Cryptographic Approaches for Privacy Preservation in Location-Based Services: A Survey

Emmanouil Magkos
Ionian University, Department of Informatics,
Plateia Tsirigoti 7, 49100, Corfu, Greece,
emagos@ionio.gr

ABSTRACT

Current research in location-based services (LBSs) highlights the importance of cryptographic primitives in privacy preservation for LBSs, and presents solutions that attempt to support the (apparently) mutually exclusive requirements for access control and context privacy (i.e., identity and/or location), while at the same time adopting more conservative assumptions in order to reduce or completely remove the need for trust on system entities (e.g., the LBS provider, the network operator, or other peer nodes). This paper surveys the current state of knowledge concerning the use of cryptographic primitives for privacy-preservation in LBS applications.

Keywords: Information systems; location-based services; privacy and security; cryptography

INTRODUCTION

In the era of mobile and wireless communication technologies, recent advances in remote sensing and positioning technologies have altered the ways in which people communicate and interact with their environment. In the not-so-far future, *Location-Based Services* (LBS) that take into account the location information of a user, are expected to be available anywhere and anytime. Such services will be highly personalized and accessible even by resource-constrained mobile devices. A classification of the most popular services includes: a) *point-of-interest* or "pull" services where a user sporadically queries an LBS provider to receive a nearby point of interest (e.g., Konidala et al, 2005; Candebat et al, 2005; Hengartner, 2006; Solanas & Balleste, 2007; Kohlweiss et al, 2007;Ghinita et al, 2008; Solanas & Balleste, 2008; Hengartner, 2008; Olumofin et al, 2009; Ardagna et al, 2009; Ghinita et al, 2009); b) *people-locator* services, where a watcher asks the LBS provider for the location of a target (e.g., Hauser & Kabatnik, 2001; Rodden et al, 2002; Bessler & Jorns, 2005; Jorns et al, (2005, 2007); Zhong et al, 2007; Sun et al, 2009); c) *notification-based* or "push"" services, where location-based alerts or notifications are sent to a user (e.g., Zhu et al, 2003; Kolsch et al, 2005).

A typical scenario involves a user with a handheld device connecting through a mobile communication network to an external third party that provides an LBS service over the Internet. As with many aspects of ubiquitous computing, there is an inherent *trade-off* between access control and user privacy in LBS applications (Hauser & Kabatnik, 2001;Langheinrich, 2001; Rodden et al, 2002; Duckham & Kulik, 2006; Ardagna et al, 2007). On one hand the system

typically needs to be protected from unauthorized access and misuse. On the other hand mobile users require the protection of their context information (e.g., location and/or identity information) against privacy adversaries (e.g., big-brother type threats, user profiling, unsolicited advertising) (Hauser & Kabatnik, 2001; Gruteser & Grunwald, 2003; Duckham & Kulik, 2006; Ardagna & Cremonini et al, 2009). 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) (Gruteser & Liu, 2004; Kulik, 2009; Ghinita, 2009).

Recent research highlights the importance of *cryptography* in privacy preservation for LBSs, and presents solutions that attempt to support the (apparently) mutually exclusive requirements for access control and context privacy, while at the same time adopting conservative assumptions in order to reduce or completely remove the need for trust on system entities (e.g., the LBS provider, the network operator, or even the peer nodes). While a number of recent survey papers (e.g., Ardagna et al, 2007; Solanas et al, 2008; Ardagna & Cremonini et al, 2009; Kulik, 2009) cover aspects of access control and privacy, to the best of our knowledge there has been no thorough survey of the use of cryptographic techniques for privacy-preservation in LBS services.

Our contribution

This paper surveys the current state of knowledge concerning the use of cryptographic primitives for achieving privacy-preservation in LBS services. Specifically, we categorize current research into three groups, based on the trust assumptions between parties involved in LBS schemes: TTP-based approaches, semi-distributed schemes, and TTP-free approaches. For each category, we review and evaluate the current literature in terms of privacy, security and efficiency.

DESIGN CONSIDERATIONS

Privacy Requirements

In general, privacy-preserving systems for LBS services are expected to satisfy some or all of the basic properties below (Pfitzmann and Kohntopp, 2000; Hauser & Kabatnik, 2001; Beresford & Stajano, 2003; Gajparia et al, 2004; Ardagna et al, 2007; Jorns et al, 2007; Kohlweiss et al, 2007; Solanas & Balleste, 2008; Hengartner, 2008; Ardagna & Cremonini et al, 2009):

- **Location privacy**: The protocol does not reveal the (exact) user's location information to the LBS provider. More generally, no unauthorized entity (or a coalition of unauthorized entities) should have access to the location data of the user, past or current.
- **Identity privacy (untraceability)**: The LBS provider is not able to find the identity of the user, based on the location information received during the user access. More generally, no unauthorized entity (or a coalition of unauthorized entities) should be able to trace the real identity of the user.
- **Tracking protection (unlinkability)**: The LBS provider is not able to link two or more successive user positions. More generally, no unauthorized entity (or a coalition of unauthorized entities) should be able to link different sessions of the user.

Security Requirements

Access control in LBS involves satisfying some or all of the following security properties (Hauser & Kabatnik, 2001; Konidala et al, 2005; Candebat et al, 2005; Jorns et al, 2007; Kohlweiss et al, 2007; Ardagna & Cremonini et al, 2009; Saroiu & Wolman, 2009):

- **Mutual authentication**: Communication messages between system entities should be authenticated and integrity-protected. For example, an LBS provider will require user authentication in order to prevent service abuse, while users may also require to identify the LBS provider, in order to protect themselves from spoofing attacks.
- **Database secrecy**: The querying user should obtain no more than the requested information from the LBS provider. For example, from the LBS provider's perspective, returning a large number of points-of-interest in response to a cloaked location query, would be against the provider's interests (Ghinita et al, 2009).
- **Location-Based Access Control (LBAC)** (also known as *context authentication*: The user may be required to prove her/his location in order to have access to a service or resource. This requirement is specific only to some location-aware applications, where a user may have an incentive to lie about her/his location.
- **Accountability**: Given the possibilities of abuse (e.g., illegal actions, abnormal access pattern of the user or when a credential is linked to an unlawful act), an option could be to have a mechanism for revoking the anonymity of a specific credential and tracing the identity of a real user, in order to establish accountability. Typically, anonymity revocation will be an off-line protocol, where an LBS provider and a *Trusted Third Party* (TTP), given credential and transaction information, will be able to trace the identity of a user. The provider can then take appropriate measures, e.g., blacklisting a user. However it should not be easy to abuse this capability (e.g., in order to impersonate a user).
- **Non-repudiation**: A related requirement is non-repudiation, under which it should be possible to produce evidence regarding an entity participating to a transaction, in order to protect against a user's false denial of having participated to a transaction.

In the following we assume that an adversary will not exploit weaknesses in the underlying cryptographic primitives, and that when needed, a Public Key Infrastructure for certificate management is in place. Furthermore, while a typical threat model contains an adversary that will also attempt to read, modify or replay messages in order to impersonate users, set up man-in-the-middle attacks or disrupt the network in other ways, we do not emphasize on trivial uses of encryption to provide secrecy, integrity and authentication for the communication channel: this can be offered by classical techniques (Kaufman et al, 2002).

Efficiency Requirements

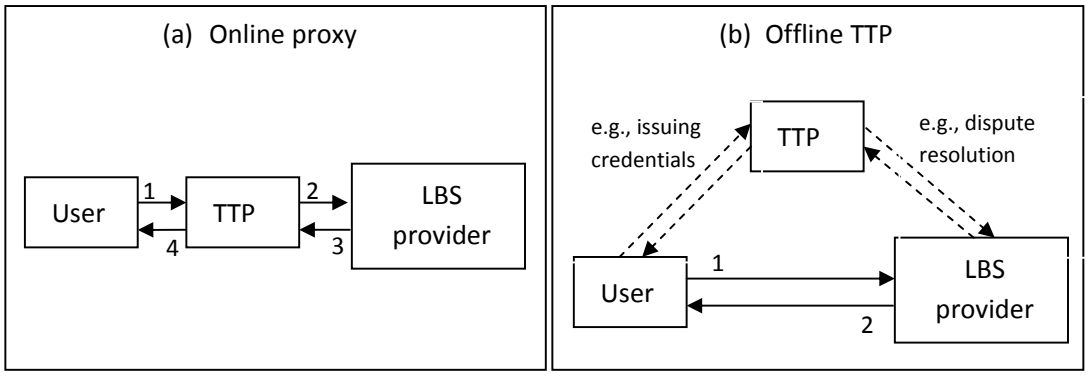
Any privacy-preserving scheme for LBS services should be efficient, mainly for the resource-constrained mobile user, in terms of:

- **Computation**: User registration and service access should be efficient, with as few public operations as possible.
- **Storage**: Users obtain and store a minimum necessary amount of credential information.
- **Communication**: The number of passes and bits that are communicated should be kept as low as possible.

A HIGH-LEVEL CATEGORIZATION OF CRYPTO-BASED LBS PRIVACY MODELS

A traditional approach for privacy is to move the users' trust from the LBS provider to a *fully-trusted* third party (TTP), in the form of an *online* application broker or proxy that mediates between the user and the LBS provider, guarantees identity and/or location privacy and is usually assumed not to conspire with the adversary (e.g., Rodden et al, 2002; Gruteser & Grunwald, 2003; Gajparia et al, 2004; Kolsch et al, 2005; Gedik & Liu, 2005; Konidala et al, 2005; Candebat et al, 2005; Mokbel et al, 2006; Khoshgozaran & Shahabi, 2007). Alternatively, the TTP may be an *offline* authority, whose role may include: certificate management, group key management, dispute resolution, credential revocation and accountability (e.g., Jorns et al, (2005, 2007)). The different roles of a TTP in various models are depicted in Figure 1.

