey related work. In Section III some of the basic concepts used in the protocol are described. The protocol 2PLoc is discussed in section IV. Section V evaluates the 2PLoc protocol and finally we conclude in Section VI.

II. Related Work

One could classify approaches for preserving the users' privacy in location-based services into three categories, specifying policies on location privacy between the user and the system, focusing on the location data itself and hiding the location before it is sent to the LBS, and lastly location privacy is preserved by hiding the relation between the user's identity and its location. In what follows we will review related works in each of these stated categories:

In policy-based approaches, a set of rules are legislated which define how information is to be stored and used. In addition, the rules show when and in what conditions the data can be revealed. Kaasinen [2] where the first to employe a policy-based approach in their proposed framework. But since the involved parties are not obligated to obey such rules, such approach would not be applicable to our problem statement.

The second category of techniques, is based on hiding the location data before sending it to the LBS. This category in itslef could be divided into three categories:

- k-anonymity works by hiding the location of a user within a set of k members. An anonymizer is employed to collect the users' locations and categorize them in some k-size sets, and then one of the members of the location set is selected as the representive of the location of all those users. Most published k-anonymity approaches use a trusted third party as an anonymizer where the implemntation could be based on a centralized [3] or distributed [4], [5] architecture. One of the important challenges in k-anonymity is to find k-1 other users to keep the anonymity. Two other problems with k-anonymity approaches are the reduction of accuracy and the need for a trusted third party.
- To overcome the lack of finding k-1 other users, dummy-based approaches are used [6], [7]. In dummy-based approaches, the user creates some dummy location and sends them beside its real location to the service provider. Lu, *et al.*[6], proposed two different solutions for generating dummy points. The approach solves the problem of inaccuracy; however, on the other hand, the cost of the service increases incredibly; indeed, in some scenarios, such as the *e.g.* Taxi Agency, such approach is not applicable.
- Another way to hide the user's location is its obfuscation. obfuscation means instead of sending some extra locations, a function of the location is calculated and sent to the service provider. Ardagna *et al.* in [8] illustrated three different ways for location obfuscation: increasing the location radius, decreasing the location radius, and transforming the location. Because of the accuracy reduction and decrease in the quality of service, this approach is also not applicable in most location-based service scenarios.

There are some shortcomings in all these aforementioned approaches. Because of the high cost of calculation or the low quality of service due to the inaccuracy of the reported location, these approaches are not applicable in most mobile location based services. In most services such as taxi services, the accurate location is needed to give a service. In such applications a method should be presented, in which the privacy is preserved while the location remains accurate. In the designed protocol, the user's location should be kept unrelated to its identity. One way to do so, is to employ the concept of tickets. Lee *et al.* in 2008 in [9] defines a ticket as, "In mobile communications, a ticket is a piece of data which is analogous to tickets we use in various social events". Therefore, the ticket lets the user prove that it has been authorized to access to a LBS such as the taxi service.

Unforgeability and non-reusability are two of the main characteristics of a ticket [10]. A ticket has also some advantages such as scalability, flexibility, and privacy[9]. Tickets are used to bind a user and a service or service providers to each other. For example, a cinema ticket can be issued without the need of specifying the person who will use it. There are many applications in which tickets can be used, therefore several types of tickets can be defined. Wang et al, in 2004, designed different types of tickets using digital signatures and multi signatures [10].

In 2008, Lee *et al.* proposed a method to issue a reusable ticket [9]. They employed a hash chain in issuing the ticket to bind the four elements: mobile user, value-added service provider, ticket server, and certificate authority. The method assumed that the users, service provider, and ticket server trust the certificate authority. Chen *et al.* in 2007 developed a ticket based on public keys[11]. Subscriber, observer, mobile network service provider, ticket service provider, and verifier were the five main elements of their protocol. They assumed that the mobile network service and observer are trusted.

