Privacy Preservation over Untrusted Mobile Networks

C.A. Ardagna[1] S. Jajodia[2] P. Samarati[1] A. Stavrou[2]

[1] Dipartimento di Tecnologie dell'Informazione
Università degli Studi di Milano
Via Bramante, 65 - Crema, Italy
{*claudio.ardagna,pierangela.samarati*}*@unimi.it*
[2] CSIS - George Mason University
Fairfax, VA, USA 22030-4444
{*jajodia,astavrou*}*@gmu.edu*

Abstract. The proliferation of mobile devices has given rise to novel user-centric applications and services. In current mobile systems, users gain access to remote servers over mobile network operators. These operators are typically assumed to be trusted and to manage the information they collect in a privacy-preserving way. Such information, however, is extremely sensitive and coveted by many companies, which may use it to improve their business. In this context, safeguarding the users' privacy against the prying eyes of the network operators is an emerging requirement.
In this chapter, we first present a survey of existing state-of-the-art protection mechanisms and their challenges when deployed in the context of wired and wireless networks. Moreover, we illustrate recent and ongoing research that attempts to address different aspects of privacy in mobile applications. Furthermore, we present a new proposal to ensure private communication in the context of hybrid mobile networks, which integrate wired, wireless and cellular technologies. We conclude by outlining open problems and possible future research directions.

1 Introduction

Recent advancements in mobile sensing technologies and the growth of wireless and cellular networks have radically changed the working environment that people use to perform everyday tasks. Today, people are used to be online and stay connected independently of their physical location. This ubiquitous connectivity empowers them with access to a wealth of mobile services. Furthermore, the ease of use of mobile e-commerce and location-based services has fostered the development of enhanced mobile applications [1–3].

Unfortunately, the pervasiveness, the accuracy, and the broadcast nature of wireless technologies can easily become the next privacy attack

vector, exposing a wide-range of information about everyday activities and personal lives to unauthorized eyes. The worst case scenario that analysts have foreseen as a consequence of an unrestricted and unregulated availability of wireless technologies recalls 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. Today, this "Big Brother" scenario is becoming more and more a reality rather than just a prediction. Some recent examples can provide an idea of the extent of the problem. In September 2007, Capla Kesting Fine Art announced the plan of building a cell tower, near Brooklyn NY, able to capture, monitor and rebroadcast wireless signals and communications to ensure public safety [4]. In addition, in 2007, the US Congress approved changes to the 1978 Foreign Intelligence Surveillance Act giving to NSA the authorization to monitor domestic phone conversations and e-mails including those stemming from the cellular network and the Internet. This legislation provides the legal grounds for the cell tower's construction and for the monitoring of users communications in the cellular network. Furthermore, there are numerous examples of rental companies that employed GPS technology to track cars and charge users for agreement infringements [5], or organizations using a location service to track their own employees [6]. The question of what constitutes a legitimate and user-approved use of the mobile tracking technology remains unclear and can only become worse in the near future.

In today's scenario, concerns about the protection of users' privacy represent one of the main reasons that limit the widespread diffusion of mobile services. Although the need of privacy solutions for mobile users arises, existing solutions are only palliative and weak in mobile contexts. Privacy solutions in fact primarily focus on protecting the users against services that collect the users' personal data for service provisioning. However, the advent of cellular (and in general hybrid) networks has made the problem of protecting the users' privacy worse: users should also be protected from the prying eyes of mobile peers and mobile network operators. The operators are in a privileged position, able to observe and analyze each communication on the network. As a consequence, they have the capability to generate, share, and maintain precise profiles of the users over long periods of time. Such profiles include personal information, such as, for instance, servers visited and points of interest, shopping and travel habits among other things. This scenario introduces a new set of requirements to be addressed in the protection of users' privacy. In particular,

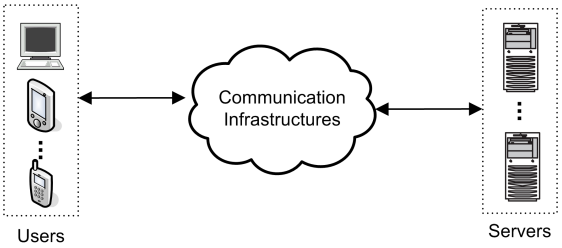

Fig. 1. Basic scenario

there is a pressing need for a mechanism that protects the communication privacy of mobile users. Such a mechanism should depart from the traditional privacy view, and consider a new threat model including operators and peers as potential adversaries. This new view of the problem is especially valid in the context of mobile hybrid networks, where users can communicate on different networks (e.g., wired, WiFi, cellular).

The remainder of this chapter is organized as follows. Section 2 illustrates basic concepts on network privacy protection. Section 3 presents recent proposals and ongoing work addressing different privacy issues in distributed and mobile networks and applications. Section 4 discusses emerging trends and a new vision of privacy in the field of mobile hybrid networks, and presents a new approach for preserving communication privacy in hybrid networks. Section 5 presents open problems and future work. Finally, Section 6 concludes the chapter.

