ISSN 2007-9737

Anonymity and Privacy Security Scheme on Location Based Services

Eleazar Aguirre Anaya[1], Gina Gallegos Garcia[1], Miriam Barboza García[2],
Moisés Salinas Rosales[1], Gualberto Aguilar Torres[3], Ponciano J. Escamilla Ambrosio[1]

[1] Instituto Politécnico Nacional,
Centro de Investigación en Computación,
Mexico

[2] Instituto Politécnico Nacional,
Escuela Superior de Ingeniería Mecánica y Eléctrica,
Mexico

[3] Comisión Nacional de Seguridad,
Mexico

{eaguirre, msalinasr}@cic.ipn.mx, ggallegosg@ipn.mx, miriam.barbozag@gmail.com,
autg79y@yahoo.com, pjorgeea@googlemail.com

Abstract. Anonymity and privacy are two security services frequently confused when schemes are designed. On the one hand, privacy refers to transform information in order to keep it from all but those who are authorized to have it. On the other hand, anonymity refers to a condition in which the information receiver does not know the sender's identity. From the Location Based Service (LBS) point of view, anonymity and privacy are security services very important to preserve, as sensitive data travel in a service request, for example the identity of participants and their location. Most of the related work focuses on protecting only one aspect of the LBS user letting secure only one aspect. in this paper we present a security scheme that consists on a set of cryptographic protocols which consider cryptographic primitives along with fake location information, in order to provide both identity anonymity and location privacy. The importance of this work relies on the fact that the proposed scheme remains transparent to the LBS provider. Moreover, the results obtained show that this approach focused on removing the trust from the LBS provider, did not represent an excessive increment on the cost and usage of the channel that makes our scheme a suitable and interesting improvement over previous works.

Keywords. Anonymity, cryptography, location based services, privacy, scheme.

1 Introduction

Along with the widespread use and proliferation of Location Based Services (LBSs), came the concern on protecting personal information of LBSs users. The personal information in a request to that kind of services includes at least the user's identity and position. If information is traveling in an insecure channel, it can be compromised by either the LBS provider or when it is stored on any of the servers the LBS provider uses. In other words, if we assume a non-trust relation with the LBS provider, any entity that obtains the user request could misuse personal information included on that request.

Protecting the privacy and anonymity in the context of LBS's generally sums up in protecting personal information of the LBS's user that is shared along with the request, such as: the identity of the user and/or some identifier linked with the identity of the user, and the position of the user.

Most of the related work focuses on protecting only one aspect of the LBS user, the identity or the position of the user. However, if it is desired to ensure that the request is truly anonymous and private, both aspects should be protected. In this work, we present a scheme that preserves user's

privacy and anonymity, by using three cryptographic protocols. The main contributions of such scheme can be seen from two lines, in the first one, it protects the most important aspects concerning LBS's security by anonymizing the identity and encrypting position of LBSs users, whereas most proposals focus on protecting only one of them. The second contribution is that the scheme remains transparent to the LBS provider by not requiring additional changes on it, because it is assumed that the LBS provider is not a trusted entity.

The remaining of the paper is organized as follows. The section named Materials and Methods gives a brief introduction of Location Based Services and its security services, it also presents a review of anonymity and privacy security services from the location based point of view. Moreover, this work presents a review of the recent proposals addressing anonymity and privacy in such kind of services. After that, details proposed scheme by describing the three designed cryptographic protocols as part of our scheme. A cost-based analysis of the scheme from the communication channel usage perspective is presented in this section together with a security analysis. In the Results and Discussion section, some ideas and interpretations of the observed results are presented. After that, conclusions for this work are given.

2 Security Services on Location Based Services

As stated in [1] Location Based Services (LBS) can be defined as services that integrate a mobile device's location or position with other information in order to provide an added value to a user. There exist many types of LBS that try to construct an anonymity scheme, designing one which fits all of them, would be an exhaustive task, therefore, privacy and anonymity are two security services that should be considered very carefully.

Privacy in LBS has become a critical security service, because there are many ways in which an attacker can intercept the data in a request. This fact can end up revealing more sensitive information of the LBS user, such as personal beliefs or patterns of life, by combining the data in the request with some other background knowledge. An attacker in LBS can be anyone with malicious intents, who can intercept the communication between the mobile device and the LBS provider or can access stored data at the communication endpoints.

Attackers can be classified according to the knowledge they possess to help them infer private information of an LBS user [2]. This classification can be made in two dimensions, namely temporal information and context information. In addition to that, in order to protect from the different kind of attacks in LBS, there are three different protection approaches: identity protection, location protection and anonymity protection.

2.1 Identity Protection

One possible protection goal to ensure privacy of a LBS user is to hide the user identity while his position can be revealed. Identification information can be for instance the name of the user, his mobile phone number, a unique identifier or any static attribute that uniquely identifies the user. It should be remarked that even when the user hides his identity, an attacker could still be successful in deriving the user's identity by analysing his position and additional context information [3].

2.2 Location Protection

Beresford and Stajano in [4], defined location privacy as the ability to prevent other parties from learning one's current or past location. Duckham and Kulik in [5], refined the concept by defining it as a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others. Furthermore, according to [6], privacy protection in LBS is concerned with the hiding of the exact location of the user making a query.

2.3 Anonymity

Pseudo anonymity was the first obvious approach to provide anonymity by replacing the real identifier of the user by an untraceable ID. However, privacy researchers have shown ways to break the

untraceable characteristic of the ID, exposing the location of the user [4, 6, 7].

Since then, new anonymity solutions in LBS have been proposed, most of them developed under the definition proposed in [8], which is stated as being not identifiable within a set of subjects named the anonymity set.

Based on the definition of anonymity given in [9], two kinds of anonymity approaches can be distinguished: Identity Anonymity and Location Anonymity. The first one is given when the identity of the subject cannot be distinguished from k−1 identities corresponding to other LBSs' users. In the second one, the location of an LBS user cannot be distinguished from k − 1 locations of other LBSs' users.

3 Privacy and Anonymity Security Services on Location Based Services

From the security point of view, solutions that provide privacy through the anonymity approach in LBS can be classified in those solutions based on a cryptographic approach and those ones that do not make use of any cryptographic approach. The cryptographic approach considers blind signatures, mixnets, oblivious transfers and private information retrieval. Those one that do not make use of any cryptographic approach use spatial cloaking and fake location information. The related works considering the cryptographic approach are presented in the next section.

3.1 Cryptographic Approach

In 1982, David Chaum introduced blind signatures. They allow a message to be signed by an entity normally called the signer, without that entity knowing the content of the message [10]. The most relevant solutions, which use blind signatures or a combination of blind signatures with other cryptographic primitives, can be found in [11-18]. The basic idea behind such cryptographic constructions is to use the blind signature to generate an authorized anonymous message and its respective signature. After that, it is possible to find the real digital signature.

From the network communications perspective, a mixnet can be defined as a multistage construction that uses cryptographic permutations to achieve anonymity [19]. The main component of a mixnet is the stage, which performs mixing operations, also known as the mix, such as: encryption, decryption and permutations. All of them consider a batch of inputs.

In LBS, there is a reduced set of solutions that have been developed, mainly because the mixes used introduce high latency into the system, so special modifications have to be done to the architecture of the mixnet system in order to be applied in a practical way inside LBS's. Examples of anonymous systems at the network layer can be found in [20, 21]. Moreover, solutions based on the application layer can be found in [22, 23].

Oblivious Transfer (OT) protocols allow one party called the sender, to transmit part of its inputs to another part called the receiver, in such a way that both parties are protected. The sender is assured that the receiver does not receive more information than its entitled, and the receiver is assured that the sender does not know which part of the input it received [23]. There are variants of OT constructions, which can be applied to protect privacy in LBS systems such as: Adaptive OT, Dynamic OT and Proxy OT. Example OT solutions that can be applied within the LBSs context are presented in [24, 25].

Other common cryptographic construction to preserve privacy in LBS is the Private Information Retrieval (PIR). The basic idea is that a user of LBSs can retrieve information from the LBS provider, without the provider knowing what particular information the user has requested. PIR-based solutions are the first to provide perfect privacy and are not vulnerable to context information attacks. This is because location information is not revealed at any moment. Some of the most relevant works in this construction are presented in [26-28]. The PIR approach proposes that no trusted Third Party is necessary to enable these solutions to work.