Piotrowski *et al.*, in [12] proposed Moneta as a payment method based on ticket. This method uses public key cryptography and supports limited anonymity. The limited anonymity means that if the ticket is used in double-spending, the identity of the user is revealed. The method relies on a certificate authority as a trusted third party. The shortcoming with this method is that that the user is able to cheat while providing its identity. Lastly, Quercia *et al.* in [13] proposed a method that includes anonymity and revoke anonymity. However the big number of the protocol rounds made the protocol inefficient.

The ticket-based protocls discussed above, have important

properties such as using TTP [1]rusted Third Party, anonymity, and the ability to revoke anonymity in; but none are able to provide these features together. The only execption woud be the work by Quercia *et al.* in [13], which has other shortcomings as we will discuss in Section V. Hence as non of the methods are suitable for mobile environments, we will propose a method to cover all those needs. The rest of the paper describes the proposed protocol.

III. Basic Concepts

Before introducing our proposed protocol, we will brifly review blind signatures and elliptic curves as we will be employing them in the proposed protocol.

A. Blind Signature

Blind signature is a method of concealing a data item from the person/entity who is signing that. Chaum's Blind Signature scheme[14] is used in 2PLoc.

In this approach, the signer signs the data regardless to what the content is. In order to sign, first the client calculates the hash value (H) of the data, then chooses a random blinding factor b and calculates the blinded hash value ($H^{'}(data)$). ((n,e) is the signer's public key).

$$H^{'}(data) = b^{e}.H(data)(mod\ n)$$

The signer signs the blinded hash using its own private key (n,d) and the resulted blinded signature($Sig^{'}$) is sent back to the client. In the signature, d is the exponent from the signer's private key.

$$sig^{'} = (H^{'}(data))^{d}(mod\ n)$$

At end, the client unblinds the blinded signature and fetches a signature (Sig) for the data.

$$Sig = b^{-1}.Sig^{'}(mod\ n)$$

B. Elliptic Curve

Based on [15], an elliptic curve E over k is defined as bellow.

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$$

Where ($a_1, a_2, a_3, a_4, a_5 \in k$). This equation is called Weierstrass.

The negation of $P = (x_1, y_1)$ is written $-P$ and is defined as $-P = (x_1, -y_1)$.

Considering the two points $P = (x_1, y_1)$ and $Q = (x2, y2)$ that $P \neq -Q$, $P + Q$ is equal to $R = (x_r, y_r)$, that

$$x_r = s^2 - x_p - x_q\ and\ y_r = -y_p + s.(x_p - x_r)$$

where ($S = (y_p - y_q)/(x_p - x_q)$). It is obvious that S is the slope of the line passing through P and Q. Elliptic Curve Discrete Logarithm Problem (ECDLP), which is being used for hiding some of the ticket information, is defined as bellow:

If E is an Elliptic Curve on a finite field K and $P \in E(K)$ in order n, Given $Q \in E(K)$, the elliptic curve discrete logarithm problem is to find the integer $d \in [0, n-1]$, such that $Q = dP$.

[1]T

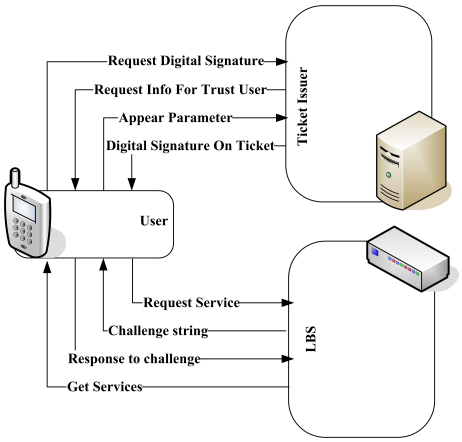

Fig. 1: 2PLoc Protocol

IV. The Proposed Protocol: 2PLoc

In this section we introduce **2PLoc**, a protocol which **P**reserves **P**rivacy in **Loc**ation based services. The protocol utilizes the concept of tickets, aimed to declare if the user is authorized for some services, without being authenticated. The designed ticket is anonymous and unforgeable; however, its anonymity is revoked when double-spending occurs.

As denoted in Figure 1, three parties are employed in our schema: users, the ticket issuer (TI), and the location-based service provider(LBS). Users or customers are the entities who request the service. LBS provides the service, based on the users' location. TI is responsible for authenticating the users and moreover, issues an anonymous ticket for the users to be used to get service from LBS.