Figure 1. Different roles of a TTP in LBS privacy models



The strongest form of privacy can be achieved when any party receiving part of the communication is considered as untrusted. For example, the most conservative threat model considers a polynomial-time adversary that monitors all communications within the network to trace/track users, may compromise the LBS provider(s) and/or the network operator(s) and/or other peers and extract their logs to infer private information. The level of assumed trust can thus be used to classify the literature for privacy preservation (Figure 2). Indeed, we consider *TTP-based*, *semi-distributed* and *TTP-free* approaches:

- **TTP-based schemes**: Most schemes within this category adopt a centralized model for privacy. Here are included approaches that employ online and/or offline TTPs for: a) protecting the location information of users i.e., *TTP spatial k-anonymity* (Gruteser & Grunwald, 2003; Gedik & Liu, 2005; Mokbel et al, 2006), *TTP cloaking/obfuscation* (Ardagna et al, 2007; Hengartner, 2008; Khoshgozaran & Shahabi, 2007); b) protecting

the link between location and user identity i.e., identity privacy with *simple pseudonyms* (Hauser & Kabatnik, 2001; Rodden et al, 2002; Konidala et al, 2005; Candebat et al, 2005) or *multiple pseudonyms* (Kolsch et al, 2005; Jorns et al, (2005, 2007)).

- **Semi-distributed schemes**: This category, lies between TTP-based and TTP-free categories. To relax the need for a single trusted party, it has been proposed that trust should be distributed on a set of of (two or more) non-colluding authorities that guarantee the privacy or the users (e.g., Kolsch et al, 2005; Kohlweiss et al, 2007; Zhong & Hengartner, (2008, 2009)). Or, a semi-trusted authority could be trusted on some but not all aspects of user privacy: this authority could be the network operator, the LBS provider (e.g., Hauser & Kabatnik, 2001) or an external authority (e.g., Zhong et al, 2007).
- **TTP-free schemes**: In TTP-free solutions, trust assumptions are very weak or completely removed. The category contains *client-server* architectures (e.g., Ghinita et al, 2008; Olumofin et al, 2009; Ghinita et al, 2009), where communication takes place between a user and an untrusted LBS provider, as well as fully-distributed or *collaborative* settings (e.g., Solanas & Balleste, (2007,2008); Ghinita et al, 2007; Zhong et al, 2007; Ardagna et al, 2009; Rebollo-Monedero et al, 2009), where trust is distributed among a set of system peers that form ad-hoc networks and collaborate to achieve privacy against a set of untrusted entities (i.e., the LBS provider, and/or mobile peers or even the network operator). 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 (Solanas & Balleste, 2008; Solanas et al, 2008; Ardagna et al, 2009). Finally, this category also includes user-centric location privacy approaches where users control access to their location information without the need of any TTPs (e.g., Sun et al, 2009;Yiu et al, 2009).

Figure 2. A categorization of crypto-based LBS privacy models

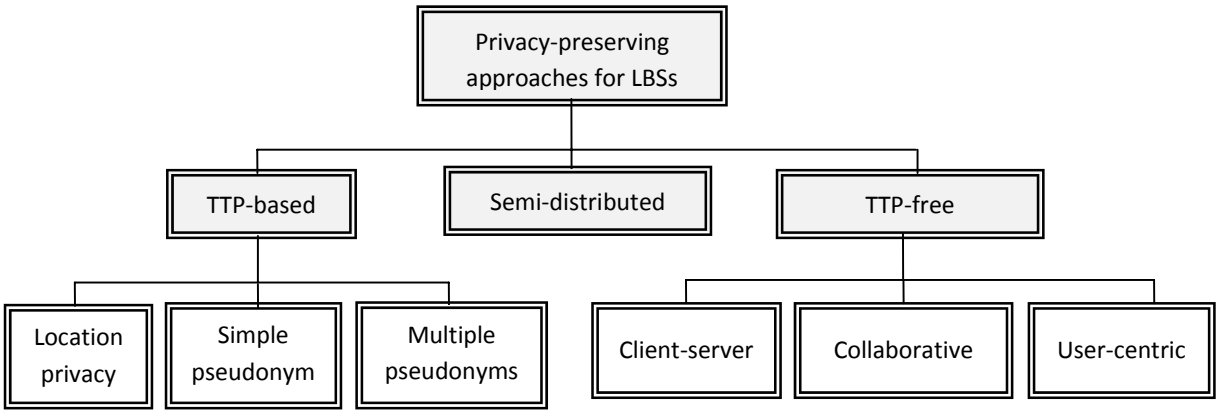


Figure 3 summarizes the typical privacy and efficiency properties for the different categories of recent cryptographic schemes for privacy-preserving LBS services. Finally, another stream of research concerns *Location-Based Access Control* (LBAC) systems (Denning & MacDoran,

1998; Bardram et al, 2003; Zhang et al, 2005; Al-Muhtadi et al, 2006; Cho et al, 2006; Ardagna et al, 2007; Atallah et al, 2007; Saroiu & Wolman, 2009), that authenticate the physical location of a network entity before granting access to a service.

Figure 3. The basic privacy models and their (typical) core properties

Properties / Models	Trust assumptions	Identity privacy	Location privacy	Unlinkability	Privacy vs accuracy	Client efficiency	LBS Server efficiency	Examples from academic literature
TTP spatial k-anonymity	√	X	√	X	√	√	√	Gruteser & Grunwald, 2003; Gedik & Liu, 2005; Mokbel et al, 2006
TTP cloaking / obfuscation	√	X	√	X	√	√	√	Ardagna et al, 2007; Khoshgozaran & Shahabi, 2007; Hengartner, 2008
Simple pseudonym	√	√	X	X	X	√	√	Hauser & Kabatnik, 2001; Rodden et al, 2002; Konidala et al, 2005; Candebat et al, 2005
Multiple pseudonyms	√	√	X	√	X	X	√	Jorns et al (2005, 2007); Kolsch et al, 2005
Semi-distributed protocols	√	X	√	X	X	√	X	Kohlweiss et al, 2007; Zhong et al, 2007; Zhong & Hengartner (2008,2009)
PIR protocols	X	X	√	√	X	X	X	Ghinita et al (2008, 2009); Olumofin et al, 2009
Collaborative protocols	X	X	√	X	√*	X	√	Solanas & Balleste* (2007,2008); Zhong et al, 2007; Ardagna et al, 2009;
User-centric	X	X	√	X	X	X	√	Sun et al, 2009; Yiu et al, 2009

TTP-BASED APPROACHES

Location privacy

Typically location privacy is suitable for applications where the resolution of the location information can be reduced without severely degrading the service offered. For example, in order to protect location privacy, the user's location information submitted to the LBS provider is *cloaked* by a TTP i.e., by sufficiently reducing its resolution in terms of space and/or time (e.g., Khoshgozaran & Shahabi, 2007). By adapting the well-known *k*-anonymity technique (Sweeney, 2002) to the spatial domain, the most popular approach has been to reduce the resolution of location information to an anonymity set of *k* users (e.g., Gruteser & Grunwald, 2003; Gedik & Liu, 2005; Mokbel et al, 2006). Or, location data may be perturbed/obfuscated by the TTP (e.g., Duckham & Kulik, 2005; Hoh & Gruteser, 2006; Ardagna et al, 2007; Lin et al, 2009) without severely degrading the offered service.

A cryptographic way to control access to location information, using simple public-key cryptography, is described in (Gajparia et al, 2004). In the proxy-based approach of Gajparia et al (2004), an online Location Information Preference Authority (LIPA) is a trusted party that

examines user-chosen constraints and makes decisions about the distribution of location information (LI) and accompanying constraints to the entity requesting the location information (i.e., an LBS provider or other users). To ensure that only the LIPA has access to users' LI and constraints, an online Location Gatherer (LG) constructs an LI token that contains the LI and constraints encrypted with the public key of the LIPA. The token also contains information which helps to identify the LI subject and the LIPA (from a list of available LIPAs). For access control, all information is digitally signed by the LG. Once the LBS provider wishing to use LI receives an LI token, verifies the signature, establishes the identity of the LI subject and submits the token to the appropriate LIPA, who checks if access to the LI is permitted for the requesting LBS provider.

A hardware-based approach for location privacy is proposed in (Hengartner, 2008), where a Trusted Computing (TC) module receives the user's location data encrypted with its public key. The module then queries the LBS database to retrieve the requested information, but for privacy it hands over location information to the LBS platform only if the platform is configured to implement an outlined privacy policy (e.g., the LBS does not learn location information). The module then signs and encrypts the LBS's response with the public key of the cellphone operator. In (Hengartner, 2008) software-based active attacks (i.e., query modification/injection) by the LBS provider are thwarted by using a *secure logging* approach, i.e., an auditing mechanism that stores logging information to the trusted module.

