A Distributed Privacy-Preserving Scheme for Location-Based Queries

Emmanouil Magkos
Department of Informatics
Ionian University
Platia Tsirigoti, 49100 Corfu, Greece
Email: emagos@ionio.gr

Panayiotis Kotzanikolaou
Department of Informatics
University of Piraeus
80, Karaoli-Dimitriou, 18534
Piraeus, Greece,
Email: pkotzani@unipi.gr

Spyros Sioutas, Konstantinos Oikonomou
Department of Informatics
Ionian University
Platia Tsirigoti, 49100 Corfu, Greece
Email:{sioutas,okon}@ionio.gr

***Abstract*—In this paper we deal with security and historical privacy in *Location Based Service* (LBS) applications where users submit accurate location samples to an LBS provider. Specifically we propose a distributed scheme that establishes access control while protecting the privacy of a user in both sporadic and continuous LBS queries. Our solution employs a hybrid network architecture where LBS users: (a) are able to communicate with an LBS provider through a network (*e.g.*, cellular) operator, and (b) they are also able to create wireless ad-hoc networks with other peers in order to obtain privacy against an adversary that performs traffic analysis. Our threat model considers the network operator, the LBS provider and other peers, as potential privacy adversaries. For historical privacy we adopt the generic approach of using multiple pseudonyms that are changed frequently. In order to establish untraceability against traffic analysis attacks, a message is not sent directly to the cellular operator, but it is distributed among mobile neighbors who act like mixes and re-encrypt a message before sending it to the LBS provider via the cellular operator. As an extension, we also discuss how to aggregate independent data from different mobile peers before sending them to the LBS provider. This approach may be suitable in applications where aggregate location data are useful (*e.g.*, traffic monitoring and control)**

I. Introduction

The advent of mobile and wireless networking combined with recent advances in sensing and positioning technologies have altered the ways in which people communicate and interact with their environment. In the near future, *Location-Based Services* (LBS) are expected to be available anywhere and anytime. As with many aspects of ubiquitous computing, there is an inherent *trade-off* between access control and user privacy in LBS applications [1], [2], [3]. On one hand the system typically needs to be protected from unauthorized access. On the other hand mobile users require the protection of their context information *e.g.*, position and/or identity information from unauthorized access. Especially when location-based queries are frequent, they can be used to track users and risk a number of fraudulent attacks against privacy (*e.g.*, build user profiles, unsolicited advertising) [4], [2]. The privacy issue is amplified by the requirement in modern telematics and location-aware applications for real-time, continuous location updates and accurate location information (*e.g.*, traffic monitoring, asset tracking, location-based advertising, location-based payments, routing directions) [5], [6], [7].

While most related work for privacy preserving LBSs has concentrated on *sporadic queries* to LBS providers (*e.g.*, asking for the nearest restaurant or finding a nearby friend), recent research is also concerned with an aspect of privacy that is also referred to as path privacy, *historical privacy*, or trajectory anonymization [8], [9], [3], [10], [7]. Here, the goal is to protect the privacy of mobile users in LBS applications against correlation attacks, *e.g.*, to prevent the disclosure of the path followed by a mobile user who walks or travels in an urban area. A typical scenario may be a mobile user that sends continuous queries to LBS applications, *e.g.*, "report the nearest restaurant while I move". LBSs of this type are also called *continuous LBSs* [6].

For privacy preservation, in this paper we adopt the *identity privacy* approach [3] where location information is kept as accurate as possible, but the link to the real identity of a user is protected. The requirement to anonymize location information also reminds of the classical notion of *untraceability* [11]. As the traditional approach of using long-term pseudonyms is not enough [8], sometimes privacy can be enhanced by establishing the *unlinkability* criterion [11], which means destroying the link between successive user positions, even from the point of view of a single LBS provider. Indeed, the provision of unlinkability has been seen as a key issue for historical privacy [10].

