Personal Privacy in Mobile Networks

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

Università degli Studi di Milano
Dipartimento di Tecnologie dell'Informazione
Via Bramante 65, 26013 - Crema, Italy
e-mail: {claudio.ardagna,sabrina.decapitani,pierangela.samarati}@unimi.it

Abstract. Technical enhancements of mobile technologies and the pervasive diffusion of mobile devices have radically changed the way in which users communicate and interact. Users stay virtually connected anywhere anytime, and information on their location and mobility is easily available and accessible. As a consequence, new mobile and online applications have been developed, which need the location information of the users to offer enhanced services. However, the availability of such advanced services and functionalities comes at the price of an increasing risk of privacy attacks that aim at monitoring users in every move and activity. This scenario results in a renewed interest in solutions for protecting the privacy of mobile users, especially in those environments where lack of protection may result in persecution, political violence, and government abuses. This chapter first analyzes potential privacy threats in mobile networks and then defines different categories of location privacy (i.e., communication, position, and path privacy). It finally presents several solutions for the protection of location privacy in different setting and mobile networks.

1 Introduction

The widespread availability of powerful mobile devices and high reliable mobile networks allows users to stay virtually connected anywhere anytime, independently from their physical position. Today, most service providers have integrated location technologies in their existing telecommunication infrastructures to reach the new market of mobile services. *Nomadic* users in fact can communicate and access services, while moving on the field. These services, called Location-Based Services (LBSs), have been extensively deployed and exploit the location information of the users to provide enhanced applications (e.g., navigation services, friend finder, personal guide, and social networks). The resulting mobile communication infrastructure offers a new world of mobile services that allow users to make decisions rapidly, also in emergency situations and in those scenarios where violence and persecutions restrict the freedom of speech and think of individuals. Users, for example, can use social media to communicate and divulgate information in real time about events in the above critical scenarios. The other side of the coin is however the widespread availability of a huge amount of personal information of the users that can be exploited by adversaries to compromise the privacy of the users.

The risk of unrestricted and unregulated wireless technologies is the one of the "Big Brother" stereotype: a society where the secondary effect of wireless technologies – whose primary effect is to enable the development of innovative and valuable services – becomes a form of implicit total surveillance of individuals, their habits, their movements, and their activities. Today, this "Big Brother" scenario is becoming more and more a reality rather than just a prediction and must be carefully considered especially in critical scenarios, such as the one of dictatorship, where the regime may use mobile technologies to identify and persecute opponents.

In this chapter, we discuss the importance of protecting personal privacy in mobile environments, including those scenarios where violence and abuses restrict the freedom of individuals and violate human rights. We first describe the mobile scenario in which mobile communications and location-based services prospered and define the concept of location privacy (Section 2). For each category of location privacy identified, we then present some of the existing techniques whose main goal is the protection of the privacy in mobile networks (Section 3 and Section 4). Finally, we present some open research challenges and gives our concluding remarks (Section 5).

2 Mobile Networks: Location Services and Privacy

We consider a scenario where users exploit the mobile network infrastructure to access LBSs. LBSs can be defined as online and distributed applications that require knowledge of the location information of the users. In this scenario, there are typically three main participating entities:

- *mobile users* carry mobile devices supporting several mobile technologies (e.g., WiFi, GSM/3G, GPS);
- *mobile network* provides mobile functionalities, communication facilities, and services to mobile users and sits between mobile users and servers;
- *servers* provide location-based services accessed by mobile users.

Several types of mobile networks currently exist that differ in how the communication is performed and in the technology used. In particular, we distinguish among *WiFi networks*, *cellular networks*, and *mobile ad-hoc networks*. WiFi networks are based on IEEE 802.11 standards, and have been principally introduced to deploy wireless LAN and allow WiFi devices to connect to the Internet. Although, WiFi technology has a limited coverage and its usage is restricted to indoor environments (e.g., buildings, airports, malls) and urban areas covered by hotspots, it achieved a huge success. Cellular networks are used by mobile users who receive signals from radio cells. Mobile users are registered with a given mobile network operator to access cellular functionalities and request services from servers accessible via the network. Cellular networks can be enriched with several different positioning systems that measure the physical location of users carrying mobile devices with good accuracy (Anisetti et al. 2008; Gustafsson and Gunnarsson 2005; Munoz et al. 2009, Song 1994). Finally, mobile ad-hoc networks (MANETs) have been recently introduced. MANETs include mobile routers and hosts that form networks of arbitrary topology by means of wireless communications. Such networks use ad-hoc routing protocols to allow users to establish ad-hoc (WiFi) point-to-point connections with other mobile users in the network and communicate among them. A *Vehicular Ad-Hoc Network* (VANET) is a form of MANET that has been recently deployed and consists of fixed equipments and vehicles equipped with sensors, forming an ad-hoc network and exchanging information.