2 Basic Concepts on Network Privacy Protection

Regardless of the technology implemented, a network infrastructure is composed at an abstract level by three main entities (see Figure 1): *users*, who join the network to interact with and access, *servers* and *communication infrastructures*, that provide the platforms enabling communications between users and servers.

Research on distributed and mobile networks has traditionally focused on providing a communication infrastructure with high performance, efficiency, security, and reliability. Today, technology improvements provide solutions to efficiently store, mine, and share huge amount of users information, thus raising privacy concerns [7]. Privacy solutions are then needed and can be aimed at protecting different aspects of a communication, depending on the scenario and on the adversary model. In this chapter, we focus on protecting the information related to the fact that

given parties communicate to each other (communication privacy). We do not discuss the problem of protecting the content of a communication (i.e., integrity and confidentiality), assuming that communication content can be protected by exploiting classical techniques [8]. Also, the vast amount of information exchanged, especially when users surf the Web, makes solutions that protect only communications content inadequate. The privacy of the identities of the participating parties has to be also preserved.

Different protection paradigms have been defined for preserving the privacy of the communications. Typically, they are based on the concept of *anonymity*. Anonymity states that an individual (i.e., the identity or personally identifiable information of an individual) should not be identifiable within an *anonymity set*, that is, a set of users. In the context of network communications, the following protection paradigms have been defined [9].

- *Sender anonymity.* It refers to the communication originator: the identity of the sender of a message must be hidden to external parties (including the receiver itself).
- *Receiver anonymity.* It refers to the communication destination: the identity of the receiver of a message must be hidden to external parties (not including the sender).
- *Communication anonymity.* It encompasses sender and receiver anonymity: the identity of both the sender and receiver of a message must be hidden from external parties. An external party only knows that a communication is in place. Communication anonymity also includes the concept of *unlinkability*, meaning that 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.

Similar protection paradigms can be introduced based on the concept of k-anonymity, rather than anonymity. k-anonymity has been originally defined in the context of databases [10, 11] and 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, we can consider the definition of sender, receiver, and communication k-anonymity.

When the above paradigms are used, an important aspect to consider is the adversary against which anonymity is to be guaranteed. Several

solutions have been developed to protect the privacy of the communication against *i)* the *servers* providing services, *ii) external parties* which can observe the communication, and *iii) internal observers* that reside in the network of the target user. Some works have also assumed the entities responsible for the management of the communication infrastructure (i.e., network operators) as potential adversaries [12]. This latter scenario poses an entirely different set of requirements in the context of mobile hybrid networks, and requires therefore careful consideration and ad-hoc solutions (Section 4).

3 Overview of related and ongoing research

While the deployment and management of mobile networks have been considered in earlier research in the area of mobile applications, approaches aimed at protecting the privacy of users have gained great relevance only in the last few years. Furthermore, research in the context of mobile networks has typically approached the privacy problem from the perspective of providing anonymous communications. In this section, we first provide a survey of the solutions that offer communication anonymity in the context of wired networks and their problems when applied to mobile networks (Section 3.1). We then discuss two different lines of research on anonymity in mobile networks. First, we discuss techniques inspired by the work on wired networks (Section 3.2). These solutions are aimed at providing communication anonymity by means of anonymous routing algorithms in the context of mobile ad-hoc networks. Second, we discuss techniques to be used in the context of location-based services (Section 3.3). These approaches focus on protecting the sender anonymity at the application layer against untrusted servers.

3.1 Communication Anonymity in Wired Networks

Chaum introduces a technique based on public key cryptography and the concept of "mix" to provide sender anonymity and communication untraceability [13]. The basic idea consists in forwarding each communication from sender to receiver through one or more mixes, which form a *mix network*. A mix is responsible for collecting a number of messages from different senders, shuffle them, and forward them to the next destination (possibly another mix node) in random order. The main purpose of each mix node is then to break the link between ingoing and outgoing messages, making the end-to-end communication untraceable and its

tracking impervious for the adversaries. In addition, each mix node only knows the node from which a message is received and the one to which the message is to be sent. This makes mix networks strong against malicious mixes, unless all the mixes in a message path from sender to receiver are compromised and collude with the adversary. The return path is statically determined by the message sender and forwarded as a part of the message sent to the receiver. The receiver uses it to communicate back to the sender, thus preserving the users anonymity. As a result, Chaum's mix network provides a solution where adversaries are not able to follow an end-to-end communication.