Recently a new paradigm of privacy for LBS applications has also emerged where network operators, LBS providers and even network peers are viewed as potential adversaries. As a result, a number of *TTP-free* solutions for enhanced location privacy in LBS services have been proposed *e.g.*, [12], [13], [14], [15], [16], [17], [18], [19], [20]. Of specific interest are fully-distributed or collaborative solutions, where trust is distributed among a set of system peers that form *ad-hoc* wireless networks and collaborate to achieve privacy against a set of untrusted entities (*e.g.*, the mobile peers, the LBS provider, or even the network operator [13], [18], [19]). This change of paradigm may also exploit the hybrid nature of current mobile networks and the capabilities of modern handheld devices that are equipped with both WLAN and cellular interfaces [18], [17], [19].

Our Contribution: In this paper we scope our research to cover LBS applications where users submit independent, highly accurate location samples. Specifically we propose a distributed privacy-preserving scheme that protects the privacy of a user in both sporadic and continuous LBS queries. Our threat model considers the network operator, the LBS provider and other peers, as privacy adversaries. For historical privacy we adopt the generic approach of using multiple pseudonyms that are changed frequently. Furthermore, in order to establish untraceability against traffic analysis attacks, a message is not sent directly to the operator, but it is distributed among mobile neighbors who act like mixes and re-encrypt a message before sending it to the LBS provider via the cellular operator. We also discuss how the privacy homomorphism could also allow to aggregate independent data from different mobile peers before sending them to the LBS provider. This approach may be suitable in applications where aggregate location data could be useful (*e.g.*, traffic monitoring and control) [5], [6], [7].

II. Related work

The use of frequently changing pseudonyms to achieve privacy against correlation attacks in LBSs, was first discussed in [8]. With identity privacy, the goal is to anonymize the location information that is provided to location-aware applications that allow the use of pseudonyms. The advantage of this approach is that location information may also be highly accurate, which is often required in LBSs applications that offer high-quality information services [5], [6]. However it has been shown that the mere use of multiple pseudonyms is not sufficient against a global observer that performs traffic analysis [8], [4], [9] and exploits spatiotemporal correlations in order to link a set of user requests. As a result, for path privacy a user may change a pseudonym at points where the spatial and temporal resolution is decreased *e.g.*, within a MIX zone [8], [21], [22] or a junction [9].

Other general approaches for privacy-preserving in LBS services include location k-anonymization [23], and the obfuscation approach. With k-anonymous protocols, the resolution of location information is decreased to an anonymity set of k users. Distributed solutions for k-anonymous users were proposed in [13], [14], [16], [18], [19], [20]. In [13], [18] for example a set of k users exchange their encrypted locations and compute a k-anonymized centroid that they use as their fake location, when communicating with the LBS provider. Both [13], [18] make use of the additively homomorphic property of several probabilistic public key encryption schemes *e.g.*, [24], where there is an operation $\oplus$ on the message space and an operation $\otimes$ on the cipher space, such that $E(M1) \otimes E(M2) = E(M1 \oplus M2)$. In [18] this property will permit the group of k users to privately compute the centroid, without decrypting single locations. Another series of works include schemes that modify/obfuscate spatial or temporal information (*e.g.*, [4], [25], [26]). Solutions based on location k-anonymization and spatiotemporal obfuscation usually introduce a *privacy vs accuracy* tradeoff and thus may not be able to meet the high position accuracy requirements of modern location tracking applications [5], [6]. Furthermore, the above approaches mostly involve sporadic location-based queries that are executed at an LBS provider and cannot protect continuous paths [10].

A final class of TTP-free approaches contains protocols that are based on Private Information Retrieval (PIR) [27]. At a high level, the LBS provider holds a database that is coded as a n-bit string X and the user wants to privately retrieve X_i, that is the i^{th} bit of X in a way that it is computationally infeasible for the provider to find out the value of i. In [15], [7] it is also shown that the PIR framework, by not revealing any spatial information could also protect LBS users against correlation attacks. A challenge is to design computationally efficient and applicable solutions that reduce the processing overhead of the early schemes, and some recent approaches seem promising towards this direction (*e.g.*, [28]).

A. The scheme of Ardagna et al [19]

The scheme in [19] describes a general framework where message splitting and multi-path communication are used to establish sender k-anonymity in any mobile hybrid network. In the threat model of [19], online servers and other peers are considered untrusted. In the sequel we describe and review the scheme of [19] in the LBS context.