Many LBSs are today available through mobile networks: Google Latitude and plugins for Facebook and Twitter, proximity-based services (e.g., Where - *www.where.com*), and location-based touristic services such as Guide Project (Cheverst et al. 2000) and mTourist (Deller et al. 2009) are just well know examples of such existing LBSs. In general, LBSs can be classified according to the service provided (Hengartner 2006): *i) nearby-information services* provide information about the environment surrounding the location of a user; *ii) locate-me services* give information about the position of a user; *iii) tracking services* offer information about user movements (e.g., path, velocity, direction) and could be used by online services that track children, employees, or vehicles, warn about dangerous areas, and so on; *iv) locate-friends and nearby-friends services* provide information to subscribers about the real-time location or proximity of other subscribers; *v) personal-navigator services* provide information about the path that has to be followed to reach a target location from the current location of the user.

In the last few years LBSs have also shown their potential in critical contexts, where the availability of a precise location can help in protecting human live. For instance, the enhanced 911 in North America (*www.fcc.gov/911/enhanced*) and 112 in Europe (*ec.europa.eu/information_society/activities/112/index_en.htm*) can immediately dispatch emergency services (e.g., emergency medical services, police, or firefighters) where they are needed, reducing the margins of error. Beside traditional LBSs, users rely on mobile protocols and technologies to simply communicate and access the Internet and its services. Even if such protocols and technologies may not directly require location information to be released, communications on mobile networks still result in the disclosure of location-related information (e.g., mobile user identifiers, location-based requests).

Although LBSs use the location information of the users for providing useful services, privacy concerns are increasing since the improper exposure of location information could result in severe consequences (Duckham and Kulik 2007): users accessing LBSs can be tracked in their movements and become the target of physical attacks or stalking; mobile communications can be eavesdropped, thus collecting which users access which servers and making users vulnerable to political, religious, sexual persecution and discrimination; users may receive unsolicited advertising of products and services available nearby their position; users may be subject to profiling and inferences of personal information (e.g., state of health, points of interest, hobbies).

The proper protection of location privacy (i.e., the protection of the location information) can pursue different objectives, depending on the scenario in which the users are moving and communicating, and on the services with which the users are interacting (Ardagna et al. 2008). Location privacy protection can be aimed at preserving the privacy of the user identity, the privacy of the communication, the single user location measurement, or the movements of the user monitored in a certain period of time. The following categories of location privacy can then be defined.

- *Communication privacy*. The main goal is to hide both the sender and receiver of a message from external parties. An external party should only know that a communication is in place without identifying the involved parties. Communication privacy encompasses *identity privacy,* that is, the protection of the identities associated with or inferable from location information. For instance, many online services provide a person with the ability to establish a relationship with some other entities without her personal identity being disclosed to those entities.
- *Position privacy*. The main goal is to perturb the location of users to protect their physical position. This type of location privacy is suitable for environments where identities of the users are required for a successful service provisioning. An example of a technique that most solutions either explicitly or implicitly exploit consists of scaling a location to a coarser granularity.
- *Path privacy*. The main goal is to protect the privacy of the users who are monitored during a certain period of time. LBSs will no longer receive a single location measurement, but they will gather many samples allowing them to track users.

In the following, we will discuss in more details the current techniques used for guaranteeing the three types of location privacy mentioned above.

3 Communication Privacy

Mobile network research traditionally focuses on providing a communication infrastructure with high performance, efficiency, security, and reliability. However, the advancements in the technology allow the storing, mining, and sharing of a huge amount of users information, thus raising privacy concerns and making the only protection of the content of a communication insufficient (Giannotti and Pedreschi 2008). As a consequence, the need for solutions protecting the *communication privacy* arises. Existing solutions are usually based on the concept of *anonymity* and aim at confusing a user (i.e., its identity or personally identifiable information) within a set of other users, meaning that the user should not be identifiable within the set. In the literature, the techniques and protocols that guarantee communication privacy may adopt the following protection paradigms (Ardagna et al. 2009-2; Reiter and Rubin 1998).