Onion routing is a solution that exploits the notion of mix network to provide an anonymous communication infrastructure over the Internet [14, 15]. Onion routing provides connections resistant to traffic analysis and eavesdropping, and is well suited for real-time and bi-directional communications. In onion routing, the sender creates the path of the connection through the onion routing network by means of an *onion proxy* that knows the network topology. The proxy produces an anonymous path to the destination, composed by several *onion routers*, and an *onion*, that is, a data structure composed by a layer of encryption for each router in the path, to be used in the sender-receiver communication. Once the path and the onion are established the message is sent through the anonymous connection. Each onion router receiving the message, peels off its layer of the onion, thus identifying the next hop, and sends the remaining part of the onion to the next router. Onion routers are connected by permanent socket connections. Similarly to mixes in mix networks, onion routers only know the previous and next hops of a communication. At the end, the message reaches the receiver in plain-text. Backward communications happen on the same anonymous path. This solution provides anonymity against internal and external adversaries (i.e., Internet routers and onion routers, respectively), since an adversary is able neither to infer the content of the message nor to link the sender to the receiver. The network only observes that a communication is taking place. Figure 2 shows an example of anonymous connection [16]. Black computer represents an onion router, while white one an onion proxy. Thick lines represent encrypted connections and thin ones a socket connection in clear. Different connections involving the same sender may require the establishment of different anonymous connections. At the end of a communication, the sender sends a destroy message. The path is then destroyed and each router deletes any information it knows about it. TOR is a second generation onion routing-based solution that provides anonymity by preventing

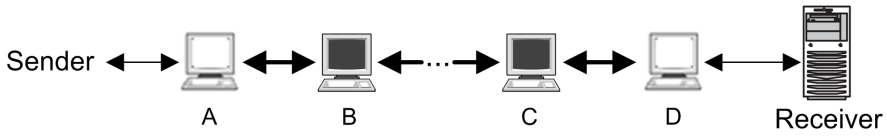

Fig. 2. Anonymous connection in an Onion Routing infrastructure

adversaries from following packets from a sender to a receiver and vice versa [17]. In addition to traditional anonymous routing, TOR allows the sender to remain anonymous to the receiver. TOR addresses some limitations affecting the original design of onion routing by adding perfect forward secrecy, congestion control, directory servers, integrity checking, configurable exit policies, and a practical design for location-hidden services via rendezvous points [17]. In TOR, the onion proxy responsible to define the anonymous connection is installed on the user's machine. When the user needs to communicate with another party, the proxy establishes the anonymous path and generates the onion. Then, the message (including the onion) is sent through the path. Each router receiving the message removes, by using its private key, a layer of encryption to the onion to know its successor. At the end of the path, the receiver node retrieves the message in plain-text. Backward communications happen on the same anonymous connection.

Another anonymizing solution, designed for Web-communications, is Crowds [9]. In Crowds, the routing path and its length are dynamically generated. A user starts a process, called *jondo*, on her computer to join a *crowd* (i.e., a set of users) through a server, called *blender*. The blender receives a connection request from the jondo and decides if the jondo is allowed to join the crowd. If the jondo is admitted, it receives all the information to interact within the crowd. After this, the blender is no longer involved in the communication. All the user requests are sent to the jondo. The first request by a user is used to start the path establishment as follows. The user's jondo selects another jondo in the crowd (including itself) and forwards the request to it. Upon receiving the request, the receiving jondo either forwards the request to another jondo or sends it to the end server, with probability p_f. As a result, the request starts from the user's browser, follows a random number of jondos, and, eventually, is presented to the end server. As soon as a path is built, every request from the same jondo follows the same path, except for the end server (which may vary depending on to whom the user wants to send a message). The server response uses the same path as the user request. The path is

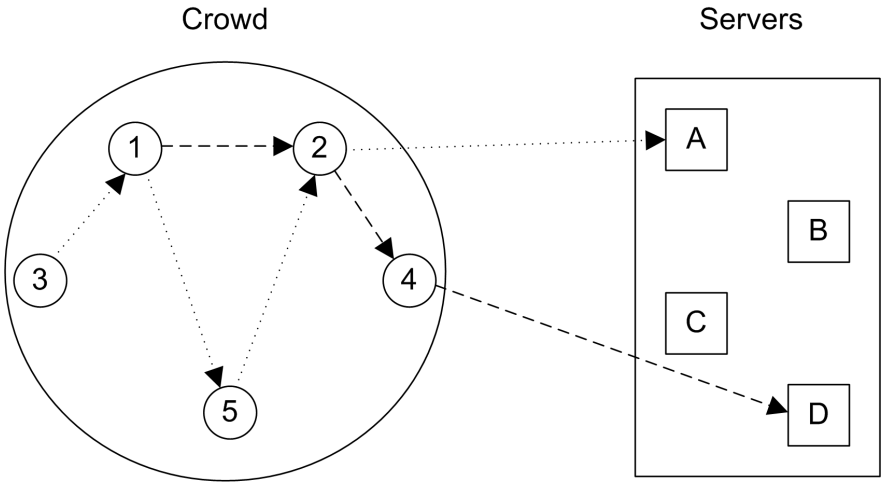

Fig. 3. Two paths in Crowds

changed when a new jondo joins the crowd or a jondo leaves it. Figure 3 shows a crowd composed of five jondos, on which two paths have been defined: 3→1→5→2→A (dotted lines) and 1→2→4→D (dashed lines). From an attacker point of view, the end server receiving a request cannot distinguish the sender among the users in the crowd. Also, collaborating users cannot know if a user is the sender or merely a node forwarding the request. Crowds is also robust against local eavesdroppers that observe all the communications of a given node in a crowd. In fact, although a local eavesdropper can understand if a user is the sender, it never knows the receiver (i.e., the server), since the receiver resides in a different domain.

