Location Privacy in Pervasive Computing

Claudio A. Ardagna, Marco Cremonini,
Sabrina De Capitani di Vimercati, Pierangela Samarati

Università degli Studi di Milano - 26013 Crema, Italy
{ardagna,cremonini,decapita,samarati}@dti.unimi.it

Abstract

Recent technological advances have made it feasible to measure and track the location of users, vehicles, and practically any mobile object. Positioning and tracking systems are then collecting a huge amount of potentially sensitive *location information*, which is a set of data describing a user's location over a period of time. Since the activities of a user are often related to the locations where such activities are performed, it is natural for users to demand privacy, that is, to require control over the access to their location information.

In this chapter, we focus on the privacy aspects of using location information in *location-based services* (LBSs). LBSs are services that take the current position of the user into consideration when performing their tasks. These services can be accessed from mobile phones, PDA, and any other mobile device. We start the chapter by characterizing the location privacy protection problem and introducing a classification of the main techniques that have been proposed to protect the location privacy. We also survey and discuss recent proposals and ongoing work in the location-based systems area.

1 Introduction

The rapid development of location technologies and the widespread adoption of mobile communication devices are fostering the development of new applications that exploit the physical position of users to offer location-based services (LBSs) for business, social, or informational purposes. A key aspect for the development of these LBSs is represented by the modern location technologies that have reached good accuracy and reliability at costs that most people (e.g., the cost of mobile devices)

and companies (e.g., the cost of integrating location technologies in existing telecommunication infrastructures) can economically sustain. Consequently, several commercial and enterprise-oriented LBSs are already available and are gaining popularity [8, 14]. While these applications offer great benefits to users, they also exhibit significant potential for abuse since positioning and tracking systems are collecting a huge amount of location information. Particularly relevant are privacy concerns and recent security incidents have revealed faulty data management practices and unauthorized trading of users personal (including location) information. In this scenario, the improper exposure of location information could result in stalking or physical harassment. Examples of security incidents are represented by legal disputes involving rental companies tracking their cars by means of Global Positioning System (GPS) technology and charging users in case of agreement infringements [11], or organizations tracking their own employees using a "Friend finder" service [35]. Furthermore, providers of online and mobile services often exceed in collecting personal information as a requirement for service provision. Such a worrisome scenario calls for more sophisticated solutions aimed at preserving the privacy of users when dealing with location information. For all these reasons, research on location privacy has gained a relevant boost and represents one of the key aspects to the success of location-based services.

It is interesting to note that privacy issues in online services have been analyzed from different perspectives by scientific and liberal disciplines. Many sociological studies of the privacy problem [8, 12] have brought to a better understanding of the concerns that users perceive when using a location-based service. Barkhuus and Dey [8] present an experimental case study that analyzes the concerns of users about location privacy and shows how such concerns are related to the nature of the service. The study is focused on *location-tracking services*, where locations of users are tracked by third parties, and on *position-aware services*, where mobile and portable devices are aware of their own positions. The result of this research is that users considered position-aware services more respectful of their privacy and therefore were more likely to subscribe to them rather than to location-tracking services. By contrast, location-tracking services represent a promising class of applications whose success depends on solutions for protecting the privacy of the users using such a service.

From a technological point of view, most of the current research on location privacy focuses on providing anonymity or support for partial identities to online and mobile services that are not

based on the personal identification of a user for their provision [9, 10, 21, 24]. However, there are situations where anonymity or partial identification are not viable options for the provision of online services [33]. Therefore, when user identity is needed for the successful service provisioning, the privacy of the location of the users can be provided by decreasing the accuracy of the location information itself [15]. As a matter of fact, in many real applications, location information can have sub-optimal accuracy levels and still offers an acceptable quality of service to end-users. Consider, for example, a LBS providing a Point of Interest (POI) service, and a user asking for the list of restaurants within 300 meters. If the position of the user is most accurate, the LBS will be able to return the exact set of restaurants within the distance specified by the user. By contrast, for less-accurate positions, the response of the LBS could include some restaurants that actually are not within the specified distance and exclude others that actually are within that distance. In any case, the outcome is likely to be still satisfying for the user, being tolerable the difference with respect to the optimal response. In similar cases, a good quality of service is still preserved even with a sub-optimal accuracy of the location service. It is the very nature of each LBS to dictate whether anonymity or personal identification is required and whether optimal location accuracy is strictly required or a less-than-optimal accuracy is sufficient.

The remainder of this chapter is organized as follows. Section 2 discusses the basic concepts of positioning systems and location-based services. Section 3 presents an overview of location privacy issues, discusses different categories of location privacy, and describes some techniques that can be used to protect location privacy. Section 4 gives an overview of current research on location-based systems. Section 5 discusses open issues of current location privacy solutions. Finally, Section 6 concludes the chapter.

2 Basic Concepts and Scenario

We briefly describe positioning systems and some basic concepts on location-based services.

2.1 Positioning Systems

Positioning systems measure the location of mobile devices by using several mobile technologies that have been developed or can be exploited to compute location information (e.g., GSM/3G, GPS [42],

WiFi, and RFID). The relevant boost in terms of accuracy and reliability enjoyed by GSM/3G technologies in recent years and the widespread adoption of cellular phones make GSM/3G one of the most suitable technologies to delivery services that make use of physical locations of users. Among the techniques used by GSM/3G technologies, we list here the most reliable and already standardized.