As Figure 1 depicts, the protocol is divided into two phases: 1)requesting and issuing the ticket, and 2)requesting and obtaining the service.

In the first phase, the user gains the trust of the TI by going through a set of cut and choose operations and receives the signed ticket. In the second phase, the user submits his/her request to LBS and receives the service after the ticket and its ownership have been being verified. This verification is required so that the ticket may not be trasferred to another user. Furthermore, this is done through a challenge and response operation. Going to the details of the two phases of the protocol, the following assumptions are worth mentioning.

- It's not important what technology is employed to obtain the user location. We only assume that the user's location is provided accuratly to the LBS.
- There is no need for the parties to trust each other in order for the protocol to operate correctly; i.e. it is not possible to make collusion even if LBS and TI cooperate to disclose the identity and location of the user.
- Before initializing the transaction, it is assumed that both the user and LBS are registered with TI. The registration of the user means that all its personal and required information are provided to Ticket Issuer and it is assigned a userID. Hence, the user is identified and

Id_{sp}	Identity of LBS
Id_u	Identity of User
Sn	Ticket Serial Number
b	Secret Value for Blind
c_1, c_2, s	User Secret for Hidden Serial Number
P	a Point On Elliptic Curve

TABLE I: 2PLoc Notations

authenticated to the system using the allocated userID.

- The user will be authenticated and therfore, identified to the system by providing its unique userID; however, no assumption on the authentication mechanism exists.

A. The Ticket Structure

The designed anonymous ticket structure is as follows:
$Ticket = (Sign(T^{'}), W, Z, A, B, t)$

Where $Sign(T^{'})$ is the signature of the issuer on $T^{'}$, and $T^{'} = Hash(W_x \bigoplus Z_x \bigoplus t \bigoplus Id_{sp})$. The identity of Service Provider makes the ticket usable for a specific service. t is the time of issuing the ticket, and shows the validity time period of the ticket. W, Z, A and B are the points on Elliptic Curve for hiding and revealing the serial number (Sn) and the serial number embedded in point W $(W = Sn.s * P)$. Ticket serial number used for identity ticket and relevant to user ID. $Sign(T^{'})$ is done by TI then user completes the ticket.

B. Issuing the Ticket

Blind signature and hidden identity are used to issue a ticket. Ticket Issuer contains a pair of public and private keys, which uses them to sign the ticket, blindly. In order to hide the identity, all the parties should agree on the elliptic curve, E, over the finite field, K, and the point, p. The notations used in 2PLoc are shown in Table. I.

The steps of issuing a ticket in 2PLoc are as follows:

1) The ticket is constructed:
   a) The user selects three random numbers, S_i, B_i and $Sn_i (1 \leqq i \leqq k)$. and calculate Z and W
   $$W_i = Sn_i \ . \ s * P, Z_i = s_i * P$$
   Note: By $'.'$ we mean number multiplication and by $'*'$ we mean elliptic curve point multiplication.
   b) The points $Z_i = (x_{z_i}, y_{z_i})$ and $W_i = (x_{w_i}, y_{w_i}) (1 \leqq i \leqq k)$ are computed over E to hide the serial numbers based on the aforementioned numbers. to simplify the notation reconsider $w_i = x_{w_i}$ and $z_i = x_{z_i}$.
   c) Using w_i, z_i, t and the identity of the service provider (Id_sp), a part of the ticket that TI must sign it, made and blinded with b_i.
   $$T_i = h(w_i \oplus z_i \oplus Id_{sp} \oplus t) \ .$$
   d) Using the secret b_i the constructed ticket becomes blind
   $$blind(T_i) = b_i^e.T_i \ .$$
   e) The user sends the k blinded tickets, t, S_{n_i}, Id_u and Id_{sp} to Ticket Issuer.
2) Ticket Issuer randomly selects $k-1$ tickets among the k tickets received from the user and asks him/her to reveal the respected s and b, by which the tickets were constructed.
3) The user sends the requested parameters to TI. $L = \{i_j | (1 \leqq i \leqq k) and (1 \leqq j \leqq k-1)\}$
4) TI computes all the $k-1$ selected tickets using the received parameters and validates them. If all the $k-1$ tickets were valid, TI trusts to the user and signs the last remaining ticket, W and Z.
   $$sign(T_i) = blind(T_i)^d \ mod \ n; i \subsetneq L \ and (1 \leqq i \leqq k)$$