The solutions presented above aim at providing anonymous communications for protecting the privacy of the users in wired networks (e.g., Internet). Such solutions are not well suited for a mobile scenario, where users can wander freely while initiating transactions and communications by means of terminal devices like cell phones (GSM and 3G). In fact, solutions for wired networks: *1)* assume that the path generated by the sender is used both for the request and the response, *2)* assume a known network topology to create meaningful routes, and *3)* often rely on trusted third parties (e.g., mix, onion router, blender) and on heavy multiparty computation. These assumptions however do not hold for a mobile environment. In fact, mobile users: *1)* move fast over time, making the path used for the request likely to be not available both for the response, *2)* form networks

of arbitrary topology, and *3)* use devices with limited capabilities, and then not suitable for solutions based on multiparty computation.

3.2 Communication Anonymity in Mobile Ad-Hoc Networks

In the context of mobile ad-hoc networks (MANETs), research on privacy protection has focused on preserving the privacy of wireless traffic by studying and providing privacy-enhanced and anonymous communication infrastructures. MANETs are composed by mobile routers and hosts that form networks of arbitrary topology, by means of wireless communications, and use ad-hoc routing protocols to communicate among them. The first routing protocols, such as AODV [18] and DSR [19], were not designed to provide or guarantee privacy and communication anonymity, rather they were aimed at increasing network performance, efficiency, security, and reliability. As a consequence, they are vulnerable to privacy violations, for instance, by exploiting the protocol state, since each node stores sender, receiver, and hop-count of each communication.

Subsequent work focused on routing protocols for mobile ad-hoc networks and attempted to protect anonymity and privacy. The solutions proposed did so by keeping secret to intermediate nodes the identities of the senders and receiver of messages. A number of anonymous routing protocols have then been presented [20–26]. Among them, MASK proposes an anonymous routing protocol, which provides both MAC-layer and network-layer communications without the need of using the real identities of the participating nodes [26]. MASK provides communication anonymity, in addition to node location anonymity and untraceability, and end-to-end flow untraceability. MASK relies on the use of dynamic pseudonyms rather than static MAC and network addresses, and on pairing-based cryptography to establish an anonymous neighborhood 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 [20]. 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 an untraceable and intrusion tolerant routing protocol [22]. It provides communication anonymity, by preventing adversaries from following packets in the network, and location privacy, by preventing the adversary to discover the real position of local transmitters (which could disclose also their identities). ANODR is based on the paradigm of “broadcast

with trapdoor information". Discount-ANODR limits the overhead, suffered by ANODR, for providing sender anonymity and communication privacy [24]. A route is blindly generated by intermediary nodes, which only know the destination of the request and the identity of the immediatly previous intermediary. Discount-ANODR provides a lightweight protocol based on symmetric key encryption and onion routing. No key exchange nor public key operations are needed. Capkun et al. propose a scheme for hybrid ad-hoc networks allowing users to communicate in a secure environment and preserve their privacy [27]. The authors assume privacy as composed of two parts: *i)* anonymity, which hides users identity in the network, and *ii)* location privacy, which protects the position of the users in the mobile environment. The solution proposed is based on continuously changing pseudonyms and cryptographic keys, it avoids users re-identification by observing the locations they visit, or the traffic they generate, and it provides secure and privacy-preserving communications in hybrid ad-hoc networks.

In the context of MANETs, a new type of ad hoc networks has been designed and developed, that is, Vehicular Ad-Hoc Networks (VANETs). VANETs, which are becoming more and more relevant and popular [28], consist of fixed equipments and vehicles equipped with sensors which form ad-hoc networks and exchange information, such as, for instance, traffic data and alarms. Traditional research in the context of VANET has ranged from the definition of efficient and reliable infrastructures to the development of enhanced applications. Only recently, few works have focused on the security and privacy problems in VANETs [28–31]. Lack of security and privacy protection, in fact, can result in attacks subverting the normal network behaviour (e.g., by inserting false information) and violating the privacy of the users. Raya and Hubaux propose a preliminary investigation of the problem of guaranteeing security in VANET still protecting the privacy of the users [28]. They provide a threat model analyzing communication aspects, attacks, and security requirements. Also, they propose initial security solutions that protect user privacy based on digital signature, cryptographic keys, and anonymous public/private key pairs. Lin et al. present GSIS, a security and privacy solution based on Group Signature and Identity-based Signature techniques [30]. GSIS provides vehicle traceability to be used in case of disputes, and *conditional privacy preservation*. Conditional means that user-related information (e.g., driver's name, speed, position) must be accessible in case of exceptional situations, such as, crime or car accidents. Sampigethaya et al. present AMOEBA, a robust location privacy scheme for VANET [31].