- *Cell Identification.* It is the simplest technique and is based on the identification of the mobile terminal serving cell. The spatial coordinates of the cell provide a broad estimation of a user position, which depends on the radius of the cell.

- *Signal Level.* It measures the signal attenuation between the mobile terminal and the base station to calculate a user's position.

- *Angle of Arrival (AoA).* It assumes that more than one single base station for signal reception is available. A user's position can be calculated by computing the angle of arrival at two base stations.

- *Time of Arrival (ToA).* It calculates the distance between a base station and a mobile phone by measuring the time for a signal to complete a round-trip between the two endpoints. Signal arrival can be delayed by walls or natural obstacles, decreasing location accuracy.

- *Time Difference of Arrival (TDoA).* It computes the time difference between station-to-terminal propagation, with the purpose of increasing the location accuracy.

Several works have described and discussed location techniques and the best accuracies that can achieve [46]. It is widely acknowledged that technological improvements allow the development of positioning systems that permit to reduce location errors to few meters, regardless to the particular environment (e.g., urban, suburban, rural, outdoor, or indoor).[1] The location accuracy of sensing technologies combined with the widespread adoption of GPS, WiFi, and cellular phones call for a urgent and careful consideration of the privacy issues. Concerns are even more critical if we consider that mobile devices are unable to enforce restrictions on location data scattering or to avoid the data flow (unless the mobile devices are switched off). The worst case scenario that some

[1]Note that also several non-standard methods [13] have been developed to further improve the accuracy of standard positioning methods.

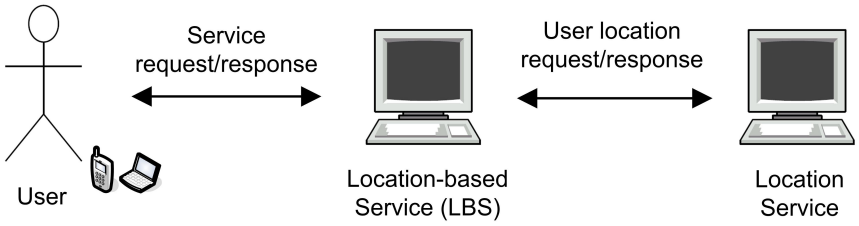

Figure 1: LBS Scenario

analysts have foreseen as a consequence of an unrestricted and unregulated availability of location technologies recalls the well-known "Big Brother" stereotype: a society where the secondary effect of location technologies, whose primary effect is to enable the development of innovative and useful services, is a form of implicit total surveillance of individuals.

2.2 Location-based Services

A typical location-based service scenario is composed of three entities (see Figure 2): the *user* is an individual that requests online services and carry mobile devices; the *Location-Based Service (LBS)* is the entity that provides location-based applications to the users and collects personal information (including location information) to grant and personalize the access to its services; *Location Service (LS)* is the entity that implements the positioning system and provides the location information at different levels of granularity and with different Quality of Service (QoS). The types of location requests that a Location Service can satisfy depend on the specific mobile technology, the methods applied for measuring users position, and environmental conditions.

The interactions among these three entities are carried out via request/response message exchanges. When the LBS receives a request that needs some location-based attributes of the requester to be evaluated, it queries the LS for retrieving the location information. Communication protocols might be adopted to negotiate quality of service attributes, service costs, and other application-specific parameters [2]. Finally, after receiving the required location information from the LS, the LBS returns a response to the requester. This decomposition shows that location functionalities are fully encapsulated into specialized entities that could provide functionally equivalent location services possibly based on different technologies and operated according to different service levels.

Academic and industrial research has already defined several prototypes of location-based ser-

vices for business, social, or informational purposes [27]. In general, these location-based services can be partitioned into the following categories.

- *"Locate-me" services.* They give information about the position of users. They should be used when authorized third parties need to know the positions of users for performing their tasks. In particular, a locate-me service is at the base of all the location-based services categories.

- *Nearby-information services.* They provide information about the environment surrounding the location of a user (e.g., point of interest, context-aware tourist guides, or weather and traffic alerts). A user subscribes to these services and receives real-time information through her mobile device.

- *Locate-friends and nearby-friends services.* They give information to subscribers about the real-time location or proximity of other subscribers. They could be used, for example, to provide services in the context of social networks or as industrial applications to coordinate the workforce.

- *Tracking services.* They allow monitoring movements of users and includes telemetric services (i.e., the observation of parameters of mobile objects such as speed, direction of movement, and so on). They could be used by online services that provide vehicles tracking, tracking of children or employees, and warning about dangerous areas.

- *Personal-navigation services.* They provide information about the path that has to be followed to reach a target location from the current user's location. These services rely on tracking services to gather the position of a user moving on the field.

LBSs can then be useful for many purposes, ranging from industrial applications to personal assistant applications. A particular but important application field of location services is represented by critical applications, where the availability of a precise location can help in protecting human live. An example is the enhanced 911 service in North America [18] that can immediately dispatch emergency services (e.g., emergency medical services, police, or firefighters) where they are needed, reducing the margin of error.