3.2 Non-Cryptographic Approach

In some cases, solutions that use a cryptographic approach are not the first choice when trying to provide privacy to the LBS's user. This is because

of the computational power needed to deploy them.

In those cases, the approaches presented in this section are spatial cloaking and fake location information.

Spatial cloaking solutions represent the most common used technique for protecting privacy in LBS.

The basic idea is that the user's exact location can be blurred into a cloaking area that satisfies a degree of anonymity, given by a metric or specified by the user.

The set of solutions can be further classified by the architectural approach they use centralized trust third party and peer to peer architecture solutions. For the first set, the most important works can be found in [29-33]. In these solutions, a trusted server, named the anonymizer, is responsible of hiding the user's exact location into the cloaked area, which satisfies the privacy requirements defined by the user and then sending the query to the service provider. A variation of the explained cloaking solution is presented in [34], where instead of sending a cloaking region to the LBS provider, a substituted position representing the cloaking region is chosen and sent to the user.

The main idea of peer to peer architecture solutions is presented in [35-38]. In these works, the functionality shows that a set of mobile devices agrees with each other in order to produce the cloaking region. A representative mobile device of the peer-to-peer system built is chosen in order to send the anonymized query to the LBS provider. A new approach to the techniques shown so far is the one presented in [39]. In this work the authors propose taking advantage of the Cloud Computing and replace the Trusted Third Party anonymizer by a cloud-based server. This cloud-based server is capable of computing the cloaking region but is not trusted by the users.

Most of the described solutions use the independent architecture approach in order to hide the user's real location among other fake locations generated by the mobile device, which tries to issue the request. The basic dummy technique is presented in [40] and consists in an LBS user sending its true position along with several false positions to the LBS Provider, which creates a reply message to all position data received. Once the LBS user receives all the responses, it simply extracts the response, which corresponds to its true position.

In addition to that, different proposals based on this approach are presented in [37, 38, 41, 42].

3.3 Cryptographic and Non-Cryptographic Approach

In order to take advantage of the best characteristics of the previous approaches, a hybrid approach can be found.

While the cryptographic approach fits into providing identity anonymity, the non-cryptographic approach fits into providing position privacy to the LBS's users.

Another special categorization could be made based on how the solutions are presented such as algorithms, frameworks, architectures, controls and schemes. Proposals based on that categorization are described in [43, 44].

4 Proposed Anonymity Scheme

Our anonymity scheme considers Identity Anonymity and Location Anonymity as a way to benefit and protect the most sensitive data of an LBS request. It was designed to be a billing service for those LBS users that wish to anonymize their request to LBSs. In other words, the anonymity scheme was designed for those LBSs, which require identity information, and need only a location point to provide the service.

The proposed scheme can be subdivided into a set of cryptographic protocols: identity anonymity, position anonymity and privacy of the response protocol. All of them are developed by different entities that are described below.

4.1 Architecture of the Proposed Anonymity Scheme

The architecture of the anonymity scheme consists mainly in five entities. The Centralized Trusted Third party approach is used as a way to minimize the workload that the mobile device has to do in order to perform the Anonymization of the requests made to a LBS Provider. Another important factor, which was considered when choosing the participating entities, was the fact that the LBS

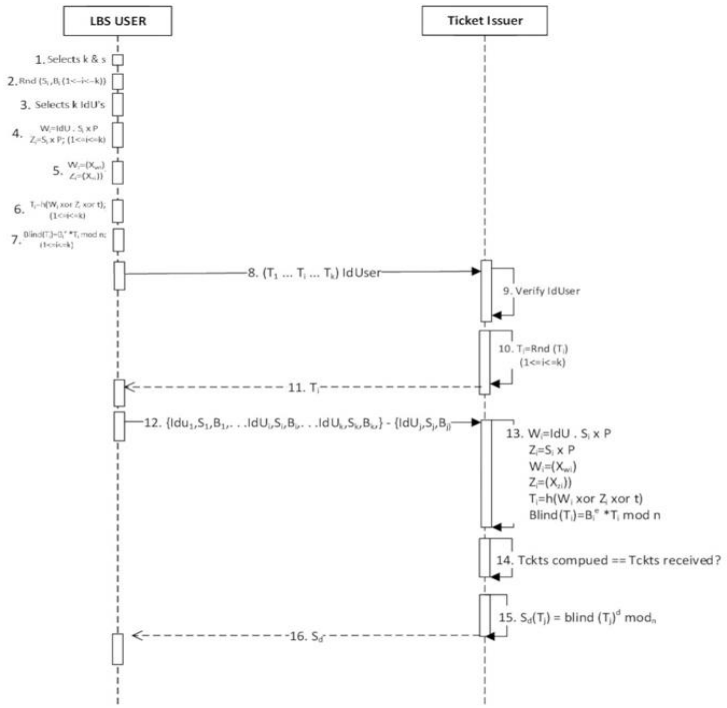

Fig. 1. Identity anonymity cryptographic protocol

Provider is not a trusted entity; therefore, intermediate trusted entities must provide the Anonymity Service.

The entities, which participate on the anonymity scheme, can be roughly divided into three types of entities: LBS users, Trusted Third Party Servers and LBS Providers.

4.2 Identity Anonymity in the Proposed Anonymity Scheme

Two main building blocks are used to design the cryptographic protocol that is focused on anonymizing the identity of the user. The first building block is referred to as 'dummies identifiers' which is considered to conceal the real identifier used to access the LBS.

The second block is referred to as the 'blind signature primitive', used to construct an anonymous ticket to be able to anonymize the position of the user. This ticket hides the real user identifier employed to access the LBS.

With a given value *k*, provided by the user of the anonymity service, a set of valid identifiers different from the real's user identifiers used to access the LBS, are selected.

From these selected identifiers the anonymous tickets are constructed based on [16], which besides using the blind signature primitive, uses the Elliptic Curve Discrete Logarithm Problem (ECDLP) [45] to hide the identifier of the LBS user, where the ECDLP deals with finding an integer $d \in [0, n-1]$ such that $Q = dP$ where P and $Q \in E(K)$. In this case, d represents the identifier of the user.

4.3 Position Anonymity in Proposed Anonymity Scheme

In order to anonymize the real position of a LBS user, we consider a building block that produces *k-1* false positions using a square grid of area s. Such real position is hidden on a vertex of the square grid. In it, only the trusted server (Position Anonymizer), which produces the false positions,

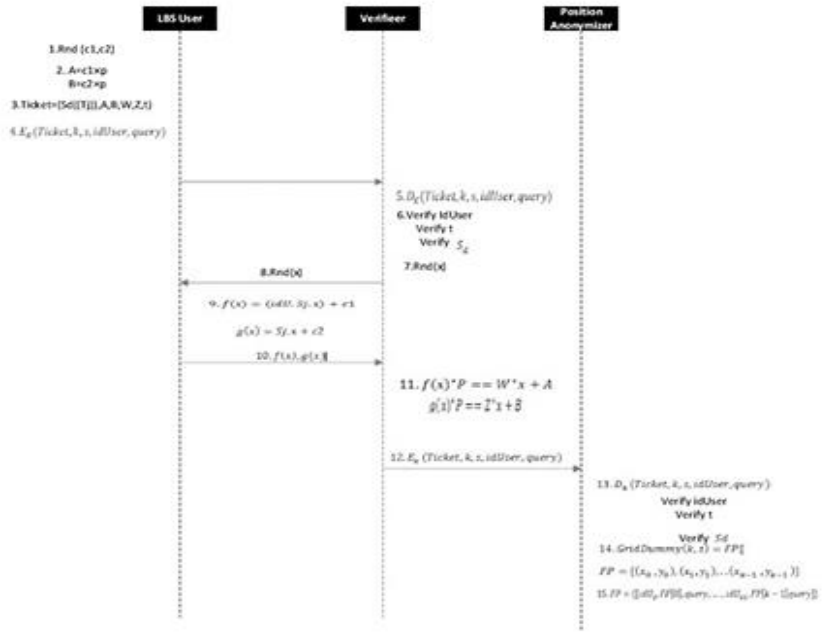

Fig. 2. Position anonymity cryptographic protocol

is the one that knows in which vertex of the square grid the real position of the user is located.

Once the false positions are produced, the Position Anonymizer proceeds on constructing the requests, which are to be sent to the LBS Provider.