AMOEBA focuses on protecting users privacy against malicious parties aiming at tracking vehicles, and building a profile of LBSs they access. To these aims, AMOEBA relies on vehicular groups and random silent periods.

The main limitation shared by the above solutions is that they heavily rely on key encryption, dynamic keys or pseudonyms, making them not always suitable in environments where communication devices have limited computational capabilities.

3.3 Sender Anonymity in Location-Based Services

Recent work on privacy protection has addressed the problem of preserving the anonymity of users (sender) that interact with Location-Based Services (LBSs) [32, 33]. LBSs are considered untrusted parties that can exploit location information of users to breach their privacy. The main goal of most of the current solutions [34] is to guarantee anonymity, by preventing adversaries to use location information for re-identifying the users. In this scenario, each location measurement is manipulated to keep users' identity hidden, still preserving the best accuracy possible. The approaches discussed in the following are based on the notion of k-anonymity [10, 11], which is aimed at making an individual not identifiable by releasing a geographical area containing at least k-1 users other than the requester. In this way, the LBSs cannot associate each request with fewer than k respondents, thus providing sender k-anonymity.

Bettini et al. propose a framework for evaluating the risk of disseminating sensitive location-based information, and introduce a technique aimed at supporting k-anonymity [35]. In this context, a *location-based quasi-identifier* (i.e., a set of attributes exploitable for linking) is defined as a set of spatio-temporal constraints, each one defining an area and a time window. The geo-localized history of the requests submitted by a user can be seen as a quasi-identifier, and used to discover sensitive information and re-identify the user. For instance, a user tracked during working days is likely to commute from her house to her workplace in a specific time frame in the morning, and to come back in another specific time frame in the evening. The notions of quasi-identifier and k-anonymity are used to provide a solution where a server collecting both the users' requests for services and the sequence of updates to users' locations, is not able to link a subset of requests to less than k users (sender k-anonymity). In other words, each data release must be such that every combination of values of quasi-identifiers can be indistinctly matched to at least k individuals. To this aim, there must exist k users having a

personal history of locations consistent with the set of requests that has been issued.

Gruteser and Grunwald propose a middleware architecture and adaptive algorithms to comply with a given k-anonymity requirement, by manipulating location information, in spatial or temporal dimensions [36]. They consider a bi-dimensional space and introduce an algorithm based on quadtree partition method to decrease the spatial accuracy of location information (spatial cloaking). Spatial cloaking perturbs the location of the user by enlarging her real position. More in details, a middleware manages a geographical area including different users. When the location information of a requester needs to be manipulated for privacy protection, the middleware incrementally partitions the whole area on the x and y axis to achieve the requested k-anonymity with the best possible location accuracy, i.e., generating the smallest area containing k users (including the requester). In addition to spatial cloaking, a temporal cloaking algorithm perturbs the location information of the user in the temporal dimension. This algorithm produces more accurate spatial information, sacrificing the temporal accuracy. A further parameter, called spatial resolution, is defined to identify an area containing the requester. 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. Figure 4 shows an example of quadtree-based spatial cloaking. Let u_1 be a user with preference k_1=3 that submits a request. First, the spatial cloaking algorithm partitions the whole area in four quadrants (i.e., Q1, Q2, Q3, Q4). Second, the algorithm selects the quadrant containing u_1 (i.e., Q1), while it discards the others, and considers u_1's privacy preference. Since k_1 is enforced by Q1, Q1 is recursively partitioned in four quadrants (dashed line). This time, however, k_1 would not be satisfied and then Q1 is returned as the k-anonymous area. The same process is applied for user u_2 with preference k_2=2. In this case, the quadrant Q4.1 is retrieved as the anonymized user location. As a result, quadrant Q1 and Q4.1 provide sender k-anonymity.

Mokbel et al. present a framework, named Casper, which includes a *location anonymizer*, responsible for perturbing the location information of users to achieve k-sender anonymity, and a *privacy-aware query processor*, responsible for the management of anonymous queries and cloaked spatial areas [37]. In Casper, users define two parameters as privacy preferences: a degree of anonymity k, and the best accuracy A_{min} of the area that