3 Location Privacy Protection

Location privacy can be defined as the right of individuals to decide how, when, and for which purposes their location information could be released to other parties. The lack of location privacy protection could be exploited by adversaries to perform different attacks [17]: *unsolicited advertising,* when the location of a user could be exploited, without her consent, to provide advertisements of products and services available nearby the user position; *physical attacks or harassment,* when the location of a user could allow criminals to carry physical assaults to specific individuals; *users profiling,* when the location of a user could be used to infer other sensitive information, such as state of health, personal habits, or professional duties, by correlating visited places or paths; *denial of service,* when the location of a user could motivate an access denial to services under some circumstances.

The concept of location privacy can assume several meanings and pursue different objectives, depending on the scenario in which users are moving and on the services users are interacting with. As previously mentioned, location privacy solutions could be aimed at protecting users by making their location information anonymous, or keeping explicit identification but perturbing their location information to decrease the accuracy. We can therefore identify different categories of location privacy.

- *Identity privacy.* The main goal is to protect users' identities associated with or inferable from location information. In this case, the best possible location measurement can be provided to other entities but users identity must be kept hidden.

- *Position privacy.* The main goal is to perturb users locations as a way to protect their actual positions. In particular, this type of location privacy is suitable when users' identities are required for the successful provisioning of a service.

- *Path privacy.* The main goal is to protect the privacy of those users that are continuously monitored during a certain period of time. In this case, location-based services will no longer receive a single location measurement, rather they will gather a flow of position samples that permits them to track users.

Based on these different categories of location privacy, three main classes of location privacy

techniques can be introduced: anonymity-based, obfuscation-based, and policy-based.

Anonymity-based techniques. Anonymity-based techniques provide solutions for the protection of identity and path privacy. In particular, this class includes all solutions based on the notion of *anonymity* [9, 10, 21, 24], which is aimed at making an individual (i.e., her identity or personal information) not identifiable.

Beresford and Stajano [9] propose a method, called *Mix zones*, using an anonymity service that delays and reorders messages from subscribers within pre-defined zones. A trusted middleware lies between the positioning systems and the third party applications and is responsible for limiting the information collected by applications. The Mix zone model introduces the concepts of *application zone*, which are homogeneous application interests in a specific geographic area, and *mix zones*, which are areas in which a user cannot be tracked. Within mix zones, a user is anonymous in the sense that the identities of all users coexisting in the same zone are mixed and become indiscernible. Furthermore, the infrastructure makes a user entering a mix zone unlinkable from other users leaving it. Other works [21, 24] are based on the concept of location k-anonymity [44], meaning that a user should be indistinguishable by other $k-1$ users in a given location area or temporal interval. Gruteser and Grunwald [24] propose a middleware architecture and an adaptive algorithm to adjust location information resolution, in spatial or temporal dimensions, to comply with the specified k-anonymity requirement. Finally, another strand of research is aimed at protecting the *path privacy* of the users [23, 25, 30]. Path privacy involves the protection of users that are continuously monitored during a temporal interval. This research area is relevant for location tracking applications, where data about users moving in a particular area are collected by external services, such as navigation systems. In summary, anonymity-based techniques are suitable for all those contexts that do not need knowledge of the identity of the users, and their effectiveness strongly depends on the number of users physically located in the same area.

Obfuscation-based techniques. Differently from anonymity-based techniques, the main goal of obfuscation-based techniques is to perturb the location information still maintaining a binding with the identities of users. This class includes all the solutions based on the notion of *obfuscation* [4, 5, 15, 41], which is the process of degrading the accuracy of the location information to provide privacy protection.

Duckham and Kulik [15, 16] define a framework that provides a mechanism for balancing the individual needs for high-quality information services and the location privacy requirements. The proposed solution is based on the *imprecision concept*, which indicates the lack of specificity of location information. The authors propose to degrade the quality of the location information and to provide obfuscation features by adding n points, with same probability, to the real user position.

Obfuscation-based techniques usually provide mechanisms for specifying privacy preferences in a common and intuitive manner through a *minimum distance*. These solutions however present several drawbacks. First, they do not provide a metric for measuring the privacy level, making them difficult to integrate into a full fledged location-based application scenario [3]. Second, they usually implement a single obfuscation technique based on the enlargement of a location area. A possibility that is often neglected by traditional location obfuscation solutions is the definition and composition of different obfuscation techniques to increase their robustness with respect to possible de-obfuscation attempts performed by adversaries. Finally, obfuscation solutions are often meaningful in a specific application context only. Ardagna et al. [4, 5, 6] address the above shortcomings by presenting a novel solution composed by a management process and several techniques aimed at preserving location privacy by artificially perturbing location information measured by sensing technologies. The proposed solution permits the specification of privacy preferences in a simple and intuitive way and the design of a framework that makes the enforcement of privacy preferences manageable for location-based services, while preserving the quality of the online service. The authors introduce the *relevance* concept as a metric for the accuracy of location information, abstracting from any physical attribute of sensing technology. The relevance quantitatively evaluates the degree of privacy introduced into a location measurement and is adopted by users to define their privacy preferences. Different obfuscation-based techniques and their composition are also discussed.

Policy-based techniques. Policy-based techniques are based on the definition of *privacy policies* and provide solutions for the protection of all privacy categories [22, 26, 28, 31, 34]. Privacy policies define restrictions that must be enforced when the location of users is used by or released to third parties. The definition of complex rule-based policies can however be difficult to understand and manage for users that often are not familiar with specific policy definition languages. Therefore,

although policies-based techniques are powerful and flexible, they can easily result in very complex and unmanageable tools for end-users.