Evaluation remarks. Schemes within this category typically achieve adequate access control assurances, since the user identity does not necessarily need to be secret (in fact, a pseudonymous LBS service could be supported); Or, as a privacy enhancement, users could be totally anonymous (at the expense of access control and/or accountability). Solutions based on location *k*-anonymization and spatiotemporal perturbation/obfuscation usually introduce a *privacy vs accuracy* trade-off and may not be able to meet the high position accuracy requirements of modern location tracking applications (Gruteser & Liu, 2004; Kulik, 2009). Furthermore, in *k*-anonymous protocols, a sufficiently large number of users must be connecting at the same time to the same service. When user density is low, other solutions need to be examined (e.g., PIR-based privacy, or location perturbation/obfuscation). In addition, most of the above approaches typically involve sporadic queries that are executed at an LBS provider and may not be able to protect continuous paths (Ghinita et al, 2008; Bettini et al, 2009).

Another disadvantage that applies in general to TTP-based approaches is that the TTP is both a bottleneck and a single point of attack (Ghinita et al, (2007, 2008); Solanas & Balleste, 2008): the TTP must process all location updates of all the system users; in addition, if an adversary gets access to the TTP's data, then the privacy of system users is destroyed. Furthermore, users are not necessarily satisfied about completely trusting proxies and intermediaries (Rebollo-Monedero et al, 2009). Although TTPs are considered trusted entities, in reality, if a single authority is able to trace a user's identity, this power may be abused and privacy be violated; or, active (impersonation) attacks against system users could also be possible. Where there is only a

single TTP, a trusted module could also be used to implement this trust, as in (Hengartner, 2008). On the other hand, the need for the acquisition of a specialized tamper-resistant module could also be seen as a drawback.

Current research focuses on approaches for *k*-anonymity and cloaking techniques that capture strong privacy guarantees while maintaining high data accuracy (e.g., Hoh et al, 2007), as well as on location privacy approaches that reduce (e.g., Zhong & Hengartner, (2008, 2009)) or completely remove trust from any internal or external system entity (e.g., Solanas & Balleste, (2007, 2008); Ardagna et al, 2009).

Identity privacy with pseudonyms

This sub-category includes cryptographic methodologies based on pseudonyms to destroy the link between location information and the user identity. Specifically, in order to preserve privacy in location-based services that cannot be accessed anonymously (i.e., they require identification) but do not require a true identity either (Beresford & Stajano, 2003; Candebat et al, 2005). An advantage of the identity privacy setting is that location information can be kept as accurate as possible, which is often required in LBSs applications that offer high-quality information services (Gruteser & Liu, 2004; Kulik, 2009), but the link to the real identity of a user is protected, in order to establish untraceability (Pfitzmann and Kohntopp, 2000).

The pseudonym-based approach was first used in (Hauser & Kabatnik, 2001) for a people-locator service and is based on public-key cryptography. In (Hauser & Kabatnik, 2001) a watcher digitally signs a query concerning a target and submits the signed query to the LBS provider. The query is accompanied with an authorization certificate, issued by the target, i.e., digitally signed by the target's private signature key, where the corresponding public key plays the role of the target's pseudonym for the specific service and is used as a reference with which the watcher can address the target. The certificate also lists the explicit permissions for the location data of the target. The watcher does not ever learn the target's pseudonym, as the pseudonym is encrypted with the public key of the LBS provider, who is also not aware of the real identity of the targets.

Another early approach was proposed in (Rodden et al, 2002). In their security model for location-tracking services, the user generates a random number X to be used as a pseudonym for communicating with an LBS provider T, and registers X to a trusted broker as (T, $Enc(K_T, X)$) where K_T is a symmetric encryption key provided by T to prevent unauthorized access to location information by other providers. The pseudonym X is used to communicate with T, only for the duration of the provision of the service. At any given time, a user may have a number of active pseudonyms. At some time the provider T queries the broker to find out the location of the user X. The broker is trusted on not revealing the real identity of the user. The LBS provider can keep querying the user's location, until the user decides to change pseudonym. All information is symmetrically encrypted, in order to deal with external observers. As shown in (Rodden et al, 2002), for people locator services the pseudonym can be securely passed to a group of watchers that are approved by the user, while the broker is trusted on managing group membership.

Another scheme (Candebat et al, 2005) for point-of-interest LBSs assumes a proxy-based PKI and employs *identity-based encryption*[1] (Baek & Zheng, 2004) and threshold cryptographic principles[8]. For privacy preservation, each user owns one private key for decryption and signatures, while multiple pseudonyms are used as the corresponding public keys to communicate with the LBS provider. In addition, each user's private key is split between the user and an online *semi-trusted* mediator (SEM) who simplifies key management by validating the user credentials and acts as a proxy to request an LBS service on behalf of the user, under the different pseudonyms. The SEM carries out cryptographic operations in conjunction with the user to decrypt messages and generate identity-based signatures. The SEM assists the decryption (respectively, signing) process provided that the security credentials of the recipient (signer) have not be revoked. As a result, this mediated architecture makes credential revocation easier.

Evaluation remarks. Approaches that combine simple pseudonyms with exact location information do not capture a strong notion of privacy. For example, an adversary (e.g., it could the provider or an adversary that analyses traffic) could trace the identity of a query by linking the physical location data to a particular individual. In addition, untraceability by itself may not be enough: if a set of distinct credentials can be linked to the same anonymous entity, then a customer profile can be built and this is considered a privacy violation. In this case, and in order to completely undermine privacy, the adversary will only have to trace one particular link of this chain (e.g., after the customer uses a credit card, with use of a camera, physical pursuit etc).

Finally, research for identity privacy in the LBS context may have something to gain from the literature on *anonymous credentials* (Camenisch & Lysyanskaya, (2001,2002,2004); Camenisch et al, 2006; Belenkiy et al, 2008), which build on top of early works on pseudonym systems (Chaum, 1985; Lysyanskaya et al, 2000). Here, a user proves to a service provider possession of a set of credentials without revealing anything other than this fact. However, state-of-the-art protocols for anonymous credentials in their present form induce high costs for both the user and servers, and so they should be carefully evaluated before adoption in the LBS context.

Multiple pseudonyms for unlinkability

As the use of traditional pseudonymity with long-term pseudonyms is not enough for strong privacy (Beresford & Stajano, 2003), sometimes privacy can be enhanced by destroying the link between successive user positions, mainly from the point of view of the LBS provider (Beresford & Stajano, 2003; Jorns et al, 2007). The pseudonym systems of the previous category were not designed with unlinkability as a key goal, although they could be modified to provide it (e.g., Hauser & Kabatnik, 2001; Rodden et al, 2002).

The provision of unlinkability is also closely related to an aspect of privacy that is also referred to as *path privacy* or *historical privacy* (Beresford & Stajano, 2003; Gruteser et al, 2004; Ardagna et al, 2007; Bettini et al, 2009; Ghinita, 2009). 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 have also been called as *continuous LBSs* (Kulik, 2009).

In (Beresford & Stajano, 2003) it was argued that access to an LBS can be controlled by using a validated list of multiple, frequently changed pseudonyms that conceal the actual identity of a node. The use of untraceable and unlinkable pseudonyms to support privacy has also been extensively studied in location-aware applications for vehicular ad-hoc networks (VANETs) (e.g., Raya & Hubaux, (2005, 2007); Sampigethaya et al, 2005; Rahman & Hengartner, 2007; Sun et al, 2007). For example in (Raya & Hubaux, (2005, 2007)), these pseudonyms are untraceable and unlinkable public keys for verifying digital signatures. Such solutions, if adopted in the LBS context, should be carefully designed to avoid increasing the complexity of user registration and the computational, storage and communication cost for the handheld devices.

The scheme in (Kolsch et al, 2005) considers a notification-based LBS, where the user gets allergy warnings based on weather conditions in the environment. Communication is encrypted, authenticated and integrity-protected with public-key encryption and signatures. A trusted location broker mediates between the LBS provider and the mobile operator. For every new LBS, a user creates a “fresh” pseudonym to interact with the operator and a different pseudonym to interact with the LBS provider, while each pseudonym is of the form of a public/private key pair for encryption and signature. For untraceability, signature data are never sent to the LBS provider; instead, warnings are sent to the user through an anonymous communication channel, opened by the user in cooperation with the broker. Mutual authentication between the LBS and the broker is performed through a *zero-knowledge proof* system[2]. The broker can link the different pseudonyms together and is aware of the user's location, but cannot trace the user. On the other hand, the mobile operator is aware of the true identity of the user and his/her location, but cannot learn the specific LBS that was used by the user.

In the people-locator service of (Jorns et al, 2007), users employ different transaction pseudonyms for different service requests, and these pseudonyms cannot be linked to each other by the LBS provider, although linking can be done by a trusted network operator. Watchers first establish a trust relation with a target, and then the network operator acts as a trusted proxy that assists users in pseudonym management and credential generation, and mediates initial handshaking between watchers and targets. Specifically, the operator, which shares a secret pw_A with a user A (the watcher), sends to A the initial element of a *hash chain* of elements (Lamport, 1981) i.e., an anchor value $h_0 = anchor_B$ that corresponds to the location of the target user B. Then, the list of n pseudonyms for a watcher A that subscribes to B's location[3] are generated by hashing the previous chain element together with the shared secret pw_A, that is: $h_i = HMAC(h_{i-1}, pw_A), 1 \le i \le n$, where HMAC could belong for example to the SHA family of functions (NIST, 2008). These pseudonyms are unlinkable by the LBS provider and are used by the watcher as authentication tokens to ask the location of the target from the provider. The provider will forward a token to the operator, who will act as a broker and return the target's location. The scheme is a successor of PRIVES (Jorns et al, 2005; Bessler & Jorns, 2005).