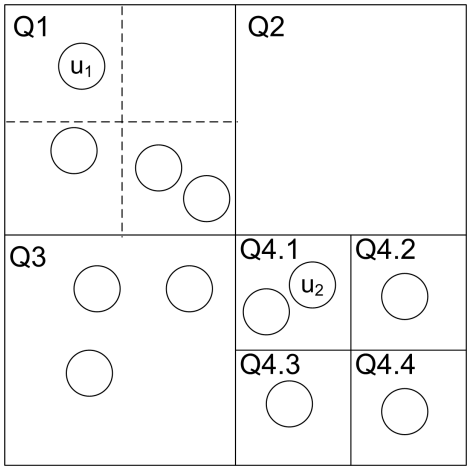

Fig. 4. Quadtree-based spatial cloaking

the user is willing to release. Two techniques which provide anonymization functionalities are implemented, that is, *basic* and *adaptive* location anonymizer. The main differences between the two techniques lie in the data structures they use for anonymizing the users, and in their maintenance. The basic location anonymizer uses a pyramid structure. At each level of height h, 4^h cells are available; the root is at level h=0 and represents the whole area. Each cell has an identifier, and maintains 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). In the adaptive location anonymizer, the contents of the grid cells and of the hash table are the same. However, an incomplete pyramid data structure is maintained, with only the cells that can be potentially used as a cloaked area. Those cells for which no privacy preference needs to be enforced are not stored. Both the techniques implement a cloaking algorithm where the anonymized area is generated starting from the lowest level of the pyramid, and selecting the first cell that satisfies the preferences k and A_{min} of the sender.

Gedik and Liu describe a k-anonymity model and define a message perturbation engine responsible for providing location anonymization of user's requests through identity removal and spatio-temporal obfuscation of location information [38]. In this framework, each user defines a minimum level of anonymity to protect her privacy, and maximum temporal and spatial tolerances for preserving a level of quality of service. The message perturbation engine generates anonymous queries through the

CliqueCloak algorithm. The CliqueCloak algorithm is based on a constraint graph where each vertex represents a message submitted by a user, and two vertices are connected if and only if the position of each user belongs to the constrained box of the other user, that is the area identified by the defined spatial tolerance. 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), such that the maximum k is less than l.

Ghinita et al. propose PRIVÈ, a decentralized architecture and an algorithm (*hilbASR*) for the protection of the sender anonymity of users querying LBSs [39]. 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 hilbASR algorithm is strong against attackers who know the distribution of all users. This is achieved by satisfying the *reciprocity* property, which assures that if the hilbASR algorithm is applied to all users in an anonymity area, the same anonymity area is produced. PRIVÈ relies on a distributed B^+-tree with additional annotation to manage the definition of anonymized areas.

Hashem and Kulik present a decentralized approach to anonymity in a wireless ad-hoc network where each user is responsible for generating her cloaked area by communicating with others users [40]. The proposed approach combines k-anonymity with obfuscation. More in details, each peer: *1)* obfuscates her position by substituting the precise location with a locally cloaked area (LCA) and *2)* anonymizes her requests by manipulating the LCA to a global cloaked area (GCA). The GCA includes the LCAs of at least other k-1 users. An anonymous algorithm selects a query requester in the GCA with a 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 that exploit collaborative and opportunistic sensing by mobile devices for service release [41]. In the proposed architecture, applications can distribute sensing works to anonymous mobile devices, and receive anonymized (but verifiable) sensor data in response.

Finally, Zhong and Hengartner present a distributed protocol for sender k-anonymity based on cryptographic mechanisms and secure multiparty computation [42]. The user interacts with multiple servers and a third party to determine if at least k people are in her area before communicating with the LBS. As a consequence, the LBS cannot re-identify the

user. In addition, the servers involved in the anonymization process can infer neither the total number of users in the area nor if the k-anonymity property is satisfied (i.e., if at least k people including the user are in the area). Finally, the user can only know if the k-anonymity property holds.

Works on location k-anonymity share some limitations: *i)* they either rely on a centralized middleware for providing anonymity functionalities (centralized approach) or let the burden of the complexity in calculating the k-anonymous area to the users (decentralized approach); *ii)* they assume trusted mobile network operators; *iii)* they only provide k-anonymity at application level.

4 Privacy Protection in Mobile Hybrid Networks

In the previous section, we presented different approaches to protect the privacy of the users in different network scenarios, including wired networks, mobile ad-hoc networks, and mobile networks providing LBSs. In this section, we introduce an emerging scenario integrating all these network types, discuss a new adversary model where each party receiving part of the communication should be considered untrusted, and present a first solution to this privacy problem.

4.1 Basic Scenario

Already noted, previously proposed privacy protection systems mostly focused on protecting sender, receiver, or communication anonymity from untrusted servers and observers. They assume the network operators to be fully trusted. However, while it is reasonable to assume that the network operators are trusted with respect to the availability and working of the network, and to the management of communication data, since they have an incentive providing uninterrupted service, some trust cannot be put on the confidentiality of the data. In fact, personal users' information can be traded as a commodity and thus, network operators can no longer be trusted with safekeeping such information. This consideration is especially true for mobile hybrid networks [17, 43, 44] where a single infrastructure integrates heterogeneous technologies, such as, wireless, cellular, and wired technologies. Figure 5 shows the overall architecture that we take as a reference in the discussion. It includes the following participating entities.

– *Mobile Users.* Users carrying mobile devices supporting both GSM/3G and WiFi protocols for communication. They request services to servers available over the network.