In summary, anonymity-based and obfuscation-based techniques are dual categories. While anonymity-based techniques have been primarily defined to protect identity privacy and are less suitable for protecting location privacy, obfuscation-based techniques are well-suited for location protection and unrelated with identity protection. Regarding path protection, both anonymity-based and obfuscation-based techniques are well-suited and able to provide the required degree of protection. Concerning policy-based techniques, they are flexible and in general well-suited for all location privacy categories, whereas their management complexity could easily become overwhelming. In the following, we discuss some architectural issues that may arise from the integration of location privacy techniques in a location-based service scenario.

4 Privacy-aware Location-based Systems

Mobile communication technologies and location sensing techniques can provide a rich set of location-based information, not limited to the position of a requester, such as the direction where a user is headed, her velocity and acceleration [3]. Also, location-based services are able to provide a wealth of additional environment-related knowledge (e.g., whether or not the user is alone in a given area). Moreover, when location measurements are coupled with a contextual description, for example, the topology of the environment where the requester is moving (e.g., a city topology) and the type of motion (e.g., walking, by car, by train), advanced reasoning methods can be applied to foresee the requester position in a time frame. In this context, location privacy has driven the design of privacy-aware location-based services. Privacy aspects are also related to the overall architecture that permits a location-based service to receive and manage location-based information, which has been manipulated for privacy purposes. Location measurements are performed by specialized location services that have the technologies and the infrastructures for collecting such an information. The location information collected by the location service must then be disclosed according to the privacy requirements.

We now focus on the architectural issues arising when a privacy-aware location-based service is

provided. We first survey existing location-based solutions and then we describe a privacy-aware LBS architecture based on the scenario depicted in Figure 1.

4.1 Summary on Current Research on Location-Based Systems

At a high level, the research work in the location-based systems area is related to: *i)* the development of architectures supporting location-based services, and *ii)* the protection of location information or the use of location information for improving security.

LBS architectures. Some proposals present architectures, designed for pervasive environments, which incorporate mobile data for security management. Myllymaki and Edlund [37] describe a methodology for aggregating location data from multiple sources thus improving the location tracking features. Most commercial location platforms include a gateway that mediates between multiple location providers and location-based applications [41]. In these architectures, the location gateway obtains subscriber's location information from multiple sources and delivers them, possibly modified according to privacy requirements, to the location-based applications. Ardagna et al. [2] present a general architecture for evaluating location-based conditions under the assumption that multiple functionally equivalent location providers are available. The architecture relies on integrating multiple sources of location information via a novel negotiation technique.

Other researchers describe the architecture and operation of an access server module for LBAC in local wireless networks [40, 47]. The need for a protocol-independent location technique has been underlined by an interesting study exploiting heterogeneous positioning sources like GPS, Bluetooth, and WaveLAN for designing location aware applications [40]. Location information and its management are also the topics of a recent study by Varshney [47] in the area of mobile commerce applications.

Some solutions propose special-purpose *location middlewares* for managing interactions between applications and location providers, while maximizing the quality of service (QoS) [38, 39, 43]. Typically, in these proposals the location middleware *i)* receives requests from the LBS asking for location information, *ii)* collects users locations from a pool of location providers, and *iii)* produces an answer. Naguib et al. [38] present a middleware framework, called *QoSDREAM*, for managing context-aware multimedia applications. Nahrstedt et al. [39] present a QoS middleware

for ubiquitous computing environments aimed at maximizing the QoS of distributed applications. Ranganathan et al. [43] present a middleware that provides a clear separation between business applications and location detection technologies. They also address the issue of managing location data from heterogeneous location technologies. Although several middleware components supporting communication and negotiation between location services and applications have been presented, only few proposals try to integrate service quality and privacy protection. For instance, Myles et al. [36] propose an architecture aimed at preserving privacy in location-based services. The architecture is based on a middleware managing the interactions between location-based applications and location providers and on the definition of policies for data release. Hong et al. [31] present an extension of the P3P language for representing user privacy preferences for context-aware applications. Ardagna et al. [5] provide a middleware-based architecture for integrating privacy preferences of the users and location accuracy of LBS in the context of a location-based access control system. The middleware component explicitly addresses the trade-off between users privacy and location accuracy by satisfying preferences set by users and maximizing the quality of location information released to location-based systems.

Location information protection. Few papers consider location information as a means for improving security. The definition of a location-based access control model is becoming an emerging research issue [3, 6]. Some early mobile networking protocols linked the notion of physical position of a terminal device with its capability of accessing network resources [1]. The widespread adoption of wireless local networks has been the subject of some recent studies, where the location information is used for monitoring users movements on Wireless-Lan [19] and 802.11 Networks [20]. Sastry et al. [45] exploit location-based access control in sensor networks. Zhang and Parashar [48] propose a location-aware extension to Role-Based Access Control (RBAC) suitable for grid-based distributed applications. Ardagna et al. [3] propose a location-based access control model and language and an evaluation infrastructure. The proposed approach encapsulates time-dependency and uncertainty of location measurements, as important features of location information, in a small set of semantically uniform service level agreement (SLA) parameters based on the notions of confidence level and temporal validity of each access request. These parameters are aimed at achieving a clean separation of the access control evaluation engine from the protocol-dependent location