- *Sender anonymity*. It protects the relationship between senders and the messages they send, that is, the identity of the sender of a message must be hidden to all external parties.
- *Receiver anonymity*. It protects the relationship between receivers and the messages they receive, that is, the identity of the receiver of a message must be hidden to all external parties except the sender.
- *Communication anonymity*. It encompasses sender and receiver anonymity, meaning that the identity of both the sender and receiver of a message must be hidden from external parties. Communication anonymity also includes the concept of unlinkability, that is, an observer might know that the sender and receiver are involved in some communications on the network, but does not know with whom each of them communicates.

In the following, we present protocols and techniques aimed to preserve sender and communication anonymity in mobile networks. Receiver anonymity is considered in the context of communication anonymity only, since the protection of receiver anonymity alone does not provide advantages in current LBS scenarios.

3.1 Sender Anonymity

Current anonymizing solutions manipulate location information to prevent re-identification of the sender by adversaries and can be divided in two main classes: *centralized solutions,* where a centralized middleware is responsible for the anonymization process; *decentralized solutions,* where mobile users interact among them to get anonymized. Since the goal consists in hiding the identity of the users, the location information can be released with the best accuracy possible. Many approaches are based on the notion of *k*-anonymity, originally defined in the data-base context (Ciriani et al. 2007; Samarati 2001). *k*-anonymity captures a traditional requirement followed by statistical agencies according to which the released data should be indistinguishably related to no less than a certain number *k* of respondents. Adapting this concept to the context of networks, a user is made not identifiable by releasing a geographical area containing at least *k*-1 other users. In this way a LBS is unable to associate each request with fewer than *k* respondents.

Beresford and Stajano (Beresford and Stajano 2003; Beresford and Stajano 2004) present Mix Zones, a centralized solution that is based on the concepts of application zones, homogeneous application interests in specific geographic areas, and mix zones, areas where a user cannot be tracked. Within each mix zone, the identities of all users are indistinguishable, and users entering the mix zone cannot be linked to users leaving it. Bettini et al. propose a framework to evaluate the risk of disseminating location information (Bettini et al. 2005). They introduce a technique aimed at supporting *k*-anonymity, where the geo-localized history of the requests submitted by a user is defined as a location-based quasi-identifier (i.e., a set of attributes exploitable for linking) and can be used to re-identify the user. LBSs observing the users' requests for services and the sequence of updates to users' locations have then the possibility of identifying the users. The notions of quasi-identifier and *k*-anonymity are used to provide a solution where it is not possible to link a subset of requests to less than *k* users. To achieve *k*-anonymity, *k* different users having a personal history of locations consistent with the set of issued requests must exist. Gruteser and Grunwald propose a middleware architecture and adaptive algorithms that manipulate location information in spatial or temporal dimensions (Gruteser and Grunwald 2003). A first algorithm recursively splits a bi-dimensional space by means of a *quadtree* partition method to decrease the spatial accuracy of location information (spatial cloaking). Spatial cloaking perturbs the location of a requester by enlarging her real position to the smallest area containing *k* users (including the requester). In addition to spatial cloaking, a temporal cloaking algorithm perturbs the location information of the requester in the temporal dimension. A spatial resolution is defined around the requester and, as soon as *k*-1 other users traverse this area, a time interval $[t_1,t_2]$ is generated and released with the area. By construction, in the interval $[t_1,t_2]$, *k* users, including the requester, have traversed the area identified by the spatial resolution parameter, thus satisfying preference *k* of the requester. Mokbel et al. present a framework, named Casper, which includes a *location anonymizer* that perturbs the location information of users to achieve sender *k*-anonymity, and a *privacy-aware query processor* that manages anonymous queries and cloaked spatial areas (Mokbel et al. 2006). In Casper, users define a degree of anonymity *k*, and the best accuracy A_{min} of the area that the user is willing to release. The authors present two alternative techniques for the local anonymizer: *basic* and *adaptive* location anonymizer. Both techniques are based on a pyramid data structure that hierarchically decomposes the spatial space into H levels, where each level *h* has 4^h grid cells; the root is at level *h*=0 and represents the whole area. The basic location anonymizer uses a complete pyramid structure, while the dynamic anonymizer maintains an incomplete pyramid with only the cells that can be potentially used as a cloaked area.