4.4 Privacy of the Response in the Proposed Anonymity Scheme

After responses are received from the LBS Provider, the entity that is responsible of sending the requests must select the response, which corresponds to the real position of the LBS user. Once the correct response is selected, the privacy of the response must be protected as it contains probable places where the LBS user can be found at some time, thus this response can end up de-anonymizing the LBS user.

The main block, which is considered to protect the service response as it travels to the LBS user, is the encryption of it. Also, the verification of the authenticity of the response by a digital signature is a block used, before delivering the final response to the LBS user.

4.5 Cryptographic Protocols in our Anonymity Scheme

As we mentioned, the proposed scheme is formed by three cryptographic protocols: The Identity Anonymity, Position Anonymity and Confidentiality of the Response Subservice. Additionally, a Setup Protocol is used to make the necessary arrangements for the other protocols to work appropriately. It consists on the agreement on an elliptic curve defined over a finite field K, the generation and load of two asymmetric key pairs for signing messages.

Identity anonymity cryptographic protocol. It is shown in Figure 1 (based on [19]). It works as follows. The LBS user selects two parameters: *k* and *s*. *k* defines how many tickets will be computed (among how many users, the identity of the user will be anonymized) and *s* defines the area that will be used to anonymize the position of the LBS user

(this parameter is used by Position Anonymity Protocol). The LSB also generates two random numbers *S* and *B*.

For each ticket produced by $\mathrm{S_i}, \mathrm{B_i}\,; 1 \leq \mathrm{i} \leq \mathrm{k}$. These random numbers must be kept secret. Then, K random dummies identifiers *(IdU)* are selected. Such identifiers will be hidden on the point *P* considering the selected elliptic curve during the Setup Protocol. For each dummy identifier $(1 \leq \mathrm{i} \leq \mathrm{k})$, the points W_i and Z_i are computed according to $W_i = IdU \cdot S_i \times P = (x_{wi}, y_{wi})$ and $Z_i = S_i \times P = (\mathrm{x_{zi}}, \mathrm{y_{zi}})$. From these *Y*-coordinates of the points W_i and Z_i with $(1 \leq i \leq k)$, are discarded becoming $W_i = (x_{wi})$ and $Z_i = (x_{zi})$. Using the points W_i, Z_i and a time stamp, partial tickets T_i are obtained from a hash function, $T_i = h(W_i \oplus Z_i \oplus t)$ with $(1 \leq i \leq k)$. Considering the random numbers Bi previously generated, computed tickets are blinded using a blinding factor and the signer's public key (n, e), according to *Blind* $(T_i) = {B_i}^e \cdot T_i \, mod \, n$.

The set of produced blind tickets T_i $(1 \leq \mathrm{i} \leq \mathrm{k})$ is sent to the Ticket Issuer, along with an identifier *(IdUser)*, which links the *LBS* User with the anonymity service. When the ticket issuer receives the mentioned tickets and identifiers, he proceeds to verify that the identifier is registered to request the anonymity service. From the received set of tickets, the ticket issuer randomly chooses one ticket to be blindly signed denoted by (T_j). The Ticket Issuer informs the Mobile Device which ticket was selected. He replies by sending the necessary parameters to compute the rest of the tickets, which will not be signed. For each ticket $\{\mathrm{T_1}, \mathrm{T_2}, \ldots, \mathrm{T_K}\} - \{\mathrm{T_j}\}$, the hidden dummies identifiers, and the random numbers generated, in the beginning, are needed. Once the Ticket Issuer receives the parameters, he computes the partial tickets the same way the mobile devices did. Then, the Ticket Issuer compares the partial tickets previously computed against the ones he received before. If true, he signs the Tj ticket with its private key (d), $S_d(T_j) = blind(T_j)^d \, modn.$ Finally, the Ticket Issuer returns the signed ticket to the LBS User.

Position anonymity cryptographic protocol. This protocol is an extension of the Identity Anonymity Protocol, where the LBS user selected the parameters *k* and *s*. In this protocol, *k* stands for the number of dummies positions that are produced, among which the real position of the user will be indistinguishable, *s* stands for the area where the real position of the user will be hidden. In it, once the LBS user has signed the partial ticket obtained in the Identity anonymity protocol, he will proceed on constructing the service request, which includes his real position, the parameters selected to anonymize his position, and the complete ticket which will grant him access to use the controls to anonymize his position i.e. the Position Anonymity Protocol.

It works as follows: The LBS user produces two random numbers *c1* and *c2*. Then, computes points A and B on the selected elliptic curve, with $A = c1 \; X \; P$ and $B = c2 \; X \; P$. In addition to that, constructs the complete ticket by concatenating the signed partial ticket, the previously computed points on the elliptic curve and a time stamp. It is made by considering $Ticket = (S_d(T_j), A, B, W, Z, t)$. Finally, the LBS user sends the verifier the Ticket along with his position, the anonymity parameters (k and s), the query to the LBS and a user identifier, which is registered at the Verifier in order to provide the anonymity service *(IdUser)*. All of these data are encrypted with a secret key. Once the Verifier receives the request, he proceeds on decrypting the data by doing the following.

He checks that: The user identifier effectively has access to the Anonymity Service, that the time stamp of the request is still valid and that the blind signature on the ticket. After that, and only if the validations are correct, the verifier selects a random number x, which will be a challenge for the LBS User. He also sends the challenge to the LBS User. The LBS User receives the challenge x and computes the response to the challenge with $f(x) = (IdU_j \, . S_j \, . x) + c1$ and $g(x) = S_j \, . x + c2$. The LBS sends the response to the challenge to the Verifier. The verifier checks that the computed responses to the challenges are correct with $f(x) \; X \; P == W \, . x + A$ and $g(x) X \; P == Z \, . x + B$. If true, the verifier sends the original encrypted request; he received form the LBS User, to the Position Anonymizer.

The Position Anonymizer receives the request, decrypts it and validates if: Is the received identifier registered to receive the anonymity service? Is the

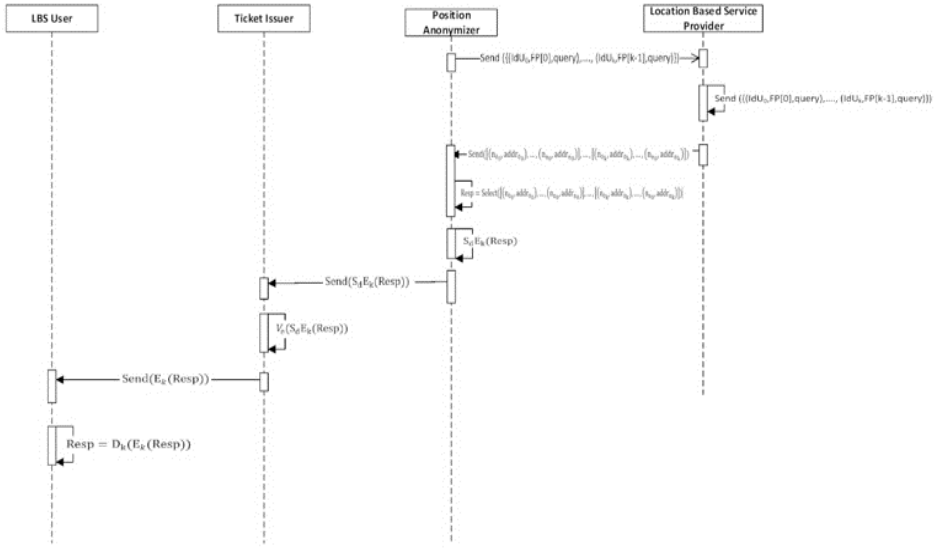

Fig. 3. Response cryptographic protocol

signature on the anonymous ticket valid? And if is the time stamp on the ticket still valid?

After that and once all the validation process turned out correct, the Position Anonymizer proceeds on producing the false positions using the GridDummy algorithm proposed at [37]. With the false positions produced, the Position Anonymizer constructs the service requests that have to be sent to the LBS Provider. It is made by concatenating a false identifier, one of the positions produced previously and the service request he received from the verifier. Among this set of false requests, the real request of the user is never known. The Position Anonymity protocol described above is presented in Figure 2.

Response cryptographic protocol: The response cryptographic protocol, aims at protecting the privacy of the response from the query made by the LBS User. It is important to notice that this protocol does not ensure the anonymity of entity that produced the response, but protects it from possible eavesdroppers of the communication between the mentioned entities, in such a way that if the mentioned response gives out some private information of the LBSs users it will not be exposed.