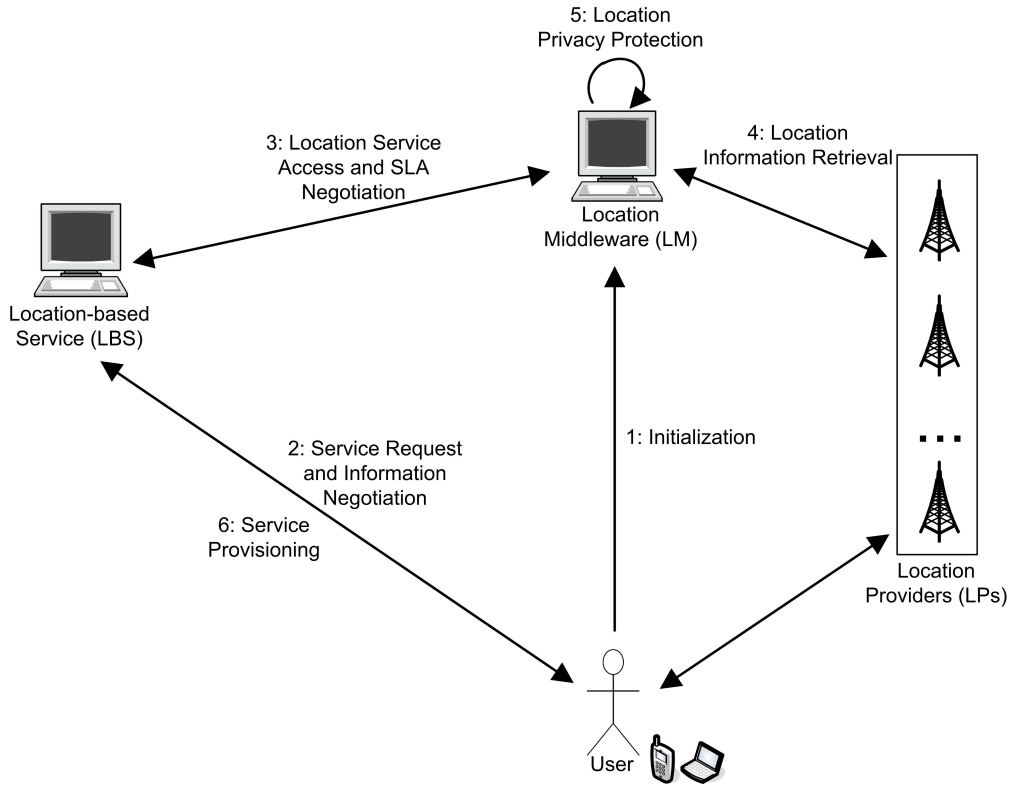

Figure 2: Privacy-aware LBS architecture

services made available by the network operators. Formal definitions of a number of location-based predicates have been also provided, together with a discussion of their management, evaluation, and enforcement. Other papers take into account time variant information for querying databases containing location information [32].

Some recent works took a different approach with respect to location information by considering it as a resource to be protected against unauthorized access. For instance, Hengartner and Steenkiste [29] describe a mechanism to protect user's location information by means of electronic certificates, delegation, and trusted location-based services. The same problem is addressed by Hauser and Kabatnik [26] that propose a privacy-aware architecture for a global Location Service, which should permit users to define rules for the access to their location information.

4.2 A Privacy-aware LBS Architecture

The design of privacy-aware location-based services poses some architectural and functional problems that were never studied before in the context of traditional distributed and Internet-based

applications. In particular, a privacy-aware LBS architecture must be designed and developed integrating components logically tied with the applications and components providing privacy-aware location services. One typical approach in the design of privacy-aware LBS architectures is to provide a location middleware acting as a trusted gateway between the LBS and the location services. Such a component is in charge of managing all interactions with sensing technologies and enforcing users privacy preferences. The logical components of a privacy-aware LBS architecture, which are showed in Figure 2, can be summarized as follows.

- *User*. It is the subject that submits service requests, and it can be located through her mobile device during the interaction with the Business Application. The user first defines her privacy preference at the Location Middleware and then interacts with the location-based service to gain the access to the Business Application.

- *Location-based Service (LBS)*. Customer-oriented application that requests location information of the users for a successful provisioning. It implements the actual location-based service and it relies on the location middleware for retrieving location-based information.

- *Location Middleware (LM)*. The entity that interacts with different location providers and provides privacy-aware location services to the LBS. The middleware component explicitly addresses the trade-off between location privacy and location accuracy by satisfying privacy preferences set by users and maximizing the quality of location information released to LBS.

- *Location Providers (LPs)*. Components using location sensing technologies to provide location information. The LM and LP components form the Location Service presented in Figure 1.

The communications among these components are performed via request/response message exchanges. The interaction flow can be logically partitioned in six macro-operations (see Figure 2) described as follows.

1. *Initialization:* user preferences are defined at the Location Middleware.

2. *Service request and information negotiation:* a user submits a service request to the Location-based Service and a negotiation process resulting in a bidirectional identification between the parties is carried out.