In short, a user u sends a k-anonymous request to an online server s via a mobile operator o, and s returns an anonymous service response that is received and decrypted only by the authorized user u.

- *User u*. The user u specifies the message M and privacy preference k, then splits message M in k packets $\{m_1, m_2, ..., m_k\}$, encrypts each packet with a secret key sk shared with s and appends an identifier mid to each encrypted packet, thus yielding $\bar{m}_i = \{E_{sk}(m_i), mid\}$ for each $i = 1, ..., k$. The user then randomly chooses $k-1$ neighboring peers in her range to distribute the packets. Packets are distributed to the neighboring peers using a random forwarding distribution algorithm [19].
- *Operator o*. Eventually all packets are sent to s via o. The operator sees packets from k different peers, including the sender u, who thus remains k-anonymous.
- *Server s*. The server prepares a response message M_r, and encrypts it with the secret key sk that is shared with u. Then, s relies on o to send the encrypted response to the k peers involved in the original anonymous request. Only u is able to decrypt the server response.

B. Some remarks on the Ardagna et al scheme

1) The server s and the user u pre-share a common secret key sk. This key is used to identify the real identity of u. As a result, all messages received by s are traced to the identity of their senders. In [19] it is stated that this is done to provide for user accountability.
2) If the scheme was adopted in a continuous LBS setting, all messages sent by u could be linked by s. All services messages sent by LBS users would be traceable and

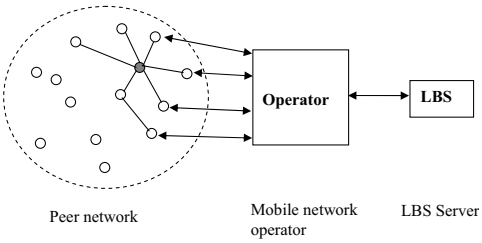

Fig. 1. System model

linkable by s and privacy would only be offered against the cellular operator o.

3) Observe that when receiving a message, s does not know that it came from user u, so an exhaustive search is needed, in order to find the correct sk to decrypt the message, which increases decryption costs for s.

III. Design and security requirements

A. System model

We view a system that consists of a set of mobile users with handheld devices, one or more cellular operators (OP) and one or more LBS providers (LP). We also assume a client-based positioning system is in place [29] *e.g.*, a GPS-enabled device, and clients use it to autonomously compute their location.

The network architecture (Fig. 1) is very similar to the mobile hybrid network described in [19]. Specifically, users possess handheld devices that are equipped with both WLAN (*e.g.*, WiFi or Bluetooth) and WWAN (*e.g.*, GSM/3G) capabilities. Locally, mobile peers are able to establish ad-hoc connections (point-to-point or broadcast) with each other. At the same time, users belong to a cellular network and are able to receive and send signals to an OP in order to access services provided by an Internet-connected LP.

B. Threat model and assumptions

We consider a global passive adversary that eavesdrops on all communications *i.e.*, between all system entities (both peers and authorities). Furthermore, the adversary can obtain the records of any party that receives or observes communication messages, including the system authorities (the OP, LP) and mobile peers, in order to obtain or construct a location history for a mobile user.

We assume that the adversary has no other ways to link or trace a user, *e.g.*, when a compromised LBS provider's links different pseudonyms to the same set of personal preferences at the service level [8]. In addition we scope away adversarial settings where the observer correlates spatiotemporal information between successive locations -instead we refer the reader to other works in the field *e.g.*, [8], [4], [9], [30], [21], [31], [22], [10]. Finally, we do not deal with tracing/linking at the physical or MAC layers [32], [33].

C. Security and privacy requirements

For security, communication messages between system entities should be authenticated. From the point of view of the LP, the need for access control is twofold. Message and entity authentication are needed in order to authorize access to a service (*e.g.*, to prevent abuse, for billing purposes), as well as to provide personalized, context-aware services.