Each cell has an identifier and keeps track of the number of users within it. The system also maintains a hash table that stores information about users (identifiers, privacy profiles, and cell identifiers in which they are located). The same cloaking algorithm is used by the two techniques: if the user is within a cell *c* that already satisfies the privacy profile (k, A_{min}), the cell is returned as the spatial cloaked area; otherwise if the combination between cell *c* and its neighbours satisfies (k, A_{min}), the combination that produces closer value to *k* is returned. If cell *c* cannot be combined with any neighbours, the algorithm is recursively executed with the parent cell of *c* until a valid cell is returned. Gedik and Liu describe a *k*-anonymity model and define a message perturbation engine responsible for providing sender anonymity through identity removal and spatio-temporal obfuscation of location information in the user's requests (Gedik and Liu 2008). User's preferences consist of a minimum anonymity level, and maximum temporal and spatial tolerances. The minimum anonymity level is a value *k* that represents the required number of mobile users in the anonymity set, that is, the users that may potentially have issued the request. The anonymity level can be achieved by either decreasing the location accuracy of the spatial area modelling the sender position or by delaying message forwarding until *k*-1 users visited the area in which the sender resides. The manipulations in spatial and temporal dimensions produce a constraint area that must respect the maximum temporal and spatial tolerances, to maintain a given level of service quality. The message perturbation engine generates anonymous queries through the CliqueCloak algorithm, which is based on a constraint graph that models the anonymization preferences of each message (i.e., the preference of the user sending the message). Each vertex in the constraint graph represents a message submitted by a user, and two vertices are connected if and only if the real position of each user belongs to the constraint area of the other user. A valid *k*-anonymous perturbation of a message *m* is found if a set of at least other *k*-1 messages form an *l*-clique (i.e., a partition of the graph including *l* messages), and the anonymity level of each message is less than *l*. This means that the anonymization process considers the preferences of all the parties involved. Masoumzadeh et al. provide a solution to anonymize location-based queries, guaranteeing anonymity in specific time windows (Masoumzadeh et al. 2009). The proposed solution is based on (*k*-*T*)-anonymity meaning that for each query at least other *k*-1 queries have been issued in the timeframe *T*. Bamba et al. introduce PrivacyGrid a framework to support anonymous location-based queries (Bamba et al. 2008). The users define their preferences using a P3P profile for location privacy. Grid cloaking algorithms are then defined to provide *k*-anonymity and *l*-diversity. In this context, location *l*-diversity ensures that the identities of the mobile users cannot be associated to less than *l* physical positions; in other words, it avoids location inferences when there are more users at a single physical location. PrivacyGrid supports temporal cloaking to improve performance and success rate.

Focusing on decentralized approaches, Ghinita et al. propose PRIVè, a decentralized architecture and an algorithm (hilbASR) for protecting sender anonymity of users querying LBSs (Ghinita et al. 2007). The hilbASR algorithm is based on the definition of *k*-anonymous areas through the Hilbert space-filling curve. Specifically, 2D positions of users are mapped in 1D values, which are used to group users in buckets of *k* (anonymity areas). The proposed algorithm is resistant to attacks that exploit information on the distribution of the users in the area of interest. By construction, in fact, the hilbASR algorithm supports the reciprocity property, meaning that, when the algorithm is applied to all users in an anonymity area, the same anonymity area is produced. Hashem and Kulik present a decentralized approach to anonymity in a mobile ad-hoc network, which combines *k*-anonymity with obfuscation (Hashem and Kulik 2007). Each user is responsible for generating her cloaked area as follows: *1)* the user obfuscates her position by substituting the precise location with a locally cloaked area (LCA); *2)* the user anonymizes her request by manipulating the LCA to a global cloaked area (GCA including the LCAs of at least other *k*-1 users. An anonymous algorithm selects a query requester in the GCA with near-uniform randomness, thus ensuring sender anonymity. Cornelius et al. discuss the problem of protecting the privacy of the users involved in large-scale mobile applications based on collaborative and opportunistic sensing by mobile devices (Cornelius et al. 2008). The authors popose a privacy-aware architecture, called AnonySense, where applications can distribute sensing tasks to anonymous mobile devices, and receive anonymized (but verifiable) sensor data reports in response.

Recent works proposed hybrid solutions that try to mix centralized and decentralized approaches. Zhang and Huang present a framework called HiSC for location and query anonymization (Zhang and Huang 2008). The proposed solution relies on a hybrid approach that balances the load on anonymizing server and mobile clients. The space is partitioned in cells (quadtree partitioning) and each mobile client selects a set of these cells as her surrounding area. The number of mobile clients in this area is maintained by both the anonymizing server and the client, thus allowing centralized and decentralized anonymization service.

3.2 Communication Anonymity

Past research focused on communication anonymity aims at preserving the privacy of wireless and mobile traffic in mobile and vehicular ad-hoc networks, wireless mesh networks, and mobile hybrid networks.