Evaluation remarks. The mere use of multiple pseudonyms is not always sufficient for location privacy against a global observer that performs traffic analysis (Beresford & Stajano, 2003; Gruteser & Grunwald, 2003; Gruteser et al, 2004). For example, when the true identity could be directly or indirectly inferred by the location of the person, or when the adversary is able to correlate historical information i.e., spatial and/or temporal information about a mobile user (Beresford & Stajano, 2003; Raya & Hubaux, 2005; Buttyan et al, 2007; Bettini et al, 2009) in order to link two or more user transmissions. As a result, for path privacy a user may have to update a pseudonym at points where the spatial and temporal resolution is decreased e.g., within a MIX zone[4] (Beresford & Stajano, 2003; Buttyan et al, 2007; Freudiger et al, 2009) or a junction (Gruteser et al, 2004; Burmester et al, 2008). Indeed, most related work for historical/path privacy attempts to decrease the spatiotemporal information that is revealed to an adversary, between successive locations (e.g., Beresford & Stajano, 2003; Gruteser & Grunwald, 2003; Gruteser et al, 2004; Buttyan et al, 2007; Hoh et al, (2007, 2008); Freudiger et al, 2009; Bettini et al, 2009; Ghinita, 2009). We refer the reader to (Ardagna et al, 2007; Bettini et al, 2009´Ghinita, 2009) for a survey and assessment of recent approaches for path privacy preservation in location-based services. Other attacks include a compromised LBS provider that links two different pseudonyms to the same set of personal preferences at the service level (Beresford & Stajano, 2003), or tracing/linking that may take place at the physical or MAC layers (Gruteser & Grunwald, 2005; Rasmussen & Capkun, 2007).

We also note that there may be cases where unlikability may be impossible or undesirable, as in reputation-based systems (Wakeman et al, 2007). Or, LBS providers may need to link information for supporting infotainment or value-added, personalization services. In such cases, the linkage may or may not necessarily require tracing the real identity, e.g., the simple pseudonym approach could be used instead (Duckham & Kulik, 2006).

A final remark is that solutions based on both simple and multiple pseudonyms can be counted as TTP-based: in reality, in order to establish accountability or non-repudiation a trusted system entity may have to keep a record of the issued pseudonyms, location data and/or the corresponding real identity of the device[5].

THE SEMI-DISTRIBUTED SETTING

At a high level, the semi-distributed approach can be seen as a trivial extension of the TTP-based privacy model. It relaxes trust assumptions by not requiring full trust on a single party but instead moving trust to a suitable set of (typically, two or more) non-colluding entities. In addition, we choose to include in this category schemes which employ one or more third parties that are trusted on some (but not all) aspects of user privacy and/or security.

For example in (Zhong & Hengartner, (2008, 2009)), a distributed *k*-anonymity protocol is proposed, and privacy is based on the existence of a set of servers, each deployed by a different organization (i.e., they are assumed not to collude). A number of *location brokers* track the location of a different subset of registered users. Each location broker learns the location and

number of users that have registered with this broker but not the total number of users in this cell, as some users may have been registered with another broker. Furthermore there is a number of secure *comparison servers*, where a server informs the user whether there are at least *k* users who have registered the user's current cell as their current location across all brokers. Similarly, the comparison server does not learn neither the user's location, nor the exact number of users in a cell. The solution in (Zhong & Hengartner, 2008) uses the *additively homomorphic* property of several probabilistic public key encryption schemes[6] (e.g., Okamoto & Uchiyama, 1998; Paillier, 1999), where for example there is an operation $\oplus$ on the message space and an operation $\otimes$ on the cipher space, such that the "product" of the encryptions equals the encrypted "sum" of the messages, i.e., $E(M_1) \otimes E(M_2) = E(M_1 \oplus M_2)$. To learn whether there are *k* users in his/her query area, the user interacts with each authoritative location broker and obtains the numbers of registered users within the user's cell, encrypted with the public key of the comparison server. The user uses the additively homomorphic property of the encryption scheme to calculate the encrypted sum of numbers, and randomizes (re-encrypts) the encrypted results, in order to hide the total number of users from the comparison server. Finally, the user interacts with the comparison server to learn whether this number is greater than *k*, without the server ever learning or infering *k*. In (Zhong & Hengartner, 2009) this is achieved by using a protocol (Blake & Kolesnikov, 2004) based on the *oblivious transfer* primitive[7] (Rabin, 1981).

Another scheme (Kohlweiss et al, 2007) assumes the existence of an online proxy *P*, an offline trustee *T* (an independent party without any commercial interests) and a number ℓ of LBS providers, whith ℓ being a security parameter. The proxy, who has a financial relationship with the user, knows the user's location and mediates between the user and the LBS providers. In a data retrieval phase, the proxy runs a protocol with every LBS provider, and obtains an encrypted result. Using the additively homomorphic property of the generalized Paillier cryptosystem (Damgard & Jurik, 2001), the proxy combines the partial messages into a single encrypted result, which only the user (and not the proxy) is able to decrypt. The assets that are protected are: the user's location (against the LBS providers), the user's subscription (against the proxy) and the database contents of the providers (against the user and the proxy), apart from the location-based information that the user retrieves. By introducing the privacy trustee, the protocol assures that the LBS providers do not even learn whether a user is accessing their service or not, even if they cooperate with the proxy; this privacy assurance was named *service unobservability* (Kohlweiss et al, 2007). The above properties are achieved at the cost of using a number of cryptographic primitives, including zero-knowledge proofs[2], oblivious transfer[7], homomorphic encryption[6], and 3-out-of-3 *threshold encryption*[8]. However, the protocol is efficient for the mobile users, since only a single public-key decryption per user is required.

In the Louis privacy-preserving protocol for buddy-tracking applications (Zhong et al, 2007) Alice considers Bob nearby if he is within a circle of some radius centered around Alice. Trent is a semi-trusted third party that helps Alice and Bob decide whether they are nearby, but Trent does not learn any other location information concerning Alice or Bob. The only thing Trent learns is Alice's identity. The Louis protocol also exploits the homomorphic property of the

Paillier public-key cryptosystem (Paillier, 1999). Alice encrypts and sends her coordinates to Bob, who "adds" his coordinates (using the additively homomorphic property of Paillier), and randomizes the result with a salt that only Trent can remove (i.e., the salt is encrypted with Trent's public key). The protocol terminates when Trent notifies Alice whether Bob is nearby.

Evaluation remarks. Semi-distributed trust assumptions are considered weak as long as the set of non-colluding entities is sufficiently large, as in (Zhong & Hengartner, (2008, 2009)), or when their interests is colluding. Note that the set of these entities can be well-known and so the risk of trusting a dishonest entity may be small (Rebollo-Monedero et al, 2009). Related to this is the notion of a *semi-honest* (also known as *honest but curious*) authority, proposed in the context of privacy-preserving data mining by Pinkas (2002), under a less conservative threat model: semi-honest adversaries are legal participants that follow the protocol specification, behave the way they are supposed to, do not collude or sabotage the process, but instead try to learn additional information given all the messages that were exchanged during the protocol. On the other hand, the assumption of a semi-honest adversary has also been seen as a strong assumption (e.g., Kargupta et al, 2007). Indeed, if the (assumingly, non-colluding) authorities misbehave and collude, then deprivatisation of a user privacy is trivial. For these reasons it is preferable that third parties are trusted on some (but not all) aspects of user privacy.

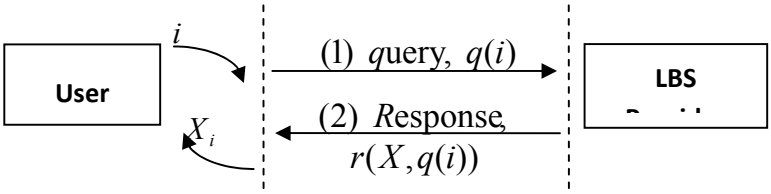
TTP-FREE SCHEMES

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., Solanas & Balleste, (2007, 2008); Ghinita et al, (2007, 2008); Zhong & Hengartner, (2008, 2009); Solanas et al, 2008; Ardagna et al, 2009). Such schemes relax or completely remove the need for unrealistic trust assumptions. Three main subcategories are the client-server approach, the collaborative approach and the user-centric approach. In most TTP-free approaches, it is implicitly assumed that mobile clients autonomously compute their own location (e.g., with GPS positioning) or else unnecessary trust assumptions should have to be made.

Client-server communication

Cryptography can help towards building client-server LBS architectures that are TTP-free. The use of identification mechanisms based on zero-knowledge proofs (Goldreich et al, 1991), was first discussed in (Duckham & Kulik, 2006) as a promising step towards balancing privacy with access control in location-aware computing. Since then, a number of privacy-preserving schemes have been proposed (e.g., Hengartner, 2006; Ghinita et al (2008, 2009); Ghinita (2008, 2009); Olumofin et al, 2009), and most of them are based on the theoretical work on *Private Information Retrieval* (PIR) (Chor et al, 1995; Kushilevitz & Ostrovsky, 1997; Chor & Gilboa, 1997). Schemes of this category introduce a new privacy model, depicted in Figure 4.