For privacy, we consider different privacy requirements, depending on the nature of the messages that are being sent to the LP. We distinguish between three kinds of interactions between a user and the LP:

1) *Sporadic queries*. *e.g.*, "Find me the closest restaurant". Sporadic queries should be untraceable and unlinkable. They also require an anonymous response by the LP, which means that while only the requesting user should be able to read the answer, neither the LP not the OP should be able to trace the response to the specific user.
2) *Continuous queries with frequent location updates*. *e.g.*, "find me the closest point-of-interest (POI) while I move". Continuous queries should also be untraceable. Concerning unlinkability, different continuous queries should not be linkable by the LP (*e.g.*, "return the closest restaurant while I move" should not be linked with "return the closest clinic while I move"). On the other hand, multiple location updates concerning a specific query may have to be linkable in order to provide the service (*e.g.*, respond with a point of interest that corresponds to the user's trajectory).
3) *Group context information*. A final class concerns the requirement in some LBS applications to manage aggregate data about a set of mobile users [6], [7], [34]. As a result we identify a third class of interactions, where an aggregate of independent context data is sent to the LP via the OP. For example in traffic monitoring systems, it may suffice to record the average velocity, traveled distance or maximum acceleration of a group of passing cars at an observation point. Atomic location data should not be linked or traced to any specific user identity.

IV. A privacy-preserving scheme

Each user employs a list of short-lived, uncorrelated credentials for each LBS provider she communicates with. Without loss of generality we will assume that there is only one LBS provider (LP) and one cellular operator (OP). We also assume that conventional digital signature (*e.g.* ECDSA [35]) and symmetric encryption (*e.g.*, AES) systems are in place. In addition, we assume the existence of a probabilistic public key encryption system that supports the homomorphic property and allows for re-encryption of messages (*e.g.*, the ElGamal scheme [36], or the Paillier encryption scheme [24]).

A. Registration phase

The list of credentials is generated during the user registration phase. For a specific service SID, a user U generates a list of credentials of the form $\{C_1, C_2, ..., C_n\}$, for up to n subsequent service transactions. These credentials are validated by the LP using a *blind signature* [37] sub-protocol, where U proves her identity to the LP, and gets a signature on

a list of "blinded" credentials. For example, the j_{th} credential is obtained in the following way:

$$U \rightarrow LP : \{[r_j]_{PK_{SID}} \cdot C_j\}_{SK_U} \quad (1)$$

$$LP \rightarrow U : r_j \cdot \{C_j\}_{SK_{SID}} \quad (2)$$

where r_j is a random nonce, $[]_{PK_{SID}}$ denotes encryption with the public key of service SID, and $\{\}_{SK_U}$, $\{\}_{SK_{SID}}$ denote signing with the private key of U and service SID respectively. The user can easily remove the random factor r_j and un-blind the credential C_j.

B. Service access phase

Each message can be either a location query (sporadic or continuous) message, or a group context message. In the following we distinguish between the two cases.

Protocol I - Location queries: For a location query message M_j, U builds a message of the form: $m_j = M_j, s_j, \bar{r}_j, \{C_j\}_{SK_{SID}}$, where s_j is a fresh symmetric key that will be transferred to the LP for encrypting and authenticating the anonymous response, $\bar{r}_j$ is a random number specific to this location query, and C_j is the validated credential that is used as a temporary pseudonym for the specific transaction. The message that is finally broadcasted is:

$$U \rightarrow PEERS : [\tilde{m_j}]_{PK_{SID}}, cid, mid \quad (3)$$

where $\tilde{m_j} = m_j, MAC_{C_j}(m_j)$[1] and $MAC_{C_j}()$ denotes a Message Authentication Code with a symmetric key that is derived from the credential C_j. Note that for unlinkability the pseudonym C_j must be updated in the next sporadic query (alternatively, it suffices to say that pseudonyms are updated when the user enters a properly constructed MIX zone [8]). On the other hand it may be the same for a continuous query *e.g.*, when the trajectory of the user needs to be determined by the LP in order to provide a specific service. For the peer nodes to discriminate between location queries and group context messages, a cid identifier is appended to each message (for simplicity, $cid = 0$ for location queries, and $cid = 1$ for group context messages). The message identifier mid is a message identifier that will be used locally by other peers to avoid re-encrypting the same message twice.