In the context of MANETs, research on privacy protection aimed to preserve the privacy of wireless traffic by studying and providing privacy-enhanced and anonymous communication infrastructures. The first routing protocols, such as AODV (Perkins and Royer 1999) and DSR (Johnson and Maltz 1996), were targeted on providing network performance, efficiency, security, and reliability. No privacy requirements were considered exposing these protocols to privacy violations that exploited the protocol state stored in each node (e.g., sender, receiver, and hop-count of each communication). Subsequent works focused on routing protocols for MANETs that attempt to protect anonymity and privacy by hiding sender and receiver identities to intermediate nodes. A number of anonymous routing protocols have then been presented. MASK proposes an anonymous routing protocol, which provides MAC- and network-layer communications that hide the real identities of the participating nodes (Zhang et al. 2006). It also provides communication anonymity and end-to-end flow untraceability. MASK uses dynamic pseudonyms and pairing-based cryptography to establish an anonymous neighbourhood authentication between nodes and an anonymous network-layer communication. SDAR proposes a novel distributed routing protocol that guarantees security, anonymity, and high reliability of the route (Boukerche et al. 2004). SDAR relies on the encryption of packet headers and allows trustworthy intermediate nodes to participate in the path construction protocol without affecting the anonymity of the nodes involved in the communication. ANODR provides a routing protocol protecting communication anonymity, by preventing adversaries from following packets in the network, and location privacy, by preventing adversaries to discover the real position of local transmitters (Kong and Hong 2003). Shokri et al. present the PseudoAODV protocol, an extension of AODV where real identifiers of nodes are substituted with random pseudonyms (Shokri et al. 2007). The protocol provides sender/recipient and relationship anonymity. Dong et al. propose an anonymous protocol that protects the identity and location of the nodes, and provides multipath communication (Dong et al. 2009). Multiple anonymous routes are employed to assure random route transmission; also, the protocol provides fake routes. Data packets are forwarded in both the real and the fake routes to confuse adversaries, at a price of an increased communication overhead.

Recently, few works have focused on security and privacy problems in VANETs, where breaches in security and privacy protection can result in attacks subverting the normal network behaviour and violating the privacy of the users. Raya and Hubaux propose a first investigation of the security problem in VANETs and provide a threat model analyzing communication aspects, attacks, and security requirements (Raya and Hubaux 2005). They also propose some early privacy solutions based on digital signature, cryptographic keys, and anonymous public/private key pairs. Lin et al. present a secure and privacy-preserving protocol that integrates the techniques of Group Signature and Identity-based Signature, called GSIS (Lin et al. 2007). In case of a traffic event dispute (e.g., a crime or a car accident) the proposed protocol provides a means to reveal the ID of the sender of the message to the authority. Sampigethaya et al. present AMOEBA, a robust location privacy scheme based on vehicular groups and random silent periods for protecting users privacy against malicious parties aiming at tracking vehicles (Sampigethaya et al 2007).

Finally, other works face the problem of protecting privacy in recently deployed wireless mesh and hybrid networks. Ren and Lou present a privacy yet accountable security framework based on multiparty computation and groups of users established a priori, with a semitrusted group manager and network operator (Ren and Lou 2008). Capkun et al. provide a scheme for secure and privacy-preserving communications in hybrid ad-hoc networks (Capkun et al. 2004). The proposed solution is based on continuously changing pseudonyms and cryptographic keys, and provides secure and privacy-preserving communications in hybrid ad-hoc networks. Ardagna et al. consider the problem of protecting communication privacy in the context of mobile hybrid networks, where users can simultaneously create WiFi point-to-point connections, join the cellular network, and access the Internet through their mobile phones (Ardagna et al. 2008). The proposed solution is based on *k*-anonymity and protects communication privacy of the users against honest-but-curious mobile network operators. Using a multi-path communication paradigm, a mobile user can achieve communication *k*-anonymity by distributing, using the WiFi network, different packets of the same message to *k* neighbouring mobile peers, which then forward the received packets through the cellular network. This scheme achieves *k*-anonymity because the mobile network operator is not able to associate the users' data flow with fewer than *k* peers.