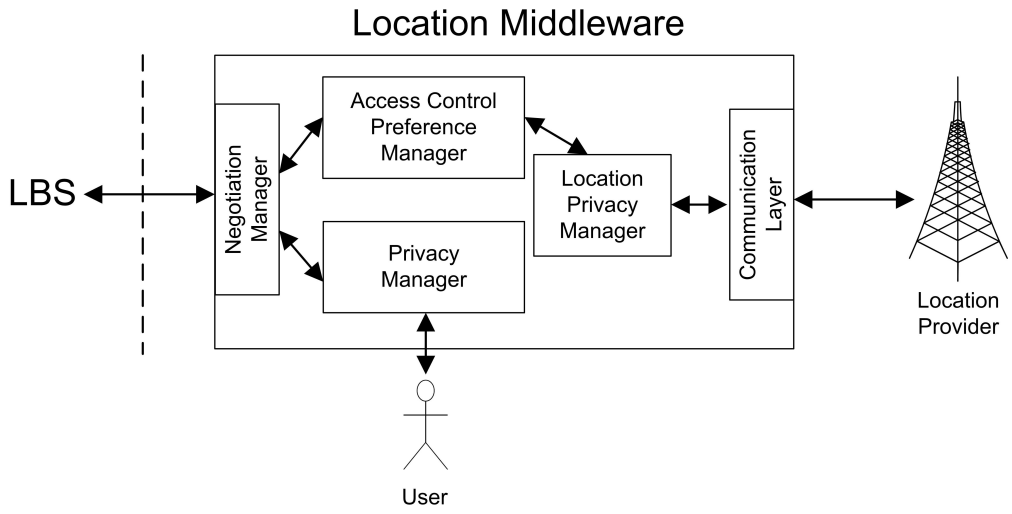

Figure 3: Location Middleware

3. *Location service access and SLA negotiation:* a Service Level Agreement (SLA) specifying QoS attributes and corresponding service costs is agreed between the Location-based Service and the Location Middleware [2].

4. *Location information retrieval:* the Location Middleware collects location information through a communication process with multiples Location Providers.

5. *Location privacy protection:* privacy techniques are used to enforce the privacy preferences expressed by the users.

6. *Service provisioning:* the Location-based Service receives the user information, possibly modified according to privacy preferences, and the request is granted or denied by permitting or blocking the access to the service by the User.

Privacy-aware location-based services require two separate contractual agreements: *i)* between the user and a telecommunication company acting as (or on behalf of) location service, regardless of the specific location technology used (e.g., satellite location information like GPS is made available to applications via the mobile network); and *ii)* between the location service and the LBS requiring location information. This dual agreement is critical because, as a generic subscriber to the mobile phone network, an individual may want her privacy strictly preserved, while, as a user of location-based services, she may want the service provider to handle the most accurate location information

to receive best-quality service. To address these conflicting requirements, a location middleware must effectively and securely manage the trade-off between accuracy and privacy. As discussed before, currently available middleware components are mostly in charge of managing interactions between applications and location providers, and communication and negotiation protocols aimed at maximizing the QoS [31, 36, 38, 39, 43]. Emerging approaches however are aimed at designing a privacy-aware middleware responsible for managing the trade-off between users privacy and location accuracy. Figure 3 illustrates how the LM can be functionally divided into the following five logical components.

- *Communication Layer.* It manages the communication process with LPs to access users location information. It hides low-level communication details to other components.
- *Negotiation Manager.* It acts as an interface with LBS, and provides negotiation functionalities and protocols [2].
- *Location Privacy Manager.* It applies privacy techniques for protecting users privacy.
- *Privacy Manager.* It collects, stores, and manages privacy preferences requested by the users.
- *Access Control Preference Manager.* It serves as the component managing location attributes required for the remote evaluation of access control policies.

5 Open Issues

We briefly describe some open issues and general requirements that need to be taken into consideration in future developments of privacy techniques for location-based services.

- *Privacy preference definition.* An important aspect to the success of privacy-aware location-based services is the definition of a mechanism for the specification of privacy preferences that balance the two traditionally conflicting requirements of *usability* and *expressiveness*. Despite its importance for the effectiveness of a privacy solution, this issue has received little attention in existing works on location privacy.
- *Balancing location privacy and accuracy.* Location privacy solutions should be able to balance the need of privacy protection required by users and the need of accuracy required by service

providers. Location privacy techniques, which are mostly focused on users needs, could make service provisioning impossible in practice due to an excessive degradation of the accuracy of the location information. A possible direction to avoid this problem is the definition of a metric of the accuracy of the location information, abstracting from any physical attribute of sensing technology, which should permit to quantitatively evaluate both the degree of privacy introduced into a location measurement and the location accuracy requested by a service provider. Both quality of online services and location privacy could then be adjusted, negotiated, or specified as contractual terms. A quantitative metric of the privacy level could ease the integration of privacy solutions into a full fledged location-based application scenario [3, 7].

- *Composition of privacy techniques.* Usually location privacy solutions implement a single privacy technique. This is evident in the case of obfuscation-based techniques, where most solutions just scale up the granularity of a location area. It is however important to provide multiple techniques and combine them to increase their robustness with respect to possible de-obfuscation attempts performed by adversaries and untrusted parties.

- *Map constraints.* Approaches to location privacy protection usually do not consider map constraints. This represents a limitation, since topological information could help adversaries in reducing location privacy by guessing the identity of the users and by producing more accurate location information. An interesting research direction is then to integrate privacy techniques with Geographical Information System (GIS) maps.

- *Path protection.* Most location privacy solutions are aimed at protecting a single user position. However, future works should extend current solutions to better protect the privacy of the users that are monitored during a certain period of time. This research area is particularly relevant given the ever-increasing interest in tracking services that monitor movements of people, animals, vehicles, and other mobile objects.