For message secrecy, U encrypts $\tilde{m_j}$ with the public key of the specific LBS service, PK_{SID}. For simplicity we consider the ElGamal encryption scheme [36]:

Input: plaintext $\tilde{m_j}$, random $r \in Z_p^*$, $PK_{SID} = (p, g, y)$
Output: Ciphertext R, C

$$R = g^r mod p \quad (4)$$

$$C = y^r \cdot \tilde{m_j} \ mod p \quad (5)$$

[1]For simplicity, we assume that the size of $\tilde{m_j}$ is bounded by p. For messages of size greater than p an additional protocol run will be required.

where $y = g^x mod p$, x is the private decryption key and g is a generator of Z_p^*. Observe that the encryption function satisfies the multiplicatively homomorphic property:

$$E(m; r) \times E(m'; r') = E(m \times m'; r + r')$$

where $E(m; r)$ denotes probabilistic encryption of message m using the random number r. As a result, for re-encrypting $E(m; r)$ it suffices to multiply with $E(1; r')$.

Indeed, the encrypted query message of Eq. 3 is then distributed among the neighboring peers (*e.g.*, using a random forwarding approach, as in [38], [19]) who act like MIXes and re-encrypt the message before submitting it to the LP through the OP. Specifically, if $cid = 0$ a receiving peer checks the identifier mid and if it is the first time it sees this message it will re-encrypt it and then forward it to the next peer (for example, with probability z) or will send it directly to the LP (with probability $1 - z$). Re-encryption is done in the following way:

Input: R, C, $r' \in Z_p^*$, $PK_{SID} = (p, g, y)$
Output: Ciphertext R', C'

$$R' = R \cdot g^{r'} mod p \quad (6)$$

$$C' = C \cdot y^{r'} mod p \quad (7)$$

We note that the re-encrypting peers do not have to be registered with the specific service SID. After receiving, say, R', C', the LP decrypts by computing $\tilde{m_j} = C'/R'^x$. For an anonymous response M_{res}, the LP prepares a message of the form:

$$LP \rightarrow PEERS : \bar{r}_j, [M_{res}]_{s_j}, MAC_{s_j}(M_{res}) \quad (8)$$

where $[]_{s_j}$ and $MAC_{s_j}()$ denote symmetric encryption and authentication with keys derived from s_j. The anonymous response is then broadcasted to the group peers, via the OP. The user U recognizes the random identifier $\bar{r}_j$, then uses s_j to decrypt the anonymous response and verify the MAC value.

Future location updates of U concerning the same continuous query will be authenticated by the same credential C_j. However, for a new location query U should use a different credential C_j.

Protocol II - Group context messages: For computing group context messages in a distributed fashion we will consider the Paillier encryption scheme [24] which provides a *trapdoor* to efficiently compute the discrete logarithm, and works as follows: For key generation, first compute $N = pq$ an RSA modulus where p and q are two large primes, and then compute the Carmichael function $\lambda := lcm(p - 1, q - 1)$. Then find a generator g of $Z_{n^2}^*$ such that $g \equiv 1(modn)$. The public key is (N, g) while the λ is the secret key. To encrypt a message $m \in Z_n$, choose a random $r \in Z_n^*$ and compute $E(m) \equiv g^m r^N (modN^2)$. For decryption, compute: $m = \frac{L(c^\lambda (modn^2))}{L(g^\lambda (modn^2))} modn$. Observe that the function satisfies the additively homomorphic property:

$$E(m_1; r_1) \times E(m_2; r_2) = E(m_1 + m_2; r_1 \times r_2)$$

where $r_1, r_2 \in Z_n^*$. Group context messages are aggregated in the following way: Without loss of generality we will assume that all peers are registered with the same service. As an example, a node U_1 encrypts a group context message m_1 with Paillier, then appends $cid = 1$, mid and an aggregate counter c with initial value $c = 1$. The message is then distributed among the neighbor mobile peers:

$$U \rightarrow PEERS : [m_1]_{PK_{SID}}, cid, mid, c \quad (9)$$

where $cid = 1$ denotes a group context message. A receiving peer U_2 will check the identifier mid and if it is the first time it sees this message it will re-encrypt it, increment counter c and then forward it to the next peer (for example, with probability z) but at the same time U_2 will also add its input m_2 in order to create the encryption of the partial aggregate:

$$E(m_1 + m_2; r_1 \times r_2) \equiv g^{m_1+m2}(r_1 r_2)^N (mod N^2) \quad (10)$$

As a result, group context messages are summed up by the group peers before being submitted to the LP via the OP. At the end of the protocol, if ℓ peers chose to add their input to the group context function, the LP will receive $E(\sum_{i=1}^{\ell} m_i, \prod_{i=1}^{\ell} r_i)$ and use the Paillier decryption function to obtain the aggregate $\sum_{i=1}^{\ell} m_i$.