4 Position and Path Privacy

Solutions for the protection of position privacy perturb the location of the users to preserve their privacy. Obfuscation is the process used to degrade the accuracy of the location information and, differently from other techniques, perturbs the location information still maintaining a binding with the identity of the users. Duckham and Kulik define a framework with a mechanism that balances the needs of the users for high-quality LBSs and for location privacy (Duckham and Kulik 2005-1). The proposed solution is based on the *imprecision concept*, which indicates the lack of specificity of location information (e.g., a user located in Milan is said to be in Italy). The authors propose to degrade location information quality by adding *n* points, at the same probability, to the real user position. The algorithm assumes a graph-based representation of the environment. When a user accesses a LBS asking for information about services in the neighbourhood, the location of the user is perturbed by releasing a set of points, also containing the real position of the user. The service calculates an imprecise query result that is returned to the user. Duckham and Kulik also present some obfuscation methods that are validated and evaluated through a set of simulations (Duckham and Kulik 2005-2). Ardagna et al. present 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 (Ardagna et al. 2007-1; Ardagna et al. 2009). Key aspects of the proposal are to permit the specification of privacy preferences in a simple and intuitive way, and to make the enforcement of privacy preferences manageable for location-based services, while preserving their quality. The authors introduce the concept of *relevance* as a metric for the accuracy of location information, abstracting from any physical attribute of sensing technology. This metric also permits to quantitatively evaluate the degree of privacy introduced into a location measurement and is adopted by users to define their privacy preferences. Based on relevance preferences, different obfuscation-based techniques and their composition are discussed. Finally, the concept of robustness is introduced to evaluate the strength of the proposed techniques against different types of adversaries.

Other relevant works consider path privacy protection when LBSs access many consecutive location samples of the users. Ghinita gives an overview of the state-of-the-art in the areas of private location-based queries and trajectory anonymization (Ghinita 2009). Gruteser and Liu define three algorithms aimed at path privacy protection, *base*, *bounded-rate*, and *k-area*, that build on the definition of a sensitivity map composed of sensitive and insensitive zones (Gruteser and Liu 2004). The base algorithm is the simplest algorithm and releases location updates that belong to insensitive areas only, without considering possible inferences made by adversaries. The bounded-rate algorithm permits the customization of location update frequency to reduce the amount of information released near a sensitive zone and to make the adversary process more difficult. Finally, the *k*-area algorithm is built on top of sensitivity maps that are composed of areas containing *k* sensitive zones. Location updates of a user entering a region with *k* sensitive areas are temporarily stored and not released. If a user leaving that region has visited at least one of the *k* sensitive areas, location updates are suppressed, otherwise they are released. Hoh and Gruteser introduce a path confusion algorithm (Hoh and Gruteser 2005). This algorithm is aimed at creating cross paths of at least two users, such that the attacker cannot retrieve the path followed by a specific user. Xu and Cai provide a cloaking algorithm for protecting trajectories of mobile users (Xu and Cai 2009). First of all, they put forward the idea that users need a simpler method for defining their preferences. Choosing *k* as a privacy preference is in fact difficult for users that have not an immediate understanding of what this choice means in terms of privacy and quality of service. The authors suggest to let the users define a *public region* as their preference with the restriction that the disclosed locations are at least popular as that region, where the popularity is calculated on the basis of footprints that mobile users have in that area. Although this preference mechanism fits well existing solutions that only anonymize a single sample of users' location, this is not true for the anonymization of trajectories. To avoid intersection attacks that try to identify common visitors of consecutive cloaking areas in the trajectory, the idea is to use those users visiting most places in the target region for anonymization. This solution is necessary because users movements are not known a-priori. Finally, Hoh et al. implement a solution for a privacy preserving traffic monitoring, where GPS receivers are installed on probe vehicles and release information about their position (Hoh et al. 2008). The concept of virtual trip lines is introduced. As soon as a probe vehicle crosses one of the lines, a location update is released. This update is split in two parts: identification information and sensing measurements that are accessible by an ID proxy server and a traffic monitoring server, respectively. An extension for temporal cloaking is introduced to guarantee *k*-anonymity also in case of low density.

5 Conclusions and Future Work

The protection of location privacy is a fundamental requirement in today's globally interconnected and pervasive society, where users rely on their mobile devices to communicate and access services. Privacy issues become then critical, especially in those contexts where lack of protection may result in persecutions, political violence, and government abuses. As a consequence, the need for solutions that protect the privacy of mobile users arises. This chapter discussed location privacy issues from a technological point of view, providing a general definition of location privacy. It also presented recent proposals that aim to address different aspects of the location privacy problem, such as, communication privacy, location privacy, and path privacy. The continuous evolution of mobile technologies leaves open many research issues that need to be further investigated: *i)* the definition of solutions that balance the privacy of the users with the accuracy of the location-based services, *ii)* the consideration of new adversary models where also the mobile network operators are potential adversaries that try to eavesdrop on the users' communications, *iii)* the definition of privacy solutions for mobile hybrid networks that mix functionalities from different types of networks (e.g., wired, wireless, ad-hoc).

Acknowledgements

This work was supported in part by the EU within the 7FP project "PrimeLife" under grant agreement 216483.