6 Conclusions

Location privacy is a challenging research topic that involves technological, legislative, and sociological issues. This chapter discussed technological aspects related to the protection of the privacy of the users in today's globally networked and pervasive society. We investigated privacy threats arising from enhancements in reliability and precision of the mobile technologies. We discussed recent proposals addressing different location privacy issues (i.e., identity protection, position protection, and path protection). We also presented a reference privacy-aware LBS architecture integrating a location-based service with multiple location providers through a privacy-aware middleware. Finally, we discussed some issues that need to be investigated to enable more complex location-based applications.

Acknowledgement

This work was supported in part by the EU, within the 7FP project, under grant agreement 216483 "PrimeLife" and by the Italian MIUR, within PRIN 2006, under project 2006099978 "Basi di dati crittografate".

References

[1] I.F. Akyildiz and J.S.M. Ho. Dynamic mobile user location update for wireless pcs networks. *Wireless Networks*, 1(2):187–196, 1995.

[2] C.A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati. Location-based metadata and negotiation protocols for LBAC in a one-to-many scenario. In *Proc. of the Workshop on Security and Privacy in Mobile and Wireless Networking (SecPri_MobiWi 2006)*, Coimbra, Portugal, May 2006.

[3] C.A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati. Supporting location-based conditions in access control policies. In *Proc. of the ACM Symposium on Information, Computer and Communications Security (ASIACCS'06)*, Taipei, Taiwan, March 2006.

[4] C.A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati. Managing privacy in LBAC systems. In *Proc. of the Second IEEE International Symposium on Pervasive Computing and Ad Hoc Communications (PCAC-07)*, Niagara Falls, Canada, May 2007.

[5] C.A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati. A middleware architecture for integrating privacy preferences and location accuracy. In *Proc. of the 22nd IFIP TC-11 International Information Secutiry Conference (IFIP SEC2007)*, Sandton, South Africa, May 2007.

[6] C.A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati. Location privacy protection through obfuscation-based techniques. In *Proc. of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, Redondo Beach, CA, USA, July 2007.

[7] V. Atluri and H. Shin. Efficient enforcement of security policies based on tracking of mobile users. In *Proc. of the 20th Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, Sophia Antipolis, France, July-August 2006.

[8] L. Barkhuus and A. Dey. Location-based services for mobile telephony: a study of user's privacy concerns. In *Proc. of the 9th IFIP TC13 International Conference on Human-Computer Interaction (INTERACT 2003)*, Zurich, Switzerland, September 2003.

[9] A.R. Beresford and F. Stajano. Mix zones: User privacy in location-aware services. In *Proc. of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW04)*, Orlando, FL, USA, March 2004.

[10] C. Bettini, X.S. Wang, and S. Jajodia. Protecting privacy against location-based personal identification. In *Proc. of the 2nd VLDB Workshop on Secure Data Management*, Trondheim, Norway, September 2005.

[11] Chicago Tribune. *Rental firm uses GPS in speeding fine.* July 2nd, p9. Associated Press: Chicago, IL, 2001.

[12] M. Colbert. A diary study of rendezvousing: implications for position-aware computing and communications for the general public. In *Proc. of the International 2001 ACM SIGGROUP Conference on Supporting Group Work (GROUP 2001)*, Boulder, Colorado, USA, September-October 2001.

[13] L. Cong and W. Zhuang. Hybrid TDOA/AOA mobile user location for wideband CDMA cellular systems. *IEEE Transactions on Wireless Communications*, 1:439–447, July 2002.

[14] T. D'Roza and G. Bilchev. An overview of location-based services. *BT Technology Journal*, 21(1):20–27, January 2003.

[15] M. Duckham and L. Kulik. A formal model of obfuscation and negotiation for location privacy. In *Proc. of the 3rd International Conference PERVASIVE 2005*, Munich, Germany, May 2005.

[16] M. Duckham and L. Kulik. Simulation of obfuscation and negotiation for location privacy. In *Proc. of Conference On Spatial Information Theory (COSIT 2005)*, Ellicottville, New York, USA, September 2005.

[17] M. Duckham and L. Kulik. *Dynamic & Mobile GIS: Investigating Change in Space and Time*, chapter Location privacy and location-aware computing, pages 34–51. Taylor & Francis, 2006.

[18] *Enhanced 911 - Wireless Services*. http://www.fcc.gov/911/enhanced/.

[19] D. Faria and D. Cheriton. No long-term secrets: Location-based security in overprovisioned wireless LANs. In *Proc. of the 3rd ACM Workshop on Hot Topics in Networks (HotNets-III)*, San Diego, CA, USA, November 2004.

[20] S. Garg, M. Kappes, and M. Mani. Wireless access server for quality of service and location based access control in 802.11 networks. In *Proc. of the 7th IEEE Symposium on Computers and Communications (ISCC 2002)*, Taormina/Giardini Naxos, Italy, July 2002.

[21] B. Gedik and L. Liu. Location privacy in mobile systems: A personalized anonymization model. In *Proc. of the 25th International Conference on Distributed Computing Systems (IEEE ICDCS 2005)*, Columbus, Ohio, June 2005.

[22] Geographic Location/Privacy (geopriv). September 2006. http://www.ietf.org/html.charters/geopriv-charter.html.