The protocol has as a starting point the set of queries constructed by the Position Anonymizer on the Position Anonymity Protocol and is presented in Figure 3. It works as follows:

The Position Anonymizer sends the set of request constructed to the LBS Provider according to:

$$Send\begin{pmatrix}\{(IdU_0, FP[0], query), \ldots..,\\ (IdU_k, FP[k-1], query)\end{pmatrix}\}.$$

The LBS Provider receives the set of requests and computes the responses to each one of them as:

$$Comp(\{(IdU_0, FP[0], query), \ldots..,\\ (IdU_k, FP[k-1], query)\}).$$

The LBS Provider sends each one of the responses to the Position Anonymizer as soon as he obtains the response, as follows:

$$Send([(n_{0_0}, addr_{0_0}), \quad \ldots,\\ (n_{n_0}, addr_{n_0})], \ [(n_{0_k}, addr_{0_k}), \ldots, (n_{n_0}, addr_{n_k})]),$$

with $(0 \leq n \leq 60)$. The Position Anonymizer receives the responses, and discards, the ones that do not correspond to the real position of the LBS User with:

$$Resp = Select([(n_{0_0}, addr_{0_0}), \ldots, (n_{n_0}, addr_{n_0})], \ldots,\\ [(n_{0_k}, addr_{0_k}), \ldots, (n_{n_0}, addr_{n_k})]),$$

where $(0 \leq n \leq 60)$.

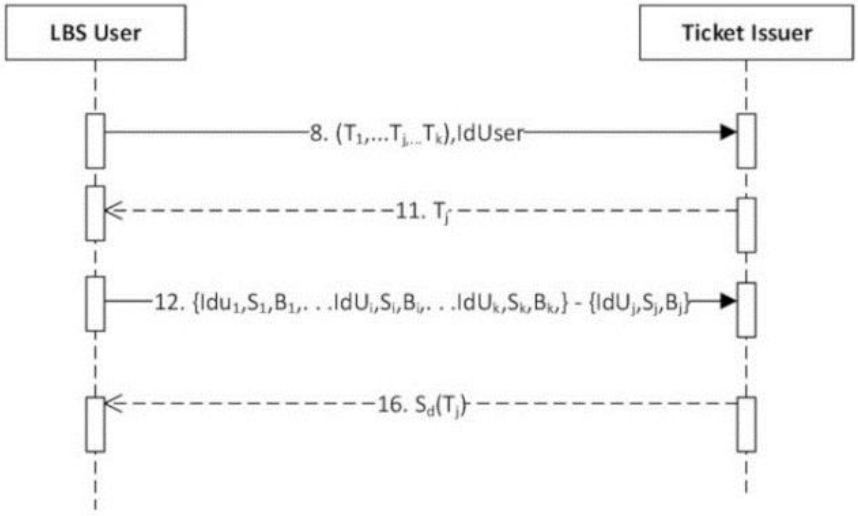

Fig. 4. Considered messages in the evaluation of the identity anonymity protocol

The Position Anonymizer encrypts the response with the pre-shared symmetric key and signs it with his private key, $Signed\ response = S_d E_k(Resp)$. After that he sends it to the Ticket Issuer. The Ticket Issuer receives the response and verifies the signature on it with the Public Key form the Position Anonymizer, $V_e = (S_d E_k(Resp))$.

The ticket Issuer sends the encrypted response to the LBS User who made the original query. The LBS User receives the encrypted response and decrypts it with the symmetric key with $Resp = D_k(E_k(Resp))$.

5 Evaluation of the Proposed Scheme

Once the proposed anonymity scheme was described, this section discusses its evaluation in terms of the amount of data exchanged trough the communication channel, considering a set of parameters defined for testing purposes and a proof of concept software implementation.

The evaluation of efficiency and performance of the proof of concept implementation developed for the Anonymity Scheme is expected to show that the proposed protocols do not depend only on the proposed designs, but depend on other factors too, like how the implementation is done.

5.1 Setting the Testing Environment

Equipment used: The architecture for the anonymity scheme mainly consists of 5 entities. Therefore, a selection of the equipment to represent each one of these entities was made. The entity of the mobile device, which is controlled by a LBS User, was represented by a Tablet ASUS MEMO Pad HD7, OS Android, Quad Core, 1.2 GHz, 1 GB RAM, 16 GB SSD. The Trusted Third Party Entities, which take part on the protocols to anonymize the identity and position of the LBS User, as well as in the protection of the service response, are all represented by a Mac Book Air, OS X Yosemite, 1.8 GHz core i5, 4 GB RAM, 128 GB HDD.

Networking settings for connection with the Trusted Third Party Servers: A TCP connection was preferred over an UDP connection due to the fact that a reliable connection with no data loss was a necessary requirement for the scheme to be correctly deployed. Moreover, fixed TCP ports were assigned to each Trusted Third Party in order to represent the communication between entities. The ports that start the communication with the fixed ports were dynamically assigned by the OS: Ticket issuer receives requests on 4444, verifier receives requests on 4040, and position anonymizer receives requests on 4446. The

service response ticket issuer waits the response on port 3333 and the mobile device keeps the connection open on the dynamically assigned port by the Operating System.

5.2 Used Software

LBS Provider: The target LBS Provider chosen to do the tests was the API offered by Google, called Google Places. It performs a nearby places search, which is a type of LBS that complies with the characteristics of the proposed Anonymity Scheme.

The request to the LBS is an https request with the following format: https://maps.googleapis.com/maps/api/place/nearbysearch/output?parameters. In order to be able to perform a request, a key needs to be assigned to each user, which links the user to his email address, therefore it is considered as the identity information of the LBS user. Additionally, to the access key, the following parameters are needed to make the request: (i) User location, given by the latitude and altitude coordinates of the mobile device. (ii) Radius definition, which defines the distance in meters where to perform the search and (iii) Types of places to return (i.e. restaurants, cinemas, schools, or other places of interest).

By default, the search returns 20 responses. In case that there exist more than 20 places in the response, an additional key is needed and included on the response to the query, then the user would have to construct the additional request. At most 60 results are returned, meaning that at most 3 requests can be made to the LBS Service. It is important to mention that the format in which the results were returned was chosen to be of the JSON type, because this is the one recommended in the Google Places API Documentation.

Mobile Device and Trusted Third Parties: The implementation of the scheme formed by our three cryptographic protocols, which were deployed on the mobile device, the ticket issuer, the verifier and the position anonymizer, was made on the Java Programming Language. The choice of the programming language was based on the fact that the hand-held device performing the role of the mobile device was assumed to run the Android Operating System, and Java is the official language for Android Development.

In order to perform the cryptographic operations needed on the protocols, such as the elliptic curve point multiplication, digital signatures, blind signatures, hash values computations, encryption and decryption of messages, two cryptographic providers were used: Bouncy Castle and Spongy Castle (the Android Version), and the SunJCE Provider.

The messages exchanged between entities were formatted with JSON, in order to have an easy parsing of the transmitted data.

5.2 Scheme Parameters

First of all, the entities participating on the Anonymity Scheme have to know the IP addresses and TCP ports, they will be communicating with, as follows: (i) The Mobile Device has to know the IP address and correspondent TCP ports of the Ticket Issuer and Verifier, (ii) The Verifier has to know the IP address and TCP port assigned to the Position Anonymizer, (iii) The Position Anonymizer has to know the IP address and TCP port assigned to receive the response at the Ticket Issuer.

Secondly, there must be an agreement on the elliptic curve to be used for computing the blind tickets. The Mobile Device, the Ticket Issuer and the Verifier must select one of the following curves: P256, P521, B233, B409. Once the elliptic curve is selected, a minimum of 9 access tokens for LBS must be loaded at the Mobile Device and the Position Anonymizer (as 9 is the minimum number of tickets to be produced). Additionally, the keys needed to sign/verify and encrypt/decrypt must be generated and loaded on each correspondent entity.

5.3 Other Definitions for the Evaluation

Based on the deployed implementation, some information about the data units (segments) that are exchanged between the entities participating on the implementation of each one of the protocols was collected. The data units, which travel at the transport level of the TCP/IP model, represent the process-to-process communication between hosts interconnected by a communication network, in our case a LAN network.