Bibliography

Anisetti, M., Ardagna, C.A., Bellandi, V., Damiani, E., Reale, S. (February 2008). Advanced Localization of Mobile Terminal in Cellular Network. *International Journal of Communications, Network and System Sciences (IJCNS)*, Scientific Research Publishing, 1:95-103.

Ardagna, C.A., Cremonini, M., Damiani, E., De Capitani di Vimercati, S., Samarati, P. (July 2007). *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.

Ardagna, C.A., Cremonini, E., De Capitani di Vimercati, S., Samarati, P. (2008). Location Privacy in Pervasive Computing. In Gritzalis, Karygiannis, Skianis (eds.), *Security and Privacy in Mobile and Wireless Networking*, Troubador Publishing.

Ardagna, C.A., Cremonini, E., De Capitani di Vimercati, S., Samarati, P. (2010). An Obfuscation-based Approach for Protecting Location Privacy. *IEEE Transaction on Dependable and Secure Computing*. (to appear)

Ardagna, C.A., Jajodia, S., Samarati, P., Stavrou, A. (2009). Privacy Preservation over Untrusted Mobile Networks. In Bettini, Jajodia, Samarati, Wang (eds.), *Privacy in Location Based Applications*, Springer.

Ardagna, C.A., Stavrou, A., Jajodia, S., Samarati, P., Martin, R. (October 2008). *A multi-path approach for k-anonymity in mobile hybrid networks*. In Proc. of the International Workshop on Privacy in Location-Based Applications (PiLBA 2008), Malaga, Spain.

Bamba, B., Liu, L., Pesti, P., Wang T. (April 2008). *Supporting Anonymous Location Queries in Mobile Environments with PrivacyGrid*. In Proc. of the 17th International World Wide Web Conference (WWW 2008), Beijing, China.

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

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

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

Boukerche, A., El-Khatib, K., Xu, L., Korba, L. (October 2004). *SDAR: A secure distributed anonymous routing protocol for wireless andmobile ad hoc networks*. In Proc. of the 29th Annual IEEE International Conference on Local Computer Networks (LCN 2004), Tampa, FL, USA.

Capkun, S., Hubaux, J.-P., Jakobsson M. (January 2004). *Secure and Privacy-Preserving Communication in Hybrid Ad Hoc Networks*. Technical Report IC/2004/10, EPFL-IC, CH-1015 Lausanne, Switzerland.

Cheverst, K., Davies, N., Mitchell, K., Friday, A. (August 2000). *Experiences of developing and deploying a context-aware tourist guide: The guide project*. In Proc. of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM 2000), Boston, MA, USA.

Ciriani, V., De Capitani di Vimercati, S., Foresti, S., Samarati, P. (2007). k-Anonymity. In Yu, Jajodia (eds.), *Secure Data Management in Decentralized Systems*. Springer-Verlag.

Cornelius, C., Kapadia, A., Kotz, D., Peebles, D., Shin, M., Triandopoulos, N. (June 2008). *Anonysense: privacy-aware people-centric sensing*. In Proc. of the 6th International Conference on Mobile Systems, Applications, and Services (MobiSys 2008), Breckenridge, CO, USA.

Deller, M., Kockerandl, G., Jans, S., Limam, L. (April 2009). *MoidEx: Location-based mTourism system on mobile devices*. In Proc. of the International Conference on Multimedia and Systems (ICMCS 2009), Ouarzazate, Morocco.

Dong, Y., Chim, T., Li, V., Yiu, S., Hui, C. (2009). Armr: Anonymous routing protocol with multiple routes for communications in mobile ad hoc networks. *Ad Hoc Networks*, 7(8):1536–1550.

Duckham, M., & Kulik, L. (May 2005). *A formal model of obfuscation and negotiation for location privacy*. In Proc. of the 3rd International Conference Pervasive Computing (PERVASIVE 2005), Munich, Germany.

Duckham, M., & Kulik, L. (September 2005). *Simulation of obfuscation and negotiation for location privacy*. In Proc. of the Conference on Spatial Information Theory (COSIT 2005), Ellicottville, NY, USA.

Duckham, M., & Kulik, L. (2007). Location privacy and location-aware computing. In Drummond, J., Billen, R., and Joao, E. (eds.), *Dynamic and Mobile GIS: Investigating Change in Space and Time*, Taylor & Francis, Boca Raton, FL, USA.

Gedik, B., & Liu, L. (January 2008). Protecting location privacy with personalized k-anonymity: Architecture and algorithms. *IEEE Transactions on Mobile Computing*, 7(1):1–18.