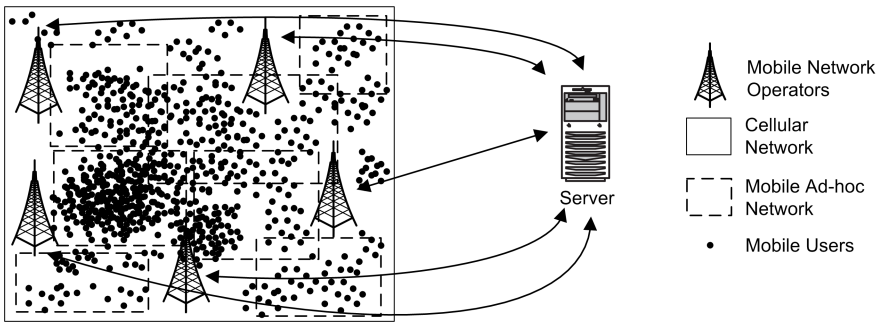

Fig. 5. Mobile network architecture

– *Cellular Network* (and corresponding *Mobile Network Operators*). A network composed of multiple radio cells, which provide network access and services to mobile users. The cellular network acts as a gateway between mobile users and servers.
– *Servers.* Entities that provide online services to the mobile users and can collect their personal information for granting access.

Users can communicate via wireless and cellular protocols to access services that are either co-located in the cellular network or in the Internet. Mobile users establish ad-hoc (WiFi) point-to-point connections with other mobile peers in the network. As a result, there are several wireless Mobile Ad-Hoc Networks (MANETs), represented by the dashed rectangles in Figure 5. In addition, mobile users receive signals from the radio cells and can connect to the cellular networks, through which they can access services. Mobile users are registered with a given mobile network operator to access cellular functionality. Different users may use different mobile operators.

4.2 A new vision of privacy

A promising research direction for protecting privacy in mobile networks exploits the hybrid nature of current networks and the capabilities of mobile devices, which support both WiFi and cellular technologies, to provide anonymous communication protocols. In our proposal [12], we depart from the assumption of having a trusted mobile operator and exploit the intrinsic characteristics of hybrid networks to provide a privacy-enhanced communication infrastructure between users and servers (see Figure 6). All parties that can receive or observe communications, including the mobile operators through which users communicate with servers, are consid-

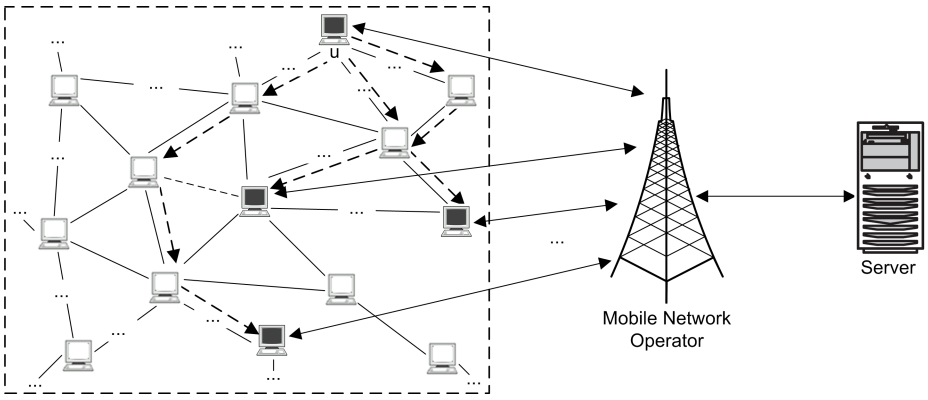

Fig. 6. A privacy-enhanced communication infrastructure

ered untrusted.[3] To address the privacy protection problem, we harness the fact that users can create WiFi point-to-point connections and at the same time join the cellular network in order to access the Internet through their mobile phones. Our solution is therefore different from the traditional research in anonymous communications [9, 13, 17, 45], since is applicable to mobile hybrid infrastructure, and is aimed at protecting sender k-anonymity against mobile network operators.

4.3 A Multi-Path Communication for Sender k-Anonymity

Our approach is based on k-anonymity and multi-path communication [12], to provide sender k-anonymity at network level. Sender k-anonymity is defined as follows.

Definition 1 (Sender k-anonymity). *Let M be a message originated by a mobile user u. User u is said to have sender k-anonymity, where k is the privacy preference of user u, if the probability of associating u as the message sender is less than or equal to $\frac{1}{k}$.*

In the following, we show *i)* how a k-anonymous request is generated and transmitted by a mobile user to the server through mobile peers and the cellular network, thus exploiting a multi-path paradigm [46], and *ii)* how the server crafts a reply that can be received and decoded only by the requester concealed from the other k-1 peers, to protect sender k-anonymity against adversaries including mobile operators.

[3] Depending on the scenario, each user can then decide if the server is trusted or not.