Table 1. Types of data units correspond to different elliptic curve

K Elliptic Curve	CE	Data	Control	T
9-P256	3	16	35	54
9-P521	3	19	21	43
9-B233	3	22	19	44
9-B409	3	20	18	41
25-P256	3	46	36	85
25-P521	3	43	41	87
25-B233	3	48	35	86
25-B409	3	46	33	82
64-P256	3	109	77	189
64-P521	3	110	79	192
64-B233	3	110	76	189
64-B409	3	108	81	192

Table 2. Total number of data units that were exchanged on the implementation of anonymity position protocol

K-Elliptic Curve	CE	Data	Control	CT	T
9-P256	6	17	19	8	50
9-P521	6	22	16	8	52
9-B233	6	12	24	8	50
9-B409	6	19	19	8	52
25-P256	6	18	18	8	50
25-P521	6	19	19	8	52
25-B233	6	18	18	8	50
25-B409	6	19	19	8	52
64-P256	6	18	21	8	53
64-P521	6	19	19	8	52
64-B233	6	18	18	8	50
64-B409	6	19	21	8	54

For this test bed, two protocols data units were considered: TCP segments and TLS segments (used on the requests to the LBS Provider). The proof of concept was divided in such a way that the data units exchanged in each protocol could be counted. The parameters, which were used in order to run the different tests, are: (i) The number of tickets to be produced or number of individuals from which the LBS wants to be anonymized, denoted by k, (ii).

The elliptic curve, which was used to produce the anonymous ticket, and which is also verified at the Verifier and Position Anonymizer.

The selection of the parameters was based on the idea that the parameter k is used in two of the three protocols, which integrate the Anonymity Scheme: Identity Anonymity Protocol and Service Response Protocol.

The selected Elliptic Curve is used in two of the three protocols: Identity Anonymity Protocol and

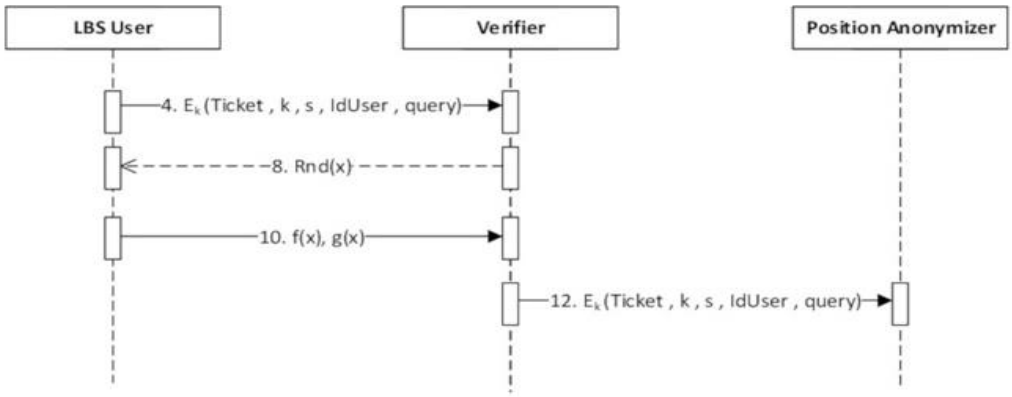

Fig. 5. Four exchanged messages considered for the evaluation of the position anonymity protocol

Position Anonymity Protocol. Therefore, a total of 12 tests for each protocol were run considering the combination between k (9, 25, or 64) and the elliptic curve (P256, P521, B233, or B409). In order to be able to perform the counting of messages, the traffic between the entities was captured and analyzed using the Wireshark Tool.

Moreover, for a TCP connection, different types of data units were counted: (1) Streams in which the connection establishment is performed, (2) Streams in which the connection termination is achieved, (3) Streams which contain the data that were meant to be sent, (4) Other types of streams such as flow control data, congestion information, error messages, retransmission of lost segments and acknowledgments without data.

5.5 Evaluation of the Identity Anonymity Protocol

For the Identity Anonymity Protocol, the messages shown in Figure 4 were considered, in order to compare them with the number of protocol data units exchanged on the implementation of this specific protocol.

In order to count the data units, which correspond to the Identity Anonymity Protocol, a TCP connection established between the LBS User and the Ticket Issuer listening at port 444 was considered. The connection termination segments were not considered on the total count as the connection finishes at the Service Response Protocol, when the LBS User receives the final response from the Ticket Issuer.

In Table 1, the different types of data units that correspond to the mentioned classification are shown as well as the total data units in each connection. In such Table, CE means connection establishment, CT means connection termination an T means total data units.

As far as observed, the maximum number of data units exchanged between the Mobile Device and the Ticket Issuer is 192, compared to 4 messages exchanged on the protocol shown in Figure 5.

5.6 Evaluation of the Identity Anonymity Protocol

The Position Anonymity Protocol exchanges 4 messages as shown in Figure 5. In order to count the number of data units exchanged on the implementation of the Position Anonymity Protocol, two TCP connections were considered:

1. LBS User connection with the Verifier, listening at port TCP 4040.
2. Verifier connection with the Position Anonymizer, listening at port TCP 4446.

The total number of data units (considering both TCP connections), which were exchanged on the implementation of this protocol are shown in Table 2. In this Table, CE means connection

Table 3. Total number of data units exchanged on the implementation of the response cryptographic protocol

K-Curve	TLS H	TLS A	TLS AD	CE	TCP D	TCP C	TCP CT	T
9-P256	47	11	166	36	8	241	52	561
9-P521	47	11	178	36	9	239	52	572
9-B233	47	11	161	36	9	229	52	545
9-B409	47	11	160	36	8	231	52	545
25-P256	111	27	487	84	8	625	116	1458
25-P521	111	27	478	84	7	632	116	1455
25-B233	111	27	492	84	10	666	116	1506
25-B409	111	27	493	84	8	604	116	1443
64-P256	270	66	1173	201	9	1473	272	3464
64-P521	270	66	1224	201	10	1546	272	3589
64-B233	270	66	1192	201	8	1467	272	3476
64-B409	270	66	1287	201	7	1522	272	3625

establishment, CT means connection termination, T means total data units.

The maximum number of data units exchanged on the Implementation of this second protocol is 54, against four messages, which are exchanged on the Protocol.

5.7 Evaluation of the Response Cryptographic Protocol Messages

The response cryptographic protocol consists of $2k + 2$ messages exchanged between the participating entities, as observed in Figure 6. In order to consider the total number of data units exchanged on the Implementation of the Service Response Protocol, a variable number of transport level connections were considered:

1. Transport level connections established between the Position Anonymizer and the LBS Provider. The number of connections depend on the number of requests made to the LBS Provider. It is important to say that the LBS User can choose the parameter k in this protocol. It represents the total number of requests that have to be made to the LBS Provider. It was found that for k = 9, a total of 11 TCP connections were made, these connections include the data units corresponding to the TLS Version 1.2 protocol built on top of the TCP Connection. For a k = 25, a total of 27 TCP connections were made, and for a k = 64, a total of 66 TCP connection.

2. One TCP connection between the Position Anonymizer and the Ticket Issuer that is listening at TCP port 3333.

3. Part of the TCP connection which was established between the LBS User and the Ticket Issuer on the Identity Anonymity Protocol Implementation, the data units which are counted here include only the data units corresponding to the response which the LBS receives and the correspondent TCP connection termination. It is important to say that the TLS data units, which were counted as part of the exchanged data on the protocol implementation, are divided into 3 types of data units: TLS Handshake data units, which include the change cipher spec data units, TLS Alert Data Units and TLS Application Data. The total number of data units exchanged on the Implementation of the Response cryptographic protocol, considering all the messages exchanged, according to Figure 6, can be seen in Table 3, where TLS H means Transport Layer Security handshake, TLS A means Transport Layer Security alert, TLS AD means Transport Layer Security application data, CE is connection establishment, TCP Data means transmission control protocol (data), TCP

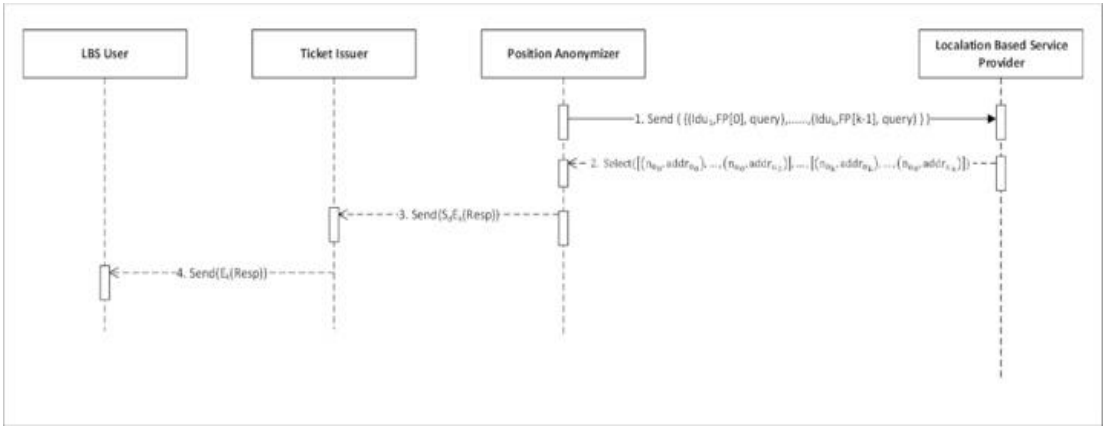

Fig. 6. Messages exchanged between the participating entities in the response cryptographic protocol

control is transmission control protocol (control), TCP CT means transmission control protocol (connection termination) and T means total data units.