C. Protocol analysis

Protocol I preserves both unlinkability and untraceability, while achieving mutual authentication for messages exchanged between users and the LP. Specifically, during the registration phase the LP authenticates the user U and then blindly signs the list of credentials provided by U. Given that successive service accesses by U will be authenticated by a different credential C_j, untraceability and unlinkability against the LP and the OP is provided.

For protection against traffic analysis, a message is not send directly to the cellular operator, but it is distributed among mobile neighbors who act like mixes and re-encrypt a message before sending it to the LBS provider via the operator. Note however that protection against traffic analysis is only guaranteed against coalitions of peers and not in the case of a global privacy adversary, since a global adversary can use the identifier mid to trace different instances of a message. Communication between the LP and U is mutually authenticated: In Eq. 3, U uses the public key of service SID to securely transfer a symmetric key s_j, and in Eq. 8 this key is used to encrypt and authenticate the response M_{res}. While only U is able to decrypt the response, user anonymity is preserved, since neither the OP nor the LP can trace the message to U.

Protocol II is suitable for applications that require aggregate location data. In the proposed protocol, peers are able to add their message in the group context message, which effectively re-encrypts the previous input from the point of view of an observer. The privacy homomorphism allows for *strong privacy* [5] without degrading the high accuracy and utility of the location data. The LP decrypts an aggregate of partial inputs without being able to link or trace atomic location data to any specific user identity. In addition, each peer adds its own message without being able to guess another peer's input. The same is true in the re-encryption phase of Protocol I. Note that in contrast with Protocol I, in Protocol II the use of the identifier mid does not allow traffic analysis to a global privacy adversary. This is due to the fact that the aggregate location queries are initiated by the LBS and they are propagated through the peers that are close to the location in question. Each peer will participate in the query in a voluntary basis. It should be noted that in Protocol II messages are not integrity protected, since this would break the additive homomorphic property of the encryption. If however message integrity is required, Protocol II could be combined with Protocol I in order to allow peers to protect the integrity of their messages.

Concerning the computational security of the public-key encryption functions, the semantic security of ElGamal encryption is based on the *Decision Diffie-Hellman* (DDH) problem [39] while the *Decisional Composite Residuosity Assumption* (DCRA) is required to show that a Paillier encryption is semantically secure. Finally, since all the exchanged messages are encrypted and integrity protected before transmission, they are protected from passive adversaries.

Concerning the computation costs, the proposed scheme requires one public key encryption plus one blind signature from the user, per each validate credential, during the registration phase. During the service access phase, the requesting user will be required to compute one public key encryption and one MAC operation during the construction of the service request. However, since the peers will re-encrypt the message with a probability z, then the total expected number of encryptions will be $\ell \cdot z$, where ℓ is the number of peers.

We note that our approach is suitable in location-aware services that cannot be accessed anonymously (*i.e.*, they require identification) but do not require a true identity either [8], thus allowing for the use of pseudonyms. (please also refer to [8], [40] for a categorization of LBS based on how they manage a user's identity). Furthermore, we do not deal with cases where unlinkability is very difficult or cannot be obtained, for example in reputation-based or people locator services [8].

V. Conclusions and Future Work

In this paper we described a hybrid network architecture and a scheme for privacy-preserving access control in LBS applications. Our solution is distributed in that users are also able to create ad-hoc networks with other peers in order to obtain privacy against a global adversary that performs traffic analysis. For unlinkability and untraceability, users obtain a list of uncorrelated pseudonymous credential during a registration protocol with the LBS provider. For privacy against traffic analysis attacks, a message is not sent directly to the cellular operator, but it is distributed among mobile neighbors who act like mixes and re-encrypt a message before sending it to the LBS provider via the cellular operator. As an extension, we also discuss how to aggregate independent data from different mobile peers before sending them to the LBS provider. The

potential of aggregated-based data collection in location-based environments is yet to be explored by future research.