C. Requesting and Obtain Service

In this phase, the user owns a partial valid ticket issued by TI and wants requests for a location-based service. Before requesting the service, the user is supposed to complete the ticket by computing and adding two other parts to it. In the rest of the phase, LBS authenticates the ticket in a challenge response approach. The steps of the phase are as follows:

1) The user unblinds the blinded signature of the ticket, $sign(T^{'})$.
2) The user selects two random numbers, c_1 and c_2, then computes two points A and B on E using them. Now the ticket is completed while composed of $sign(T^{'}), W, Z, A, B,$ and t. The completed ticket as part of the request send to the LBS.
   $$A = c_1 * P, \ B = c_2 * P, \ Ticket = (sign(T^{'}), A, B, W, Z, t)$$
3) LBS verifies the signature. If the signature is valid, a challenge, x, is sent to the user.
4) The user computes f(x) and g(x), and sends them to the LBS as the response.
   $$f(x) = Sn.s.x + c_1, \ g(x) = s.x + c_2$$
5) LBS evaluates the two expressions as follows
   $$f(x) * P = W * x + A, \ g(x) * P = Z * x + B$$
   if both are true LBS provides the service to the user.

D. Revoking Anonymity

2PLoc avoids users from double-spending; i.e. the user is not able to use one ticket twice for getting a service. The ticket is designed in a manner that by double-spending the serial number of the ticket is revealed. Since TI maintains the ticket serial number and its aligned user's identity, LBS can reveal the Id of the user by interacting with TI.

In each use of the ticket, a challenge is given to the user and it is supposed to compute the response. The response $(f(x)$ and $g(x))$ are stored beside the ticket in LBS. If double-spending occurs, LBS asks the user to calculate a second response by sending him a second challenge. By the means of the two pairs of the responses, LBS can reveal the serial number of the ticket by computing the following expression:

C_{hash}	Computation of Hash function
C_{blind}	Computation of Blind Data
$C_{unblind}$	Computation of unBlind Data
C_{xor}	Computation of XOR
C_{mul}	Computation of ECC Multiplicity
C_{enc}	Computation of Encrypt Data
C_{dec}	Computation of Decrypt Data
$C_{service}$	Computation of Calculate Services

TABLE II: 2PLoc Time Notions

$$Sn = \frac{f(x_1)-f(x_2)}{g(x_1)-g(x_2)}$$

V. Discussion and Evaluation

In this section, we discuss a number of issues about the proposed protocol, 2PLoc, in a number of aspects: discovery of users' fraud, possible attacks on the protocol, and lasly computational evaluation of 2PLoc.

A. Discovery of Fraud

The user may cheat in any of the two phases, ticket issuance or usage. In the first phase, the ticket is issued using the identity of the user. Since TI is not aware of the content of the ticket, the user can insert any false identity in the ticket. In this case, even if the anonymity is revoked, the true identity of the user will not be determined. The other type of fraud can occur in the second phase by using the ticket for more than one time.

In order to solve the first problem, the user should create a defined number of tickets, k, and send to TI. TI is supposed to validate the k-1 tickets by the help of the user. If all the k-1 tickets are valid, Ticket Issuer signs the last ticket. If the user tries to cheat in this stage, two cases may occur: The user has created more than one false ticket. In this case, because TI validates k-1 tickets, it will certainly out figure the fraud.

The user creates only one false ticket. Since TI selects and checks k-1 tickets randomly, the probability of discovering the fraud equals to k-1/k. Thus, if the number k increases the probability of fraud discovery increases too. Therefore, there is a trade of between the efficiency of the system and the probability of the fraud discovery. One solution to ease the problem of trade off may be using the history of the trustiness of the user's in determining the number k.