As observed in Table 3, the maximum number of exchanged data units in the Implementation of the Response cryptographic protocol, is 3625 against $2k + 2 = 2(64) + 2 = 130$ messages from the protocol.

6 Results of the Evaluation of the Proposed Scheme

Regarding the parameter k, the obvious hypothesis is to say that the smaller the value, the less number of total data units are to be produced, consequently the results turned out to prove such hypothesis; however, considering that k is a parameter which represents the degree of anonymity that the LBS User will have, it keeps up to the user itself to decide which number of dummies are to be used to make it indistinguishable.

Even though, the obtained results did not give any clear recommendation of the scheme's parameters in order to minimize network traffic by producing the minimum number of data units; if such kind of suggestion has to be made, then the recommendation would be to choose the binary curve B-409 in combination with a value $k = 25$.

Hence, B-409 has turned out to be the curve, which produced the minimum number of exchanged data units in two of the three protocols.

However, the value $k = 25$ could be considered as a good balance between the degree of anonymity wanting to be achieved and the total data units exchanged on the protocols.

Other important remarks regarding the total data units produced by the proof of concept implementation of the Anonymity Scheme turned out to be:

- The theoretical number of messages exchanged considered when designing a protocol turns out to be outnumbered by the real number of messages exchanged in an implementation.
- The real number of messages (PDU) exchanged between the entities of an architecture depends on many factors like: the encoding used, the kind of connection desired (reliable or not reliable), as well as clearness on the network which can lead to the need of retransmitting data units if a reliable connection was chosen.

The selection of an architectural approach involving Trusted Third Parties and dummy locations instead of using Spatial Regions in order to provide Anonymity let us manage the level of privacy of the LBS user even considering possible raises of the communication costs.

In this sense, even the expected results show that communication costs would rise above most of the proposed solutions, the resulting number of

messages exchanged between the entities participating in the proposed anonymity scheme ends up being considerable higher than the combination of protocols with the minimum number of messages (lower communication cost), but not higher than the combination of protocols with the maximum number of messages, which leads us to enunciate that: A trusted relation with the LBS Provider is not a necessary condition to provide anonymity and maintain the communication costs in a reasonable margin.

7 Security Analysis of the Proposed Anonymity Scheme

The identity and position anonymity protocols were designed in such a way that each Trusted Third Party Server only know part of the sensitive data to be anonymized (the identity or the position). In our scheme, the ticket issuer (first Trusted Third Party Server) did not learn any information of the user (nor his identity or his position). Additionally, even though the verifier and position anonymizer do know the position of the user, they do not keep records of the requests received that could lead them to perform a correlation attack. Lastly, it is important to mention that besides the controls used to guarantee the anonymity of the LBS Users, a trust relation is assumed between the Trusted Servers and the LBS User, this could be easily achieved by a confidentially Agreement between the LBS User and the Provider of the Anonymity Service.

Finally, the security analysis is done by describing the resistance to single request attacks, which were considered when designing the Anonymity Scheme.

It is important to notice that a Service request, in the context of this investigation, is composed of a set of *k-queries* made to the LBS Provider, which include the real position of the user. This set of requests can be linked to one IP address (the Position Anonymizer IP address).

Each of the *k-queries* include: User identifier or token used to access the LBS, location associated with the LBS User (latitude and longitude coordinates, radius, defines the distance (in meters) within which to return the response and type which restricts the results to places from the specified type.

A service request can be represented as an array of the afore-mentioned values:

$$[((token_0),(x_0,y_0),radius,type),\ldots,](token_k),((x_k,y_k),radius,type),$$

for a set of defined attacks, the possible adversaries and the power they have and the information they possess is mentioned as follows. Also, the theorem, which enunciates the resistance to the attack, and its resistance proof is presented. The single request attacks that are analysed are centre of K-ASR attack, abnormal points attack, colluding attack and inference attack.

7.1 Centre of K-ASR Attack

The scope of this attack is to produce an anonymizing spatial region enclosing *k-users* within it. It consists on the real position of the user being easily revealed as it tends to be found in the center of the spatial region [46,47]. Even though the proposed anonymity scheme does not produce a region to be sent to the LBS Provider, the set of false positions produced along with the real position form a region itself, which represents the Spatial Region. As a consequence, the resistance against this attack can be proved. Possible adversaries are the LBS Provider or an eavesdropper between the Position Anonymizer and the LBS Provider. His power could be used with one service request from one LBS User.

Theorem: The proposed Anonymity Scheme is resistant to the center of K-ASR attack

Proof: It is assured that the false positions produced by the proposed scheme does not produce an area, which center has a large probability of being the real position of the user; this relies true because the true position of the user is attached to a grid vertex which is randomly chosen. As long as the random function, which is used to choose the vertex of the grid, remains secure, the scheme is proven to be resistant to the center of K-ASR attack.

7.2 Abnormal Points Attack

This attack is successful when an uneven distribution of the positions is used to construct a

spatial region or when the users are not distributed homogeneously in the spatial region [48]. Possible adversaries are the LBS provider or an eavesdropper between LBS Provider and position anonymizer. His power could be used with one service request from one LBS User.

Theorem: The proposed anonymity scheme is resistant to the abnormal points attack.

Proof: A scheme that produces a cloaking region or a spatial region containing a set of false positions including the real position of the user. It can give out the real position of the user if the real position of the user is isolated from the rest of positions. If the adversary tries to perform this attack to the proposed anonymity scheme, he first would need to reconstruct the area formed by the set of requests received in around the same time frame.

Once the area is constructed, if a position is isolated from the rest of positions, then probably that position is the real position of the user. The proposed anonymity scheme uses the Grid Dummy algorithm, which produces a set of false positions. These false positions are equally distributed in a grid along with the real position of the user. The distance between each pair of positions is given by the parameter g. This parameter determines the side length of each grid cell, therefore a position which is isolated from the other positions of the grid cannot be the output of the algorithm and as a consequence it cannot be a position sent to the LBS Provider. Based on that statement, it is concluded that the proposed scheme is resistant to the abnormal points attack.

7.3 Colluding Attack

A colluding attack consists on a set of users colluding with each other in order to obtain sensitive information of a target user (the identity or position of a LBS User). A scheme is said to be colluding attack resistant if user's information is independent from other users [49]. Possible adversaries are a set of colluding users authorized to use the anonymity scheme. His power is as follows: each colluding user has access to the scheme, meaning he can interact with the trusted third party entities, but cannot know exactly which false requests were made in his name (his service request). Answer to the service request each colluding user made. Theorem: The proposed Anonymity scheme is resistant to the colluding attack.

Proof: Each query made to the LBS provider contains locations and fake tokens (identifier of the LBS User) to access the LBS. The false locations and fake tokens have the same probability of being produced through the scheme meaning that the colluding users will have $1/k$ probability of guessing the identity or position of the target user (the same probability that an eavesdropper between the position anonymizer will get). Furthermore, due to the fact that the position anonymizer acts as a proxy between the real user and the LBS provider, the LBS provider cannot know which one was the real LBS's user that did the request.

If the colluding users make use of the scheme to try to figure out the real position or identity of the user, they will not get any information of the target user. This is because every set of positions and fake tokens produced are independent from previously generated data, every parameter used to anonymize the identity and position of the user is new on every execution of the scheme. Moreover, a pattern cannot be identified of how the fake positions or fake tokens are chosen, just by using the anonymity protocol in our proposed anonymity scheme. As the LBS user's information produced through the scheme is independent from other LBS users, a set of colluding LBS users cannot obtain information related to other LBS's user (the target user) just by using the anonymity service, thus it is concluded that the proposed anonymity scheme is colluding attack resistant.