Figure 4. A client-server model for privacy in LBSs



The new location privacy model is described in (Ghinita et al, 2008), building upon the *computational PIR* (cPIR) protocol introduced in (Kushilevitz & Ostrovsky, 1997). Specifically, the LBS provider holds a database that is coded as an n-item ordered array $X[1..n]$. The query of a user is transformed to a query-by-index, i.e., the user wants to easily retrieve the i-th item $X[i]$ in a way that is computationally infeasible for the LBS provider to find out the value of i (in the LBS setting, this could reveal for example the user's location). When initiating a query, the user creates an encrypted query object $q(i)$; the LBS provider computes privately, using a mathematical transformation, the result $r(X, q(i))$ and sends the result back to the user. An extension of PIR, *Symmetric PIR* (SPIR) (Mishra & Sarkar, 2000) establishes database secrecy by assuring that no information, other than what is relevant to the current location, is leaked to the querying user. At a high level, the SPIR primitive can be seen as a generalization of the oblivious transfer primitive (Rabin, 1981) -please also refer to (Olumofin et al, 2009) for an overview and historical perspective of the PIR approach.

In (Ghinita et al, 2008) PIR is used by a client to query an LBS provider for a nearby point of interest. The cost in (Ghinita et al, 2008) is acceptable by letting the user retrieve a small fraction of the LBS database. The approach was extended in (Ghinita et al, 2009), where the user locations are hidden inside a cloaked region, and then a PIR protocol is run between the client and the LBS provider in order to disclose an optimally small number of points-of-interest, for database protection.

The hardware-based architecture in (Hengartner, 2006) uses Trusted Computing (TC) technologies to ensure that a compromised LBS provider does not access user location information, and a PIR technique to ensure that the user only learns information about his/her current location and that the provider cannot infer the location of a user by observing which location-specific data sets are retrieved by the user. The PIR algorithm is implemented within the TC module, at the LBS provider's premises. The TC module also acts as a trusted proxy and (securely) obtains the user's location data, submits queries and forwards the responses, encrypted with the user's public key.

Evaluation remarks. PIR-based approaches provide the strongest privacy assurances with the weakest trust assumptions, as it is computationally untractable to reveal the link between the user and location data, while on the other hand the user only learns information relevant to his/her

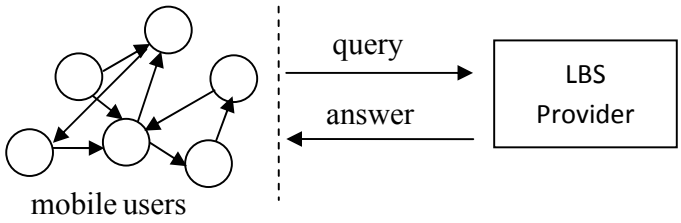
location. In (Ghinita et al, 2008; Ghinita, 2009) it is also shown how the PIR framework, in contrast to *k*-anonymous cloaking, could protect LBS users against correlation attacks (path privacy), by not revealing any spatial information.

A challenge is to design computationally efficient and practical solutions that reduce the processing overhead of the early schemes, in view of the low-computing and resource-poor end devices, and some recent approaches seem promising towards this direction (e.g., Ghinita, 2008; Olumofin et al, 2009; Ghinita et al, 2009). Such approaches consider a tradeoff between privacy and computational overhead in order to improve performance in PIR-based LBS queries.

The collaborative setting

The fully distributed or collaborative privacy model does not rely on centralized trusted entities, but trust is distributed among system peers that may also form ad-hoc networks and collaborate to achieve privacy against a set of untrusted entities (e.g., other mobile peers, the LBS provider, or even the network operator (Solanas & Balleste (2007, 2008); Ardagna et al, 2009).

Figure 5. A distributed model for privacy in LBSs



In the TTP-free approach of Solanas & Balleste (2007, 2008) a user U interacts with $k-1$ companions, requests their location information and computes a *k*-anonymized location, as the centroid of the current locations in the cloaked area (a similar approach was also taken in (Ghinita et al, 2007), where users also shared their location prior to computing a *k*-anonymized location). In (Solanas & Balleste, 2008), the masked location is then sent to the LBS provider and to U's companions. To deal with the threat that a malicious user learns the exact location of her/his companions and violates their privacy, an extended second scheme is also proposed in (Solanas & Balleste, 2008). The scheme exploits the additively homomorphic property of probabilistic public-key encryption. Specifically, users possess the public key of an untrusted LBS provider, signed by a Certificate Authority. Then, a user U initiates a location request in cooperation with a set of $k-1$ companions: each companion encrypts and sends back to U its encrypted location coordinates, then U "combines" the encrypted coordinates and computes the encrypted aggregate. In this second scheme, stronger privacy is established under the assumption that the users will not trust each other (Solanas & Balleste, 2008). In this version, location privacy is guaranteed even against collisions of other peers with the LBS provider.

Another scheme, the Lester scheme in (Zhong et al, 2007) implements a nearby-friends service in a collaborative manner. In the Lester scheme, users learn information about their

friend's location only if this friend is actually online. Specifically, Alice and Bob execute a secure two-party protocol and jointly compute, in two communication steps, whether their positions are near to each other, without learning their exact positions. The protocol uses the homomorphic encryption property of a variation[6] of the ElGamal scheme (Cramer et al, 1997).

Another collaborative *k*-anonymity scheme for hybrid network architectures is presented in (Ardagna et al, 2009), where the threat model views the network operator and other peers as potential adversaries. The scheme considers a hybrid network architecture, where 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, a user *u* belongs to a cellular network and is able to receive and send signals to a cellular network operator *o* in order to access services provided by an Internet-connected LBS provider. The scheme in (Ardagna et al, 2009) works as follows: during a key setup phase, the sender *u* establishes a symmetric key *SK* with *s*. At some time in the future, *u* specifies a message *M* and a preference *k*, then splits *M* in *k* packets $\{m_1, m_2, ..., m_k\}$, encrypts each packet m_i with the key *SK* and then appends a message identifier *mid*, that is: $\overline{m}_i = E_{SK}(m_i) \,||\, mid$, for each $i \le k$. The user then randomly selects $k-1$ peers in his/her range, and sends a different packet to each of them. Packets are distributed to the neighboring peers using a random forwarding distribution algorithm (Ardagna et al, 2009). Eventually the peers will forward the packets to the server *s* through the operator *o*, who will see packets from *k* different users, so *k*-anonymity is preserved. The server *s* can also reply to *u*, by encrypting a message reply with the key *SK*, and then transmiting the result to all *k* peers, through *o*. Only *u* will be able to receive and decrypt the message.

Evaluation remarks. With collaborative protocols privacy is based on much less strong assumptions (even in cases when users trust each other), while the bottleneck of the TTP-based approaches is removed. In addition, such protocols can achieve higher fault tolerance and resilience against privacy and security attacks. However, the cost for the above advantages is usually higher communication and computation for the low computing, resource-constrained system clients.

User-centric model

Some very recent approaches employ cryptographic methods in order to give the user control over who is allowed to access her/his location information, and in some cases with which granularity. Typically, such properties are useful in people-locator services (e.g., Cox et al, 2007; Sun et al, 2009; Yiu et al, 2009). Since no trust assumptions concerning privacy are made, protocols of this category can be considered as TTP-free.

For example in (Sun et al, 2009) each target defines and controls a group of entities that are allowed to access its encrypted location information, and group decryption keys are established and distributed to the members of the group. The proposed system also allows the user to define the granularity with which different group members have access to location information. For

relatively small groups, the user will generate her/his own location information, encrypt it and then directly distribute the keys to the other members, by running a *group-key management* protocol (e.g., Rafaeli & Hutchison, 2003; Sun et al, 2009) such as Diffie-Hellman group key exchange (Diffie & Hellman, 1976; Kim et al, 2000).

In (Yiu et al, 2009) users decide which trusted friends can perform spatial queries on their location data, using an untrusted LBS provider. A user transforms her/his spatial information using conventional (e.g., AES) symmetric encryption. A query is evaluated through a distributed, multiple round protocol between the user and the LBS provider.

Evaluation remarks. Scalability is the key factor determining whether schemes of this category will flourish. Current schemes impose high costs in terms of computation and communication. For large groups, it seems inevitable that there will also be a third party, trusted or semi-trusted, that at a minimum will handle group management. In (Sun et al, 2009) for example, when larger groups are considered, the user needs to build a trust relationship with a server of the network. In (Sun et al, 2009) the user encrypts and uploads the location information into a Location Server (LS); on demand, the LBS provider requests the location from the LS and sends it to a trusted Group Server who manages the group keys (e.g., key distribution, re-keying and key updating) by using a *hierarchical key tree* structure (Sun et al, 2009). The idea is to hierarchically conceal location data with different keys, where each key corresponds to a particular granularity, and distribute the decryption keys to group members with the necessary permissions.

LOCATION-BASED ACCESS CONTROL

Another increasingly important issue for location-aware security services, is how to authenticate the physical location of a network entity before granting access to a service or resource (e.g., Zhu et al, 2003; Bardram et al, 2003; Al-Muhtadi et al, 2006; Cho et al, 2006; Atallah et al, 2007; Saroiu & Wolman, 2009). The notion of Location-Based Access Control (LBAC) is not new (Denning & MacDoran, 1998) and in the recent past a number of cryptographic mechanisms have been proposed to facilitate LBAC (e.g., Zhang et al, 2005; Cho et al, 2006; Al-Muhtadi et al, 2006). With context authentication, there are schemes that authenticate either the exact location information (e.g., Zhang et al, 2005) or an approximation of location information, such as the areas enclosed within a set of access points (e.g., Cho et al, 2006).