The second problem is referred to double-spending in the secend phase. As being shown in former section, at the time of providing the ticket to LBS by the user the fraud is discovered. When a double-spent ticket is given to LBS, it starts a challenge response with the faulty user. By receiving the responses from the user, LBS is able to reveal the ticket's serial number by calculating expression that introduce in subsection D. Therefore, LBS and TI can determine the identity of the cheating user.

B. The Possible Attacks

1) Eavesdropping: In this attack, the attacker listens to the messages transmitting without altering the message. This sort of attacks occur more in the wireless environments. Eavesdropping is not a sever attack in $2PLoc$, because there is not any relation between issuing the ticket and using it. At the time of issuing the ticket, because of the blind signature, even TI is not aware of the content of the ticket of the ticket. The attacker also will find out no useful information by eavesdropping at the time of achieving the service. It can only find out some information about the service itself, which does not violate the privacy of the user.

2) Manipulating the Data: The integrity mechanism used in $2PLoc$ avoids any alteration of data while transmitting them. Using digital signature assures the integrity of the ticket at the time of issuing it. At the time of using the ticket, the challenge response mechanism used in the protocol leads to the discovery of manipulation.

C. Computational Evaluation

In this section we will study the number and type of computations used in different phases of 2PLoc protocol and represent computational order needed for each part of the system. In order to gain more clarity, we use the pre-compute concept that was introduced in [16]. The pre-compute concept is used for those computations which can be performed before a transaction starts and are independent of other computations results. Therefore, we will not consider pre-computable parts of the transactions in in our analysis of the total work required.

We evaluate the protocol in two phase: Issuing ticket phase and services phase. Briefly in issuing phase, user constructs k tickets and opens k-1 of them for proving his honesty to issuer and then the issuer signs the remaining ticket. In the services phase, no significant work is done by the user, and the computations are limited to some mathematical operations like add and multiply to verify the ticket ownership.

As depicted in table III, all computations are done before starting the transaction for issuing the ticket, therefore the mobile user should not do any extra work and it will be o(0). notice that, in next phase in table IV all the work the user does online is to unblind the signature and all other tasks can be done offline. so the computational cost of the second phase is $C_{unblinde}$. Notations used for the computational evaluation can be found in table II.

The most computational work is done on the ticket issuer side. The amount of computational work depends on issuers trust level to users and hence the value selected for k. We can find a proper value for k by practical experiments and implementation in a real environment.

As described in the related works section, the protocol proposed by Quercia, et. al. [13] called "motet" is the closest work to th proposed 2PLoc protocol. In their method, both features of anonymity and anonymity revocation exists and similar to 2PLoc, the "motet" method does not take advantage of a trusted third party In Table V, the computation cost and the number of rounds that each transaction needs are depicted. As shown in the table, the number of required rounds in "motet" is 10 where only 8 rounds are required in 2PLoc, where a 20% decrease would result in a shorter communication cost. In addition, only $C_{unblind}$ is included in

	User	Ticket Issuer
Generate Tikcet	$C_{mul} + 3C_{xor} + C_{hash} + C_{blind}$	-
Verify Ticket	-	$C_{mul} + 3C_{xor} + C_{hash} + C_{blind}$
Sign	-	C_{enc}
Total	–	$(k-1)C_{mul} + 3C_{xor} + C_{hash} + C_{blind} + Cenc$

TABLE III: Ticket Issuing

	User	LBS
UnBlind Ticket	$C_{Unblind}$	-
Calculate two point	$2C_{mul}$	-
Verify signture	-	$3C_{xor} + C_{hash} + C_{dec} + 4C_{mul}$
Serve	-	$C_{service}$
Total	$C_{unblind}$	$3C_{xor} + C_{hash} + C_{dec} + 4Cmul + C_{service}$

TABLE IV: Obtain Service Phase

		Motet	2PLoc
Ticket Issue	TI	$4C_{enc}$	$2C_{mul} + C_h + C_{blind} + C_{enc}$
	User	$3C_{enc}$	-
	Round	4	4
Obtain Service	LBS	$4C_{dec}$	$4C_{mul} + C_{dec}$
	User	$2C_{enc}$	$C_{unblind}$
	Round	6	4

TABLE V: Compare with Motet [13]

the computation cost of 2PLoc whereas the cost of "motet" approach is $5C_{enc}$. This is of great importance, considering the fact that encryption is a much more expensive operation as compared to the unblinding operation.