7.4 Inference Attack

This attack consists on deducing sensitive information, which in this case is the real location or identity of the LBS's user from information publicly available [49]. The possible adversaries are the LBS provider or an eavesdropper between the LBS provider and the Position Anonymizer. The power of the adversary is one service request from a LBS's user.

Theorem: The proposed anonymity scheme is resistant to the inference attack.

Proof: A scheme is said to be inference attack resistant if all the LBS users that make queries to a LBS Provider have the same probability to be

targeted as the real user. A way to accomplish this is by satisfying the k-1 anonymity metric, where the LBS users have 1⁄*k* probability of being identified.

As the fake positions sent along with the real position of the user are produced with the Grid Dummy algorithm, which ensures that k-anonymity is achieved (all users on the spatial region have 1⁄*k* probability of being identified as the real LBS User); it is concluded that the proposed anonymity scheme is resistant to the inference attack.

The set of analyzed single request privacy attacks to LBS were chosen from the set of related works, which present their solution as a scheme. In Table 4, a comparison between the related works and the proposed scheme, regarding the resistance to privacy attacks, is presented.

8 Conclusions

A theoretical higher degree of privacy against single request attacks in LBS can be achieved by anonymizing the identity and the position of LBSs' users. By analyzing the theoretical resistance to single request attacks, it can be shown that the proposed anonymity scheme is resistant to all single request attacks shown on other related works. Even though the level of privacy chosen by the LBS' user is a small value (i.e. $k = 9$), the anonymity that the scheme offers guarantees that the LBS' user will be indistinguishable from that number of users, delimited by the parameter *k*. A trust-relation with an LBS Provider is not a necessary condition to provide LBSs' users privacy.

This was shown by not adding any additional module or process to the LBS provider, and, actually, the LBS provider does not even notice that an anonymous request is made, as the anonymity offered is transparent to it. The separation of duties among the trusted third party server principle was a critical factor for the success of the proposed scheme, as we assure that only the servers, which participate either on the identity anonymity protocol or position anonymity protocol know the necessary information of the LBS' user in order to achieve its function. Due to the diversity of LBSs types that exist, a generic solution for providing privacy to LBSs' users require the development of a scheme with modular processes to handle all the different kind of LBS services.

In order to achieve these many considerations, in this work the best combination of approaches have been made, which are applicable to the most used LBSs.

Acknowledgements

The authors thank Instituto Politécnico Nacional for financial support under Project Grants SIP-1917, SIP-1999, SIP-20196694 and SIP-20190264.

References

1. **Schiller, J. & Voisard, A. (2004).** *Location-Based Services*. Morgan Kaufmann of Elsevier.
2. **Wernke, M., Skvortsov, P., Dürr, F., & Rothermel, K. (2014).** A classification of location privacy attacks and approaches. *Personal Ubiquitous Computing*. Vol. 18, No. 1, pp. 163–175. DOI: 10.1007/s00779-012-0633-z.
3. **Zurbaran, M., Gonzalez, L., Wightman-Rojas, P., & Labrador, M. (2014).** A Survey on Privacy in Location-Based Services. *Ingeniería y Desarrollo*, Vol. 32, No. 2, pp. 314–343.
4. **Beresfor, A. & Stajano, F. (2003).** Location privacy in pervasive computing. *IEEE Pervasive Computing*, Vol. 2, pp. 46–55. DOI: 10.1109/MPRV.2003.1186725.
5. **Duckham, M. & Kulik, L. (2005).** Simulation of obfuscation and negotiation for location privacy. *International conference on spatial information theory COSIT´05*. Springer, pp. 31–48. DOI: 10.1007/11556114_3.
6. **Gruteser, M. & Hoh, B. (2005).** On the anonymity of periodic location samples. *Second international conference on security in pervasive computing*, pp. 179–192. DOI: 10.1007/978-3-540-32004-3_19.
7. **Krumm. J. (2009)**. A survey of computational location privacy. *Personal and Ubiquitous Computing.* Vol. 13, No. 6, pp. 391–399. DOI: 10.1007/s00779-008-0212-5.
8. **Pfitzmann, A. & Hansen, M. (2005).** *Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology*. Vol. 28, pp. 1–54.
9. **Sweeney, L. (2002)** k-Anonymity: A Model for Protecting Privacy. *Uncertainty, Fuzziness, and*

Knowledge-Based Systems, Vol. 10, No. 5, pp. 557-570. DOI: 10.1142/S0218488502001648.

10. **Chaum, D. (1982).** Blind signatures for untraceable payments. *Proceedings of CRYPTO '82*, pp. 199–203. DOI: 10.1007/978-1-4757-0602-4_18.
11. **Tu, Z., Zheng, S., & Yuille, A. (2008).** Shape matching and registration by data-driven EM. *Computer Vision and Image Understanding,* Vol. 109, No. 3, pp. 290–304. DOI: 10.1016/j.cviu.2007.04.004Get.
12. **Shuang, W., Ha, Y., & Dongnan, L. (2018).** A new identity based blind signature scheme and its application. *IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference,* pp. 672–676. DOI: 10.1109/IAEAC.2018.8577730.
13. **Asuquo, P., Cruickshank, H., Morley, J., Anyigor-Ogah, C.P., Lei, A., Bao, S., & Sun, Z., (2018).** Security and Privacy in Location-Based Services for Vehicular and Mobile Communications: An Overview, Challenges, and Countermeasures. *IEEE Internet of Things Journal*, Vol. 5, No. 6. pp. 4778–4802. DOI: 10.1109/JIOT.2018.2820039.
14. **Ashouri-Talouki, M., Baraani-Dastjerdi, A., & Movahedinia, N. (2017).** BlindLocation: Supporting User Location Privacy Using Blind Signature. *7th International Conference on Computer and Knowledge Engineering,* pp. 53–59. DOI: 10.1109/ICCKE.2017.8167928.
15. **Geng, Z., He, Y., Niu, T., Li, H., Sun, L., Cheng, W., & Li, X. (2017).** Poster: Smart-Contract Based Incentive Mechanism for K-Anonymity Privacy Protection in LBSs. *IEEE Symposium on Privacy-Aware Computing,* pp. 200–201. DOI: 10.1109/PAC.2017.33.
16. **Vora, J., Devmurari, P., Tanwar, S., Tyagi, S., Kumar, N., & Obaidat, M.S. (2018).** Blind Signatures Based Secured E-Healthcare System. *International Conference on Computer, Information and Telecommunication Systems,* pp. 1–5. DOI: 10.1109/CITS.2018.8440186.
17. **Ahmadi, M. & Ghahfarokhi, B. (2016).** Preserving Privacy in Location Based Mobile Coupon Systems Using Anonymous Authentication Scheme. *13th International Iranian Society of Cryptology Conference on Information Security and Cryptology,* pp. 60–65. DOI: 10.1109/ISCISC.2016.7736452.
18. **Green, M. & Miers, I. (2017).** Bolt: Anonymous Payment Channels for Decentralized Currencies. *ACM Conference on Computer and Communications Security*, pp. 473–489. DOI: 10.1145/3133956.3134093.
19. **Verma, G.K. & Singh, B.B. (2016).** New based fair blind signatures. *International Conference on Futuristic Trends in Engineering, Science, Humanities, and Technology*. Vol. 1, pp. 26–32.
20. **Zuberi, R.S. & Ahmad. S.N. (2016).** Secure Mix-Zones for Privacy Protection of Road Network Location Based Services Users. *Journal of Computer Networks and Communications,* Vol. 2016, pp. 1–8. DOI: 10.1155/2016/3821593.
21. **Mayank, P. & Singh. A.K. (2017).** Tor Traffic Identification. *IEEE 7th International Conference on Communication Systems and Network Technologies,* pp. 85–91.
22. **Yin, H. & He, Y. (2019).** I2P Anonymous Traffic Detection and Identification. *IEEE 5th International Conference on Advanced Computing & Communication Systems*, pp. 157–162. DOI: 10.1109/ICACCS.2019.8728517.
23. **Sonklin, K., Feng, Y., Jayalath, D., & Wang, C. (2019).** *A New Location-Based Services Framework for Connected Vehicles Based on the Publish-Subscribe Communication Paradigm.* Preprints, pp. 1–16. DOI: 10.20944/preprints201901.0193.v1.
24. **Chanphearith, S., Santoso, A., & Suyoto, S. (2016).** Analysis and Implementation of Location-Based Augmented Reality Mobile Application for Searching Tourist Attractions and Culinary Places in Phnom Penh City, Cambodia. *International Journal of Computer Science Trends and Technology*, Vol. 4, No. 6, pp. 106–136.
25. **Jannati, H. & Bahrak, B. (2017).** An Oblivious Transfer Protocol Based on Elgamal Encryption for Preserving Location Privacy. *Wireless Personal Communications*, Vol. 97, No. 2, pp. 3113–3123. DOI: 10.1007/s11277-017-4664-7.
26. **Bhandwalkar, M., Bhatia, R., Bhujbal, O., Shinde, A., & Gitem, B.B. (2016).** Privacy Preserving and Content Protecting Location Based Queries. *International Journal of Advanced Research in Computer Science and Software Engineering,* Vol. 6, No. 4, pp. 703–704.
27. **Hu, Q., Wang, S., Hu, C., Huang, J., Li, W., & Cheng, X. (2018).** Messages in a concealed bottle: Achieving query content privacy with accurate location-based services**.** *IEEE Transactions on Vehicular Technology,* Vol. 67, No. 8, pp. 7698–7711. DOI: 10.1109/TVT.2018.2838041.
28. **Solanas, A., Domingo-Ferrer, J., & Martínez-Ballesté, A. (2008).** Location Privacy in Location-Based Services: Beyond TTP-based Schemes. *Proceedings of the 1st international workshop on privacy in location-based applications (PILBA),* pp. 12–23.
29. **Tan, Z., Wang, C., Zhou, M., & Zhang, L. (2018).** Private Information Retrieval in Vehicular Location-Based Services. *IEEE 4th World Forum on Internet*