In (Zhang et al, 2005) for example, LBAC is established among static sensor nodes in a distributed sensor network, and location is used as a node's identity when communicating with other nodes. In (Zhang et al, 2005) sensor nodes are localized by mobile, GPS-enabled robots who securely pass to each sensor a location-based key (LBK) i.e., a symmetric key that corresponds to a node's geographic location. Based on the principle of identity-based public-key cryptography[1], LBKs are later used to derive public keys and perform mutually authenticated key establishment with neighboring nodes, while security of the key establishment is based on the bilinear Diffie-Hellman assumption (Boneh & Franklin, 2001).

The work of Al-Muhtadi et al (2006) for pervasive computing environments (PCEs) introduces *location-based encryption*: resources are stored in an encrypted form and they can be decrypted only when the requestor is at the correct location. In (Hengartner, 2006), it is argued that location-based encryption can be used for implementing a people-locator LBS, where the LBS provider could encrypt its information with location-dependent symmetric keys and make the encrypted data publicly available by using a distributed hash table, while the network operator would provide decryption keys to customers based on their current location. In (Atallah et al, 2007) a key management technique for geo-spatial access control is described, where the access control policy assigns to a user a specific geographic area, and every user obtains access only to her/his area of information.

In (Cho et al, 2006) access to a WLAN is granted only if a mobile node is located within the shared areas covered by multiple access points (APs). The protocol authenticates location claims and establishes shared session keys for each node/AP pair using Diffie-Hellman key exchange. Finally in (Saroiu & Wolman, 2009) the identities of mobile clients and the local infrastructure components (e.g., APs) are represented by public keys: clients send to the infrastructure a signed request for a location proof, to enable a mobile location-aware application or service. The AP validates the request, then signs and sends to the client a location proof with a current timestamp.

Evaluation remarks. Schemes of this category give an emphasis not on privacy, but on security for access control. Clearly, privacy can be challenging when exact locations are used, or when users are granted access rights to a specific area. Under this view, the privacy of mobile clients in LBAC systems could be enhanced with pseudonym-based techniques. Future research could also build on recent results for TTP-free and collaborative solutions that reduce the trust assumptions of third parties. The goal may be to fill the need for high-quality LBAC systems while establishing privacy for the end users. Issues and challenges for privacy in LBAC systems are also given in (Ardagna et al, 2007; Ardagna & Cremonini et al, 2009; Saroiu & Wolman, 2009).

CONCLUSION

Current research focuses in the inherent *trade-off* between user privacy and access control in LBS applications: 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 from unauthorized access. This paper surveyed the state-of-the-art in cryptography-based solutions for achieving privacy-preservation in LBS services. Specifically, we categorized current research into three groups, based on the trust assumptions between parties involved in LBS schemes: TTP-based approaches, semi-distributed schemes, and TTP-free approaches. For each category, we reviewed and evaluated the current literature in terms of privacy, security and efficiency.

ENDNOTES

1. With identity-based encryption, first proposed in (Shamir, 1984), key management is simplified as users are not required to exchange digital certificates of their public keys, but instead they are allowed to use their identity as their public key.

2. Such proofs are prover-verifier interactive protocols, where the prover proves a statement to the verifier and the verifier learns nothing from the prover that he could not learn by himself, apart from the fact that the prover knows the proof (Goldreich et al, 1991).

3. As noted in (Jorns et al, 2007), a user may also subscribe as a watcher to his/her own location (e.g., in a GPS navigation service).

4. Analogously to MIX nodes in communication networks (Chaum, 1981), a MIX zone is a spatial area where a user can enter and exit anytime, in a way that it is not possible for an observer to link a user position *before* entering the zone, with a position *after* exiting the zone.

5. In a scheme for VANETs (Rahman & Hengartner, 2007), for example, each public key (pseudonym) is validated by a system entity, using *blind signatures* (Chaum, 1983) (the cryptographic equivalent of signing carbon paper-lined envelopes). The issued certificate also contains the real identity of the vehicle, encrypted with the public key of a trusted third party.

6. The idea was first conceived in the context of privacy-preserving Internet elections (Cramer et al, 1997). The scheme in (Cramer et al, 1997) uses a homomorphic variation of the ElGamal encryption scheme (ElGamal, 1985), with addition as group operation of the message space. Specifically, a message *m* is encrypted by choosing a random number $r \in Z_q$ and computing two values $(R, S) = g^r, y^r g^m$, where $y = g^s$ is the public key of the receiver, g is generator of Z_q and all operations are modulo *p*. Encryption functions of this type also allow for *universal re-encryption* (Jakobsson et al, 2004), e.g., randomization by calculating (R', S') where $R' = Rg^{r'}$ and $S' = Sy^{r'}$, where $r' \in Z_q$ is a random number.

7. In a trivial example of the oblivious transfer primitive (ElGamal, 1985), Bob has two secrets S_0, S_1 and Alice is able to learn exactly one secret S_i, while Bob will not know number i, i.e, which of the two secrets Alice got.

8. In a typical setting, a set of system entities share a private key in a threshold public-key encryption system (Desmedt, 1994), and there is only one public key corresponding to the shared private key. The user submits an encrypted message with the public key of the authorities, and only a qualified set of honest entities are able to combine their shares and decrypt the message.

REFERENCES

Al-Muhtadi, J., Hill, R., Campbell, R., & Mickunas, M. (2006). Context and location-aware encryption for pervasive computing environments. In *Proceedings of the 4th annual IEEE international conference on Pervasive Computing and Communications Workshops* - PERCOMW '06 (pp. 283–288). IEEE Computer Society, Washington, DC, USA.

Ardagna, C.A., Cremonini, M., Capitani di Vimercati, S. D., & Samarati, P. (2009). Access control in location-based services. In *Privacy in Location-Based Applications* (pp. 106–126). Lecture Notes in Computer Science, 5599, Springer Berlin / Heidelberg.

Ardagna, C.A., Cremonini, M., Capitani di Vimercati, S. D., & Samarati, P. (2007). Privacy-enhanced location-based access control. In M. Gertz & S. Jajodia (Ed.), *The Handbook of Database Security: Applications and Trends* (pp. 531-552). Springer-Verlag.

Ardagna, C.A., Jajodia, S., Samarati, P. & Stavrou, A. (2009). Privacy preservation over untrusted mobile networks. In C. Bettini, S. Jajodia, P. Samarati, & S. Wang (Ed.), *Privacy in Location Based Applications* (pp. 84-105). Lecture Notes in Computer Science, 5599, Springer Berlin / Heidelberg.

Atallah, M., Blanton, M., & Frikken, K. (2007). Efficient techniques for realizing geo-spatial access control. *ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security* (pp. 82–92). ACM, New York, NY, USA.

Baek, J., & Zheng, Y. Identity-based threshold decryption. In F. Bao, R. Deng, & J. Zhou (Ed.), *Public Key Cryptography - PKC 2004* (pp. 262-276). Lecture Notes in Computer Science, 2947, Springer Berlin/ Heidelberg.

Bardram, J., Kjær, R., & Pedersen, M. (2003). Context-aware user authentication–supporting proximity-based login in pervasive computing. In *5th International Conference on Ubiquitous Computing - UbiComp 2003* (pp. 107–123). Lecture Notes in Computer Science, 2864, Springer Berlin / Heidelberg.

Belenkiy, M., Chase, M., Kohlweiss, M., & A. Lysyanskaya (2008). P-signatures and noninteractive anonymous credentials. In *Proceedings of the 5th conference on Theory of Cryptography* (pp. 356–374). Springer-Verlag.

Beresford, A.R., & Stajano, F. (2003). Location privacy in pervasive computing. *IEEE Pervasive Computing*, *2*(1), 46–55.

Bessler, S., & Jorns, O. (2005). A privacy enhanced service architecture for mobile users. In *Third IEEE International Conference on Pervasive Computing and Communications Workshops* (pp. 125–129). IEEE.

Bettini, C., Mascetti, S., Wang, S., Freni, D., & Jajodia, S. (2009). Anonymity and historical-anonymity in location-based services. In C. Bettini, S. Jajodia, P. Samarati, & S. Wang (Ed.),

Privacy in Location Based Applications (pp. 1-30). Lecture Notes in Computer Science, 5599, Springer Berlin/ Heidelberg.

Blake, I. F. & Kolesnikov, V. (2004). Strong conditional oblivious transfer and computing on intervals. In *10th International Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT 04* (pp. 515-529). Lecture Notes in Computer Science, 3329, Springer.

Boneh, D., & Franklin, M. (2001). Identity-based encryption from the Weil pairing. In *Advances in Cryptology - CRYPTO 2001* (pp. 213–229). Springer.

Burmester, M., Magkos, E., & Chrissikopoulos, V. (2008). Strengthening privacy protection in VANETs. In *Proceedings of the 2008 IEEE International Conference on Wireless & Mobile Computing, Networking & Communication* (pp. 508–513). IEEE Computer Society, Washington, DC, USA.

Buttyan, L., Holczer, T., & Vajda, I. (2007). On the effectiveness of changing pseudonyms to provide location privacy inVANETs. In *Proceedings of the Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks* (pp. 129–141). Lecture Notes in Computer Science, 4572, Springer Berlin / Heidelberg.