General Assembly of the United Nations (December 1948). *Universal Declaration of Human Rights*. United Nations Resolution 217 A (III).

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

Ghinita, G., Kalnis, P., Skiadopoulos, S. (May 2007). *Privè: Anonymous location-based queries in distributed mobile systems*. In Proc. of the International World Wide Web Conference (WWW 2007), Banff, Canada.

Giannotti, F., & Pedreschi, D. (2008). *Mobility, data mining and privacy - Geographic knowledge discovery*. Springer.

Gruteser, M., & Grunwald, D. (May 2003). *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 2003), San Francisco, CA, USA.

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

Gustafsson, F., & Gunnarsson, F. (2005). Mobile positioning using wireless networks: possibilities and fundamental limitations based on available wireless network measurements. *IEEE Signal Processing Magazine*, 22(4):41–53.

Hashem, T., & Kulik, L. (September 2007). *Safeguarding location privacy in wireless ad-hoc networks*. In Proc. of the 9th International Conference on Ubiquitous Computing (UbiComp 2007), Innsbruck, Austria.

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

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

Hoh, B., Gruteser, M., Herring, R., Bana, J., Work, D., Herrera, J.-C., Bayen, A.M., Annavaramb, M., Jacobsonc, Q. (June 2008). *Virtual Trip Lines for Distributed Privacy-Preserving Traffic*. In Proc. of the International Conference on Mobile Systems, Applications, and Services (MobiSys 2008), Breckenridge, CO, USA.

Johnson, D.B., & Maltz, D.A. (1996). *Dynamic Source Routing in Ad Hoc Wireless Networks*. Volume 353. Kluwer Academic Publishers.

Kong, J., & Hong, X. (June 2003). *ANODR: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks*. In Proc. of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC 2003), Annapolis, MD, USA.

Lin, X., Sun, X., Ho, P.H., Shen, X. (November 2007). GSIS: A secure and privacy preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology* 56(6):3442–3456.

Masoumzadeh, A., Joshi, J., Karimi, H.A. (November 2009). *LBS (k,T)-Anonymity: A Spatio-Temporal Approach to Anonymity for Location-Based Service Users*. In Proc. of the 17th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, Seattle, WA, USA.

Mokbel, M., Chow, C.Y., Aref, W. (September 2006). *The new casper: Query processing for location services without compromising privacy*. In Proc. of the 32nd International Conference on Very Large Data Bases (VLDB 2006), Seoul, Korea.

Munoz, D., Lara, F.B., Vargas, C., and Enriquez-Caldera, R. (2009). *Position Location Techniques and Applications*. Academic Press.

Perkins, C., & Royer, E. (February 1999). *Ad-hoc on demand distance vector routing*. In Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA99), New Orleans, LA, USA.

Raya, M., & Hubaux, J.P. (November 2005) *The security of vehicular ad hoc neworks*. In Proc. of the 3rd ACM Workshop on Security of Ad hoc and Sensor Networks (SASN 2005), Alexandria, VA, USA.

Reiter, M., & Rubin, A. (1998). Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security*, 1(1):66–92.

Ren, K., & Lou, W. (June 2008). *A sophisticated privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks*. In Proc. of the 28th IEEE International Conference on Distributed Computing Systems (ICDCS 2008), Beijing, China.

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

Sampigethaya, K., Li, M., Huang, L., Poovendran, R. (October 2007). AMOEBA: Robust location privacy scheme for VANET. *IEEE Journal on Selected Areas in Communications*, 25(8):1569–1589.

Shokri, R., Yabandeh, M., Yazdani, N. (April 2007). *Anonymous Routing in MANET using Random Identifiers*. In Proc. of the 6th International Conference on Networking (ICN 2007), Sainte-Luce, Martinique.

Song, H.L. (November 1994). Automatic vehicle location in cellular communications systems. *IEEE Transaction on Vehicular Technology*, 43(4):902–908.

Xu, T., & Cai, Y. (November 2009). *Feeling-based Location Privacy Protection for Location-based Services*. In Proc. of the ACM Conference on Computer and Communications Security (CCS 2009), Chicago, IL, USA.

Zhang, C., & Huang, Y. (2008). Cloaking locations for anonymous location based services: A hybrid approach. *GeoInformatica*, 159-182, Springer.

Zhang, Y., Liu, W., Lou, W., Fang, Y. (September 2006). Mask: Anonymous on-demand routing in mobile ad hoc networks. *IEEE Transaction on Wireless Communications*, 5(9):2376-2385.