of Things (WF-IoT), pp. 56–61. DOI: 10.1109/WF-IoT.2018.8355189.

30. **Fei, F., Li, S., Dai, H., Hu, C., Dou, W., & Ni, Q. (2017).** A K-anonymity based schema for location privacy preservation. *IEEE Transactions on Sustainable Computing,* Vol. 4, No. 2, pp. 156–167. DOI: 10.1109/TSUSC.2017.2733018.
31. **Chan, M., Elsherbini, H., & Zhang, X. (2016).** User Density and Spatial Cloaking Algorithm Selection: Improving Privacy Protection of Mobile User. *IEEE 37th Sarnoff Symposium,* pp. 1–2. DOI: 10.1109/SARNOF.2016.7846722.
32. **Zhang, S., Raymond-Choo, K.K., Liu, Q., & Wang, G. (2018).** Enhancing privacy through uniform grid and caching in location-based services. *Future Generation Computer Systems,* Vol. 86, pp. 881–892. DOI: 10.1016/j.future.2017.06.022.
33. **Zhang, S., Wang, G., Alam Bhuiyan, M.Z., & Liu. Q. (2018).** A Dual Privacy Preserving Scheme in Continuous Location-Based Services. *IEEE Internet of Things Journal,* Vol. 5, No. 5, pp. 4191–4200. DOI: 10.1109/JIOT.2018.2842470.
34. **Wang, Y., Xu, D., & Li, F. (2016).** Providing Location-Aware Location Privacy Protection for Mobile Location-Based Services. *Tsinghua Science and Technology,* Vol. 21, No. 3, pp. 243–259. DOI: 10.1109/TST.2016.7488736.
35. **Yu, R., Bai, Z., Yang, L., Wang, P., Ann-Move, O., & Liu, Y. (2016)** A Location Cloaking Algorithm Based on Combinatorial Optimization for Location-Based Services in 5G Networks. *IEEE Access,* Vol. 4, pp. 6515–6527. DOI: 10.1109/ACCESS.2016.2607766.
36. **Hwang, R.H., Hsueh, Y.L., Wu, J.J., & Huang, F.H. (2016).** SocialHide: A generic distributed framework for location privacy protection. *Journal of Network and Computer Applications,* Vol. 76, pp. 87-100. DOI: 10.1016/j.jnca.2016.09.009.
37. **Peng, T., Liu, Q., Meng, D., & Wang, G. (2017).** Collaborative trajectory privacy preserving scheme in location-based services. *Information Sciences,* Vol. 387, pp. 165–179. DOI: 10.1016/j.ins.2016.08.010.
38. **Ye, A., Li, Y., & Xu, L. (2017).** A novel location privacy-preserving scheme based on l-queries for continuous LBS. *Computer Communications,* Vol. 98, pp. 1–10. DOI: 10.1016/j.comcom.2016.06.005.
39. **Zhang, S., Li, X., Tan, Z., Peng, T., & Wang, G. (2019).** A caching and spatial K-anonymity driven privacy enhancement scheme in continuous location-based services. *Future Generation Computer Systems,* Vol. 94, pp. 40–50. DOI: 10.1016/j.future.2018.10.053.
40. **Abdo, J.B., Bourgeau, T., Demerjian, J., & Chaouchi, H. (2016).** Extended Privacy in Crowdsourced Location-Based Services Using Mobile Cloud Computing. *Mobile Information Systems,* Vol. 2016, pp. 1–13. DOI: 10.1155/2016/7867206.
41. **Zhao, H., Wan, J., & Chen, Z. (2016).** A Novel Dummy-Based KNN Query Anonymization Method in Mobile Services. *International Journal of Smart Home,* Vol. 10, No. 6, pp. 137–154. DOI: 10.14257/ljsh.206.10.6.15.
42. **Zhao, H., Yi, X., & Wan, J. (2016).** Privacy-area Aware All-dummy-based Location Privacy Algorithms for Location-based Services. *Joint International Conference on Artificial Intelligence and Computer Engineering (AICE´16) and International Conference on Network and Communication Security NCS´16),* pp. 1–10. DOI: 10.12783/dtcse/aice-ncs2016/5680.
43. **Li, F., Chen, Y., Niu, B., He, Y., Geng, K., & Cao, J. (2018).** Achieving Personalized k-Anonymity against Long-Term Observation in Location-Based Services. *IEEE Global Communications Conference GLOBECOM,* pp. 1–6. DOI: 10.1109/GLOCOM.2018.8647719.
44. **Ghaffari, M., Ghadiri, N., Manshaei, M.H., & Lahijani, M.S. (2017).** P4QS: A Peer-to-Peer Privacy Preserving Query Service for Location-Based Mobile Applications. *IEEE Transactions on Vehicular Technology,* Vol. 66, No. 10, pp. 9458–9469. DOI: 10.1109/TVT.2017.2703631.
45. **Brambilla, G., Amoretti, M., & Zanichelli, F. (2016).** Using Block Chain for Peer-to-Peer Proof-of-Location. *arXiv preprint arXiv:1607.00174.1-11.*
46. **Hankerson, D., Vanstone, S., & Menezes, A. (2004).** *A. Guide to elliptic curve cryptography*. Springer-Verlag, pp. 75–142.
47. **Kalnis, P., Ghinita, G., Mouratidis, K., & Papadias, D. (2007).** Preventing location–based identity inference in anony- mous spatial queries. *IEEE Transactions on Knowledge and Data Engineering*, Vol. 19, No. 12, pp. 1719–1733. DOI: 10.1109/TKDE.2007.190662.
48. **Chow, C.Y., Mokbel, M.F., & Liu, X. (2011).** Spatial cloaking for anonymous location based services in mobile peer-to-peer environments. *Geoinformatica*, Vol. 15, No. 2, pp. 351–230. DOI: 10.1007/s10707-009-0099-y.
49. **Yao, L., Lin, C., Chi, Liu, G., Deng, F., & Wu, G. (2012).** Location Anonymity Based on Fake Queries in Continuous Location-Based Services. *7th International Conference on Availability, Reliability and Security*. pp. 375–382. DOI: 10.1109/ARES.2012.40.

50. Zhu, X., Chi, H., Niu, B., Zhang, W., Li, Z., & Li. H. (2013). MobiCache: When k-anonymity meets cache. *IEEE Global Communications Conference,* pp. 820–825. DOI: 10.1109/GLOCOM. 2013.6831174.

Article received on 06/09/2019; accepted on 14/11/2019. Corresponding author is Gina Gallegos Garcia.