Camenisch, J., Hohenberger, S., Kohlweiss, M., Lysyanskaya, A., & Meyerovich, M. (2006). How to win the CloneWars: efficient periodic n-times anonymous authentication. In Proceedings of the *13th ACM conference on Computer and Communications Security* (pp. 201–210). ACM Press, New York, NY, USA.

Camenisch, J., & Lysyanskaya, A. (2001). An efficient system for non-transferable anonymous credentials with optional anonymity revocation. *Advances in Cryptology- EUROCRYPT 2001* (pp. 93–118). Lecture Notes in Computer Science, 2045, Springer.

Camenisch, J., & Lysyanskaya, A. (2002) Dynamic accumulators and application to efficient revocation of anonymous credentials. *Advances in Cryptology - CRYPTO 2002* (pp. 101–120). Lecture Notes in Computer Science, 2442, Springer.

Camenisch, J., & Lysyanskaya, A. (2004). Signature schemes and anonymous credentials from bilinear maps. In *Advances in Cryptology – CRYPTO 2004* (pp. 1–6). Lecture Notes in Computer Science, 3152, Springer.

Candebat, T., Dunne, C. & Gray, D. T. (2005). Pseudonym management using mediated identity- based cryptography. In *Proceedings of the 2005 workshop on Digital Identity Management - DIM '05* (pp. 1–10). ACM Press, New York, NY, USA.

Chaum, D.L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, *24*(2), 84–90.

Chaum, D. (1983). Blind signatures for untraceable payments. In D. Chaum, R.L. Rivest, & A.T. Sherman (Ed.), *Advances in Cryptology – Proceedings of Crypto 82* (pp. 199–203). Plenum Press.

Chaum, D. (1985). Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, *28*(10), 1030–1044.

Cho, Y.S., Bao, L., & Goodrich, M. (2006). Secure access control for location-based applications in WLAN systems. In *2nd IEEE International Workshop on Wireless and Sensor Networks Security - WSNS06* (pp. 852–857). IEEE.

Chor, B., & Gilboa, N. (1997). Computationally private information retrieval (extended abstract). In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing STOC '97* (pp. 304–313), ACM Press, New York, NY, USA.

Chor, B., Goldreich, O., Kushilevitz, E., & M. Sudan (1995). Private information retrieval. In *Annual IEEE Symposium on Foundations of Computer Science* (pp. 41-50). IEEE Computer Society.

Cox, L. P., Dalton, A., & Marupadi, V. (2007). Smokescreen: flexible privacy controls for presence-sharing. In *Proceedings of the 5th international conference on Mobile Systems applications and services - MobiSys '07* (pp. 233-245). ACM Press, New York, NY, USA.

Cramer, R., Gennaro, R., & Schoenmakers, B. (1997). A secure and optimally efficient multi-authority election scheme. *European Transactions on Telecommunications*, *8*(5), 481–490.

Damgard, I., & Jurik, M. (2001). A generalisation, a simplification and some applications of Paillier's probabilistic public-key system. In *Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography - PKC '01* (pp.119–136). Lecture Notes in Computer Science, 1992, Springer-Verlag.

Denning, D., & MacDoran, P. (1996). Location-based authentication: Grounding cyberspace for better security. *Computer Fraud & Security*, *1996*(2),12–16.

Desmedt, Y.G. (1994). Threshold cryptography. *European Transactions on Telecommunications*, *5*(4), 449–457.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644-654.

Duckham, M., & Kulik, L. (2005). A formal model of obfuscation and negotiation for location privacy. In *3rd International Conference on Pervasive Computing – Pervasive 2005* (pp. 152-170). Lecture Notes in Computer Science, 3468, Springer.

Duckham, M., & Kulik, L. (2006). Location privacy and location-aware computing. In J.Drummond, R. Billen, D. Forrest, and E. Joao (Ed.), *Investigating Change in Space and Time*. CRC Press.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, *31*(4), 469–472.

Even, S., Goldreich, O., & Lempel, A. (1985). A randomized protocol for signing contracts. *Communications of the ACM*, *28*(6), 647.

Freudiger, J. Shokri, R., & Hubeaux, J. (2009). On the optimal placement of MIX zones. In *9th International Symposium, Privacy Enhancing Technologies – PETS 2009* (pp. 216-234). Lecture Notes in Computer Science, 5672, Springer.

Gajparia, A., Mitchell, C., & Yeun, C. (2004). The location information preference authority: Supporting user privacy in location based services. In S. Liimatainen and T. Virtanen (Ed.), The *9th Nordic Workshop on Secure IT-systems - Nordsec 04* (pp. 91–96)..

Gedik , B., & Liu, L. (2005). Location privacy in mobile systems: A personalized anonymization model. In *25th IEEE International Conference on Distributed Computing Systems ICDCS 2005* (pp. 620–629). IEEE..

Ghinita, G. (2008). Understanding the privacy-efficiency trade-off in location based queries. In *Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS* (pp. 1–5). ACM Press, New York, NY, USA.

Ghinita, G. (2009). Private Queries and Trajectory Anonymization: a Dual Perspective on Location Privacy. *Transactions on Data Privacy*, *2*(1), 3–19.

Ghinita, G., Kalnis, P., Khoshgozaran, A., Shahabi, C., & Tan, K. (2008). Private queries in location based services: Anonymizers are not necessary. *In Proceedings of the 2008 ACM SIGMOD international conference on management of data* (pp. 121–132). ACM Press, New York, NY, USA.

Ghinita, G., Kalnis, P., Kantarcioglu, M., & Bertino, E. (2009). A hybrid technique for private location-based queries with database protection. In *Advances in Spatial and Temporal Databases - SSTD 2009* (pp. 98-116). Lecture Notes in Computer Science, 5644, Springer Berlin/Heidelberg.

Ghinita, G., Kalnis, P., & Skiadopoulos, S. (2007). PRIVE: anonymous location-based queries in distributed mobile systems. In *Proceedings of the 16th international conference on World Wide Web* (pp. 371–380). ACM Press, New York, NY, USA.

Goldreich, O., Micali, S., & Wigderson, A. (1991). Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM, 38*(3), 690–728.

Gruteser, M., Bredin, J., & Grunwald, D (2004). Path privacy in location-aware computing. In *Proceedings of MobiSys 04, Workshop on Context Awareness*.

Gruteser, M., & Grunwald, D. (2003). Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st international conference on Mobile systems, applications and services - MobiSys '03* (pp. 31–42). ACM Press, New York, NY, USA.

Gruteser, M., & Grunwald, D. (2005). Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis. *Mobile Networks and Applications, 10*(3), 315–325.

Gruteser, M., & Liu, X. (2004). Protecting privacy, in continuous location-tracking applications. *IEEE Security & Privacy, 2*(2), 28–34.

Hauser, C., & Kabatnik, M. (2001). Towards privacy support in a global location service. In *IFIP Workshop on IP and ATM Traffic Management - WATM/EUNICE 01* (pp. 81-89).

Hengartner, U. (2006). *Enhancing user privacy in location-based services*. Technical Report CACR 2006-27, University of Waterloo, Centre for Applied Cryptographic Research.

Hengartner, U. (2008). Location privacy based on trusted computing and secure logging. In *Proceedings of the 4th international conference on security and privacy in communication networks - SecureComm '08* (pp. 1–8). ACM Press, New York, NY, USA.

Hoh, B., & Gruteser, M. (2006). Protecting location privacy through path confusion. In *1st International Conference on Security and Privacy for Emerging Areas in Communications Networks, - SecureComm 05* (pp. 194-205). IEEE.

Hoh, B., Gruteser, M., Herring, R., Ban, J., Work, D., Herrera, J.C., Bayen, A.M., Annavaram. M., & Jacobson, Q. (2008). Virtual trip lines for distributed privacy-preserving traffic monitoring. In *Proceedings of the 6th international conference on mobile systems, applications and services – MobiSys 08* (pp. 15–28). ACM Press, New York, NY, USA.

Hoh, B., Gruteser, M., Xiong, H., & Alrabady, A. (2007). Preserving privacy in GPS traces via uncertainty-aware path cloaking. In *Proceedings of the 14th ACM conference on Computer and communications security* (pp. 161-171). ACM Press, New York, NY, USA.

Jakobsson, M., Juels, A., & Syverson, P. (2004). Universal re-encryption for mixnets. In *Proceedings of the 2004 RSA Conference, Cryptographers track* (pp. 163–178).

Jorns, O., Bessler, S., & Pailer, R. (2005). An efficient mechanism to ensure location privacy in telecom service applications. In *Network Control and Engineering for QoS, Security and Mobility, III* (pp. 57-68). IFIP International Federation for Information Processing, 165, Springer Boston.

Jorns, O., Quirchmayr, G., & Jung, O. (2007). A privacy enhancing mechanism based on pseudonyms for identity protection in location-based services. In 5th Australasian symposium on ACSW frontiers - ACSW '07 (pp. 133–142). Australian Computer Society.

Kargupta, H., Das, K., & Liu, K. (2007). A game theoretic approach toward multi-party privacy-preserving distributed data mining. In *11th European Conference on Principles and Practice of KDD - PKDD,* Warsaw, Polland.

Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network Security: Private Communication in a Public World*, 2nd Edition. Prentice Hall PTR.

Khoshgozaran, A., & Shahabi, C. (2007). Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. In *10th international conference on Advances in spatial and temporal databases* (pp. 239–257). Springer-Verlag.