[23] M. Gruteser, J. Bredin, and D. Grunwald. Path privacy in location-aware computing. In *Proc. of the Second International Conference on Mobile Systems, Application and Services (MobiSys2004)*, Boston, Massachussetts, USA, June 2004.

[24] M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proc. of the 1st International Conference on Mobile Systems, Applications, and Services (MobiSys)*, San Francisco, CA, USA, May 2003.

[25] M. Gruteser and Xuan Liu. Protecting privacy in continuous location-tracking applications. *IEEE Security & Privacy Magazine*, 2(2):28–34, March-April 2004.

[26] C. Hauser and M. Kabatnik. Towards Privacy Support in a Global Location Service. In *Proc. of the IFIP Workshop on IP and ATM Traffic Management (WATM/EUNICE 2001)*, Paris, France, March 2001.

[27] U. Hengartner. Enhancing user privacy in location-based services. Technical Report CACR 2006-27, Centre For Applied Cryptographic Research (CACR), 2006.

[28] U. Hengartner and P. Steenkiste. Protecting access to people location information. In *Proc. of First International Conference on Security in Pervasive Computing*, Boppard, Germany, March 2003.

[29] U. Hengartner and P. Steenkiste. Implementing access control to people location information. In *Proc. of the ACM Symposium on Access Control Models and Technologies 2004 (SACMAT 2004)*, IBM, Yorktown Heights, USA, 2004.

[30] B. Ho and M. Gruteser. Protecting location privacy through path confusion. In *Proc. of IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)*, Athens, Greece, September 2005.

[31] D. Hong, M. Yuan, and V. Y. Shen. Dynamic privacy management: a plug-in service for the middleware in pervasive computing. In *Proc. of the 7th International Conference on Hu-*

man Computer Interaction with Mobile Devices & Services (MobileHCI'05), Salzburg, Austria, September 2005.

[32] H. Hu and D.L. Lee. Energy-efficient monitoring of spatial predicates over moving objects. *Bulletin of the IEEE Computer Society Technical Committee on Data Engineering*, 28(3):19–26, 2005.

[33] M. Langheinrich. Privacy by design-principles of privacy-aware ubiquitous systems. In *Proc. of the 3rd international conference on Ubiquitous Computing (Ubicomp 2001)*, Atlanta, Georgia, USA, September-October 2001.

[34] M. Langheinrich. A privacy awareness system for ubiquitous computing environments. In *Proc. of the 4th International Conference on Ubiquitous Computing (Ubicomp 2002)*, Goteborg, Sweden, September-October 2002.

[35] J-W. Lee. *Location-tracing sparks privacy concerns.* Korea Times. http://times.hankooki.com, 16 November 2004. Accessed 22 December 2006.

[36] G. Myles, A. Friday, and N. Davies. Preserving privacy in environments with location-based applications. *IEEE Pervasive Computing*, 2(1):56–64, 2003.

[37] J. Myllymaki and S. Edlund. Location aggregation from multiple sources. In *Proc. of the 3rd IEEE International Conference on Mobile Data Management (MDM 02)*, Singapore, January 2002.

[38] H. Naguib, G. Coulouris, and S. Mitchell. Middleware support for context-aware multimedia applications. In *Proc. of the IFIP TC6 / WG6.1 3rd International Working Conference on New Developments in Distributed Applications and Interoperable Systems*, Deventer, The Netherlands, September 2001.

[39] K. Nahrstedt, D. Xu, D. Wichadakul, and B. Li. QoS-aware middleware for ubiquitous and heterogeneous environments. *IEEE Communications Magazine*, pages 140–148, November 2001.

[40] J. Nord, K. Synnes, and P. Parnes. An architecture for location aware applications. In *Proc. of the 35th Hawaii International Conference on System Sciences*, Hawaii, USA, January 2002.

[41] Openwave. *Openwave Location Manager*, 2006. http://www.openwave.com/.

[42] B. Parkinson et al. *Global Positioning System: Theory and Application*, volume 163. Volume II, Progress in Austronautics and Aerounautics Series, V-164, American Institute of Astronautics and Aeronautics (AIAA), Reston, Virginia, USA, 1996.

[43] A. Ranganathan, J. Al-Muhtadi, S. Chetan, R. H. Campbell, and M. D. Mickunas. Middlewhere: A middleware for location awareness in ubiquitous computing applications. In *Proc. of the ACM/IFIP/USENIX 5th International Middleware Conference (Middleware 2004)*, Toronto, Ontario, Canada, October 2004.

[44] P. Samarati. Protecting respondents' identities in microdata release. *IEEE Transactions on Knowledge and Data Engineering*, 13(6):1010–1027, 2001.

[45] N. Sastry, U. Shankar, and S. Wagner. Secure verification of location claims. In *Proc. of the ACM Workshop on Wireless Security (WiSe 2003)*, San Diego, CA, USA, September 2003.

[46] G. Sun, J. Chen, W. Guo, and K.J. Ray Liu. Signal processing techniques in network-aided positioning: A survey of state-of-the-art positioning designs. *IEEE Signal Processing Magazine*, July 2005.

[47] U. Varshney. Location management for mobile commerce applications in wireless internet environment. *ACM Transactions on Internet Technology*, 3(3):236–255, August 2003.

[48] G. Zhang and M. Parashar. Dynamic context-aware access control for grid applications. In *Proc. of the 4th International Workshop on Grid Computing (Grid 2003)*, Phoenix, Arizona, November 2003.