REFERENCES

[1] M. Langheinrich, "Privacy by design-principles of privacy-aware ubiquitous systems," in *Ubiquitous Computing - Ubicomp 2001*, ser. Lecture Notes in Computer Science, vol. 2201. Springer, 2001, pp. 273–291.

[2] M. Duckham and L. Kulik, "Location privacy and location-aware computing," in *Investigating Change in Space and Time*, J.Drummond, R. Billen, D. Forrest, and E. Joao, Eds. CRC Press, 2006.

[3] C. Ardagna, M. Cremonini, S. De Capitani di Vimercati, and P. Samarati, "Privacy-enhanced location-based access control," in *The Handbook of Database Security: Applications and Trends*, M. Gertz and S. Jajodia, Eds. Springer-Verlag, 2007.

[4] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *MobiSys '03: Proceedings of the 1st international conference on Mobile systems, applications and services*. ACM, 2003, pp. 31–42.

[5] M. Gruteser and X. Liu, "Protecting privacy, in continuous location-tracking applications," *IEEE Security & Privacy*, vol. 2, no. 2, pp. 28–34, 2004.

[6] L. Kulik, "Privacy for real-time location-based services," *SIGSPATIAL Special*, vol. 1, no. 2, pp. 9–14, 2009.

[7] G. Ghinita, "Private Queries and Trajectory Anonymization: a Dual Perspective on Location Privacy," *Transactions on Data Privacy*, vol. 2, no. 1, pp. 3–19, 2009.

[8] A. Beresford and F. Stajano, "Location privacy in pervasive computing," *Pervasive Computing, IEEE*, vol. 2, no. 1, pp. 46–55, 2003.

[9] M. Gruteser, J. Bredin, and D. Grunwald, "Path privacy in location-aware computing," in *Proceedings of MobiSys 2004, Workshop on Context Awareness*, 2004.

[10] C. Bettini, S. Mascetti, S. Wang, D. Freni, and S. Jajodia, "Anonymity and historical-anonymity in location-based services," in *Privacy in Location Based Applications*, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2009, vol. 5599, pp. 1–30.

[11] A. Pfitzmann and M. Köhntopp, "Anonymity, unobservability, and pseudonymity - a proposal for terminology," in *Workshop on Design Issues in Anonymity and Unobservability*, 2000, pp. 1–9.

[12] C. Chow, M. Mokbel, and X. Liu, "A peer-to-peer spatial cloaking algorithm for anonymous location-based service," in *Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems*. ACM, 2006, p. 178.

[13] A. Solanas and A. Martínez-Ballesté, "Privacy protection in location-based services through a public-key privacy homomorphism," in *Public Key Infrastructure, 4th European PKI Workshop: Theory and Practice, EuroPKI 2007*, ser. Lecture Notes in Computer Science, vol. 4582. Springer, 2007, pp. 362–368.

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

[15] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K. Tan, "Private queries in location based services: anonymizers are not necessary," in *SIGMOD '08: Proceedings of the 2008 ACM SIGMOD international conference on Management of data*. New York, NY, USA: ACM, 2008, pp. 121–132.

[16] G. Zhong and U. Hengartner, "Toward a distributed k-anonymity protocol for location privacy," in *WPES '08: Proceedings of the 7th ACM workshop on Privacy in the electronic society*. New York, NY, USA: ACM, 2008, pp. 33–38.

[17] A. Solanas, J. Domingo-Ferrer, and Martínez-Ballesté, "Location privacy in location-based services: Beyond TTP-based schemes." in *Proceedings of the 1st International Workshop on Privacy in Location-Based Applications - PiLBA 2008*, vol. 397. CEUR-WS.org, 2008.

[18] A. Solanas and A. Martínez-Ballesté, "A TTP-free protocol for location privacy in location-based services," *Computer Communications*, vol. 31, no. 6, pp. 1181–1191, 2008.