Kim, Y., Perrig, A., & Tsudik, G. (2000). Simple and fault-tolerant key agreement for dynamic collaborative groups. In *7th ACM conference on Computer and Communications Security* (pp., 235–244). ACM Press, New York, NY, USA.

Kohlweiss, M., Faust, S., Fritsch, L., Gedrojc, B., & Preneel, B. (2007). Efficient oblivious augmented maps: Location-based services with a payment broker. In *Privacy Enhancing Technologies* (pp. 62–76). Lecture Notes in Computer Science, 4776, Springer Berlin/Heidelberg.

Kolsch, T., Fritsch, L., Kohlweiss, M., & Kesdogan, D. (2005). Privacy for profitable location based services. In *Security in Pervasive Computing, Second International Conference - SPC 05* (pp. 164-178), Lecture Notes in Computer Science, 3450, Springer Berlin/Heidelberg.

Konidala, D. M., Yeun, C.Y., & Kim, K. (2005). A secure and privacy enhanced protocol for location-based services in ubiquitous society. In *Global Telecommunications Conference - GLOBECOM'04* (pp. 2164–2168). IEEE.

Kulik. L. (2009). Privacy for real-time location-based services. *SIGSPATIAL Special, 1*(2), 9–14.

Kushilevitz, E. and Ostrovsky, R. (1997). Replication is not needed: single database, computationally-private information retrieval. In *38th Annual Symposium on Foundations of Computer Science - FOCS '97* (pp. 364–373). IEEE Computer Society.

Lamport, L. (1981). Password authentication with insecure communication. *Communications of the ACM, 24*(11), 770–772.

Langheinrich, M. (2001). Privacy by design-principles of privacy-aware ubiquitous systems. In *Ubiquitous Computing - Ubicomp 2001* (pp. 273-291). Lecture Notes in Computer Science, 2201, Springer.

Lin, D., Bertino, E., Cheng, R., & Prabhakar, S. (2009). Location Privacy in Moving-Object Environments. *Transactions on Data Privacy, 2*(1), 21–46.

Lysyanskaya, A., Rivest, R., Sahai, A., & Wolf, S. (2000). Pseudonym systems. In *Selected Areas in Cryptography* (pp. 184–199). Lecture Notes in Computer Science, 1758, Springer.

Magkos, E., Kotzanikolaou, P., Sioutas, S., & Oikonomou, K. (2010). A distributed privacy-preserving scheme for location-based queries. In *IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks - WoWMoM* (pp. 1–6). IEEE.

Mishra, S. K., & Sarkar, P. (2000). Symmetrically private information retrieval. In, 1st International Conference in Cryptology - INDOCRYPT '00 (pp. 225-236). Lecture Notes in Computer Science, 1977, Springer.

Mokbel, M.F., Chow, C.Y., & Aref, W.G. (2006). The new Casper: Query processing for location services without compromising privacy. In *Proceedings of the 32nd international conference on Very large data bases* (pp. 763–774). VLDB Endowment.

National Institute of Standards and Technology (2008). *FIPS PUB 180-3: Secure Hash Standard (SHS)*.

Okamoto, T., & Uchiyama, S. (1998). A new public-key cryptosystem as secure as factoring. In *Advances in Cryptology – EUROCRYPT '98* (pp. 308). Lecture Notes in Computer Science, 1403, Springer Berlin / Heidelberg.

Olumofin, F., Tysowski, P., & Goldberg, I. (2009). *Achieving efficient query privacy for location based services*. Technical Report CACR Tech Report 2009-22, University of Waterloo, Centre for Applied Cryptographic Research.

Paillier, P. (1999). Public-key cryptosystems based on discrete logarithms residues. In *Advances in Cryptology – EUROCRYPT* '99 (pp. 221-236). Lecture Notes in Computer Science, 1592, Springer Berlin / Heidelberg.

Pfitzmann, A., & Kohntopp, M. (2000). Anonymity, unobservability, and pseudonymity- A proposal for terminology. In *Workshop on Design Issues in Anonymity and Unobservability* (pp. 1–9).

Pinkas, B. (2002). Cryptographic techniques for privacy-preserving data mining. *SIGKDD Explorations Newsletter, 4*(No. 2), pp. 12–19.

Rabin, M. (2009). *How to exchange secrets by oblivious transfer*. Technical Report TR-81, Harvard University, Aiken Comp. Lab.

Rafaeli, S., & Hutchison, D. (2003). A survey of key management for secure group communication. *ACM Computing Surveys, 35*(3), 309–329.

Rahman, S., & Hengartner, U. (2007). Secure crash reporting in vehicular ad hoc networks. *In 3rd International Conference on Security and Privacy in Communication Networks - SecureComm '07* (pp. 443 - 452). ACM Press, New York, NY, USA.

Rasmussen, K.B., & Capkun, S. (2007). Implications of radio fingerprinting on the security of sensor networks. In *3rd International Conference on Security and Privacy in Communication Networks – SecureComm* (pp. 331 - 340). IEEE.

Raya, M., & Hubaux, J. P. (2005) The security of vehicular ad hoc networks. In *3rd ACM workshop on Security of ad hoc and sensor networks - SASN '05* (pp. 11–21). ACM Press, New York, NY, USA.

Raya, M., & Hubaux, J.P. (2007). Securing vehicular ad-hoc networks. *Journal of Computer Security, 15*(1), 39–68.

Rebollo-Monedero, D., Forne, J., Subirats, L., Solanas, A., & Martınez-Balleste, A. (2009). A collaborative protocol for private retrieval of location-based information. In *Proceedings of the IADIS International Conference on e-Society*, Barcelona, Spain.

Rodden, T., Friday, A., Muller, H., & Dix, A. (2002). *A lightweight approach to managing privacy in location-based services*. Technical Report CSTR-07-006, University of Nottingham and Lancaster University and University of Bristol.

Sampigethaya, K.. Huang, L., Matsuura, K., Poovendran, R., & Sezaki, K. (2005). CARAVAN: Providing location privacy for VANET. In *3rd Embedded Security in Cars Workshop - ESCAR '05*.

Saroiu, S., & Wolman, A. (2009). Enabling new mobile applications with location proofs. In *10th Workshop on Mobile Computing Systems and Applications* (pp. 3–9). ACM.

Shamir, A. (1984). Identity-based cryptosystems and signature scheme. In *Advances in Cryptography - CRYPTO '84* (pp. 47-53). Lecture Notes in Computer Science, 985, Springer Berlin.

Solanas, A., Domingo-Ferrer, J., & Martınez-Balleste, A. (2008). Location privacy in location-based services: Beyond TTP-based schemes. In *1st International Workshop on Privacy in Location-Based Applications - PiLBA 2008*, CEUR-WS, 397.

Solanas, A., Martınez-Balleste, A. (2007). Privacy protection in location-based services through a public-key privacy homomorphism. In 4th European PKI Workshop: *Theory and Practice - EuroPKI '07* (pp. 362-368). Lecture Notes in Computer Science, 4582, Springer.

Solanas, A., & Martınez-Balleste, A. (2008). A TTP-free protocol for location privacy in location-based services. *Computer Communications, 31*(6), 1181–1191.

Sun, Y., La Porta, T. F., & Kermani, P. (2009). A flexible privacy-enhanced location-based services system framework and practice. *IEEE Transactions on Mobile Computing, 8*(3), 304–321.

Sun, J., Zhang, C., & Fang, Y. (2007). An ID-based framework achieving privacy and non-repudiation in vehicular ad hoc networks. In *Military Communications Conference-MILCOM '07* (pp. 1-7). IEEE.

Sweeney, L. (2002). k-anonymity: a model for protecting privacy. *International Journal of Uncertainty Fuzziness and Knowledge Based Systems, 10*(5), 557–570.

Wakeman, I. Chalmers, D., & Fry, M. (2007). Reconciling privacy and security in pervasive computing: the case for pseudonymous group membership. In *5th international workshop on Middleware for pervasive and ad-hoc computing - MPAC '07* (pp. 7–12), ACM Press, New York, NY, USA.

Yiu, M.L., Ghinita, G., Jensen, C.S., & Kalnis, P. (2009). Outsourcing search services on private spatial data. In *25th International Conference on Data Engineering - ICDE'09* (pp. 1140–1143). IEEE.

Zhang, Y., Liu, W., Lou, W., & Fang, Y. (2005). Securing sensor networks with location-based keys. In *Wireless Communications and Networking Conference - WCNC '05* (pp. 1909–1914). IEEE.

Zhong, G., Goldberg, I., & Hengartner, U. (2007). Louis, Lester and Pierre: Three protocols for location privacy. In *Privacy Enhancing Technologies* (pp. 62-76). Lecture Notes in Computer Science, 4776, Springer Berlin / Heidelberg.

Zhong, G., & Hengartner, U. (2008). Toward a distributed k-anonymity protocol for location privacy. In *7th ACM workshop on Privacy in the electronic society - WPES '08* (pp. 33–38). ACM Press, New York, NY, USA.

Zhong, G., & Hengartner, U. (2009). A distributed k-anonymity protocol for location privacy. In *International Conference on Pervasive Computing and Communications* (pp. 1–10). IEEE.

Zhu, F., Mutka, M., & Ni, L. (2003). Splendor: A secure, private, and location-aware service discovery protocol supporting mobile services. In *1st IEEE International Conference on Pervasive Computing and Communications- PerCom '03* (pp. 235–242). IEEE.