VI. Conclusion

Developing M-Commerce solutions is difficult due to some limitations such as low bandwidth, computational power and storage capabilities in the mobile devices. One of the main types of services given in this environment is based on the mobile user's location. This sort of services is given by location-based service provider (LBS). Because of the sensitivity of the user's privacy such as location, it is necessary to keep it anonymous. In this paper, we proposed 2PLoc, a protocol for preserving the privacy of the user's location, in m-commerce transactions. The protocol is among three untrusted parties: the mobile user, LBS, and ticket issuer. A new ticket is designed, which requires no trust among any of the involved parties. The ticket disconnects the relation between the location and identity of the mobile user. The evaluations show that the protocol is strong enough against some of the possible attacks, and is able to discover the user's fraud in the event of double spending.

References

[1] M. Duckham and L. Kulik, "Location privacy and location-aware computing," *Dynamic and Mobile GIS: Investigating Change in Space and Time*, p. 3451, 2006.

[2] E. Kaasinen, "User needs for location-aware mobile services," *Personal and Ubiquitous Computing*, vol. 7, no. 1, pp. 70–79, 2003.

[3] B. Gedik, L. Liu, and G. Tech, "Location privacy in mobile systems: A personalized anonymization model," 2005.

[4] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "Prive: anonymous location-based queries in distributed mobile systems," *Proceedings of the 16th international conference on World Wide Web*, pp. 371–380, 2007.

[5] A. Solanas and A. Martnez-Ballest, "A ttp-free protocol for location privacy in location-based services," *Computer Communications*, vol. 31, no. 6, pp. 1181–1191, 2008.

[6] H. Lu, C. S. Jensen, and M. L. Yiu, "Pad: Privacy-area aware, dummy-based location privacy in mobile services," in *Seventh International ACM Workshop on Data Engineering for Wireless and Mobile Access*, (Vancouver, Canada), 2008.

[7] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *Proceedings of IEEE International Conference on Pervasive Services, ICPS*, p. 8897, 2005.

[8] C. A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati, "Location privacy protection through obfuscation-based techniques," *Lecture Note In Computer Sience*, vol. 4602, p. 47, 2007.

[9] Y. Lei, A. Quintero, and S. Pierre, "Mobile services access and payment through reusable tickets," *Computer Communications*, vol. 32, no. 4, pp. 602–610, 2008.

[10] H. Wang, Y. Zhang, J. Cao, and Y. Kambayahsi, "A global ticket-based access scheme for mobile users," *Information Systems Frontiers*, vol. 6, no. 1, pp. 35–46, 2004.

[11] Y. Y. Chen, C. L. Chen, and J. K. Jan, "A mobile ticket system based on personal trusted device," *Wireless Personal Communications*, vol. 40, no. 4, pp. 569–578, 2007.

[12] K. Piotrowski, P. Langendrfer, and D. Kulikowski, "Moneta: An anonymity providing lightweight payment system for mobile devices," *Grimm, R., N J., eds.: Virtual Goods*, 2004.

[13] D. Quercia and S. Hailes, "Motet: Mobile transactions using electronic tickets," *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, pp. 374–383, 2005.

[14] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology: Proceedings of Crypto*, vol. 82, p. 199203, 1983.

[15] D. R. Hankerson, S. A. Vanstone, and A. J. Menezes, *Guide to elliptic curve cryptography*. Springer-Verlag New York Inc, 2004.

[16] R. C. W. C. C. Yang, Y. L. Tang, "A secure and efficient authentication protocol for anonymous channel in wireless communications," *Applied Mathematics and Computation*, vol. 169, pp. 1431–1439, 2005.