[19] C. Ardagna, S. Jajodia, P. Samarati, and A. Stavrou, "Privacy preservation over untrusted mobile networks," in *Privacy in Location Based Applications*, ser. Lecture Notes in Computer Science. Springer, 2009, vol. 5599, pp. 84–105.

[20] G. Zhong and U. Hengartner, "A distributed k-anonymity protocol for location privacy," *IEEE International Conference on Pervasive Computing and Communications*, pp. 1–10, 2009.

[21] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in vanets," in *Proceedings of the Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS2007)*, 2007, pp. 129–141.

[22] J. Freudiger, R. Shokri, and J. Hubeaux, "On the optimal placement of MIX zones," in *9th International Symposium, Privacy Enhancing Technologies – PETS 2009, Seattle, WA, USA, August 5-7, 2009*, ser. Lecture Notes in Computer Science, vol. 5672. Springer, 2009.

[23] P. Samarati and L. Sweeney, "Generalizing data to provide anonymity when disclosing information (abstract)," in *PODS '98: Proceedings of the seventeenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of database systems*. New York, NY, USA: ACM, 1998, p. 188.

[24] P. Paillier, "Public-key cryptosystems based on discrete logarithms residues," in *Eurocrypt 99*, ser. LNCS, vol. 1592. Springer-Verlag, 1999, pp. 221–236.

[25] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in *Third International Conference on Pervasive Computing – Pervasive 2005*, ser. Lecture Notes in Computer Science, vol. 3468. Springer, 2005, pp. 152–170.

[26] D. Lin, E. Bertino, R. Cheng, and S. Prabhakar, "Location Privacy in Moving-Object Environments," *Transactions on Data Privacy*, vol. 2, no. 1, pp. 21–46, 2009.

[27] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," in *Annual IEEE Symposium on Foundations of Computer Science*. IEEE Computer Society, 1995, pp. 41–50.

[28] F. Olumofin, P. Tysowski, and I. Goldberg, "Achieving efficient query privacy for location based services," Centre for Applied Cryptographic Research, University of Waterloo, Tech. Rep. CACR Tech Report 2009-22, 2009.

[29] B. Schilit, J. Hong, and M. Gruteser, "Wireless location privacy protection," *IEEE Computer*, pp. 135–137, 2003.

[30] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *IEEE Wireless Communications and Networking Conference (WCNC 2005), IEEE Computer Society Press, Los Alamitos*, 2005.

[31] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Preserving privacy in GPS traces via uncertainty-aware path cloaking," in *Proceedings of the 14th ACM conference on Computer and communications security*. ACM, 2007, p. 171.

[32] K. Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," *Proceedings of IEEE SecureComm*, 2007.

[33] M. Gruteser and D. Grunwald, "Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis," *Mobile Networks and Applications*, vol. 10, no. 3, pp. 315–325, 2005.

[34] S. Orlando, R. Orsini, A. Raffaeta, A. Roncato, and C. Silvestri, "Spatio-temporal aggregations in trajectory data warehouses," in *Proceedings of Data Warehousing and Knowledge Discovery, 9th International Conference,*.

[35] SECG, "Standards for efficient cryptography group. SEC 1: Elliptic curve cryptography," Available at: http://www.secg.org/download/aid-385/sec1_final.pdf, 2005.

[36] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE transactions on information theory*, vol. 31, no. 4, pp. 469–472, 1985.

[37] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology – Proceedings of Crypto 82*, D. Chaum, R. Rivest, and A. Sherman, Eds., 1983, pp. 199–203.

[38] P. Cencioni and R. Di Pietro, "VIPER: A vehicle-to-infrastructure communication privacy enforcement protocol," in *IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems, 2007. MASS 2007*, 2007, pp. 1–6.

[39] Y. Tsiounis and M. Yung, "On the security of ElGamal-based encryption," in *Proceedings of the First International Workshop on Practice and Theory in Public Key Cryptography: Public Key Cryptography*.

[40] T. Candebat, C. Dunne, and D. Gray, "Pseudonym management using mediated identity-based cryptography," in *Proceedings of the 2005 workshop on Digital identity management*. ACM, 2005, p. 10.