4.3.1 Overview of the Approach

Let $\mathcal{P}$, $\mathcal{O}$, and $\mathcal{S}$ be the set of mobile peers, mobile network operators, and servers in the hybrid network, respectively. In our discussion, user $u \in \mathcal{P}$ is the mobile peer that submits the request, $s \in \mathcal{S}$ the server, and $o \in \mathcal{O}$ the mobile network operator. Server s and the cellular network are in business relationship and u is subscribed to the cellular network. Also, s and u are assumed to be in a producer-consumer relationship and to share a common secret key SK that is generated through a Diffie-Hellman key exchange protocol. Each message M between u and s is encrypted, thus protecting confidentiality and integrity of the message through symmetric encryption (e.g., 3DES, AES). Standard notation $E_K()$ and $D_K()$ is used to denote encryption and decryption operations with key K. $E_{SK}(M)$ denotes a message M encrypted with symmetric key SK. Also, a random number mid is used as a message identifier. The complete protocol is shown in Figure 7 and is composed by an anonymous request and response, which are discussed in the following.

Anonymous Request. The anonymous request process is initiated by a mobile user u, which wishes to access a service provided by a server s. No overhead is given to u in the management of the mobile and anonymous process; u needs to first specify the message M and her privacy preference k. Then, u generates a message identifier mid and splits message M in k data flows producing a set of packets $\{m_1, m_2, \ldots, m_k\}$. The resulting packets are distributed among the neighbor mobile peers (peers for short) in the mobile ad-hoc network. Different algorithms (e.g., based on network state or on peer reputations) can be implemented for distributing packets among peers. Here, a simpler approach is used which consists in randomly forwarding the packets to the peers in u's communication range.

The distribution algorithm works as follows. Requester u encrypts each packet m_i using the symmetric key SK shared between u and s, and then appends mid in plain-text to it, that is, $\overline{m}_i = \{E_{SK}(m_i) \| mid\}$ for each i=1...k. The presence of message id mid in every packet allows mobile peers to distinguish different packets belonging to the same message M. Requester u then randomly selects k-1 peers p in her communication range, and sends a packet (from $\overline{m}_2$ to $\overline{m}_k$) to each of them. It then sends $\overline{m}_1$ to s via o.

Upon receiving a packet $\overline{m}_i$ each peer p first checks mid. If she has already agreed to send a packet with the same mid (i.e., $mid \in$ SENT), p forwards $\overline{m}_i$ to another peer in the communication range. Otherwise, it

Initiator: Requester $u \in \mathcal{P}$
Involved Parties: Mobile peers $\mathcal{P}$, Mobile network operator o, Server s
Variables: Original message M, Response message M_r, Secret key SK shared between u and s

INITIATOR ($u \in \mathcal{P}$)
u.1 Define message M and privacy preference k
u.2 Generate a random number mid and split M in k packets $\{m_1, \ldots, m_k\}$
u.3 Encrypt each packet m_i, with i=1...k, and append mid to them, $\overline{m}_i = [E_{SK}(m_i) \| mid]$
u.4 **for** j:=2...k **do**
Select a peers $p_j \in \mathcal{P}$
Send to p_j a packet $\overline{m}_j$
u.5 Select packet $\overline{m}_1$ and send it to o after a random delay
u.6 Upon receiving response message M_r from o, decrypt M_r /*response*/

Peer $p \in \mathcal{P}$
p.1 Receive a packet $\overline{m}$
p.2 **if** $\overline{m}.mid \in$ SENT
then forward $\overline{m}$ to a peer $p \in \mathcal{P}$
else case (p_f)
$\leq \frac{1}{2}$: forward $\overline{m}$ to a peer $p \in \mathcal{P}$
$> \frac{1}{2}$: $\overline{m} = \overline{m} - mid$
send $\overline{m}$ to o
p.3 Upon receiving M_r from o, delete it /*response*/

Operator $o \in \mathcal{O}$
o.1 Receive a packet $\overline{m}$ from p
o.2 Forward $\overline{m}$ to s
o.3 Upon receiving M_r from s, forward it to p /*response*/

Server $s \in \mathcal{S}$
s.1 Receive a packet $\overline{m}$ from p via o
s.2 Decrypt the packet with key SK and assemble M
s.3 Generate and encrypt the response message M_r
s.4 Send M_r to p through o /*response*/

Fig. 7. Anonymous communication protocol

randomly selects, with probability $p_f = \frac{1}{2}$, either to forward $\overline{m}_i$ to another peer in the communication range, or to send $\overline{m}_i$, without the mid, to s via o.

After the distribution process, each selected peer p independently sends the packet received to s, through operator o. Operator o then sees packets that comes from k different peers, including u (who then remains k-anonymous), and forwards them to s. Now, server s can decrypt each packet, incrementally reconstruct the original message, and retrieve the user request.

Example 1. Figure 8(a) shows an example of communication. In the figure, white computer represents a peer that forwards a packet to another

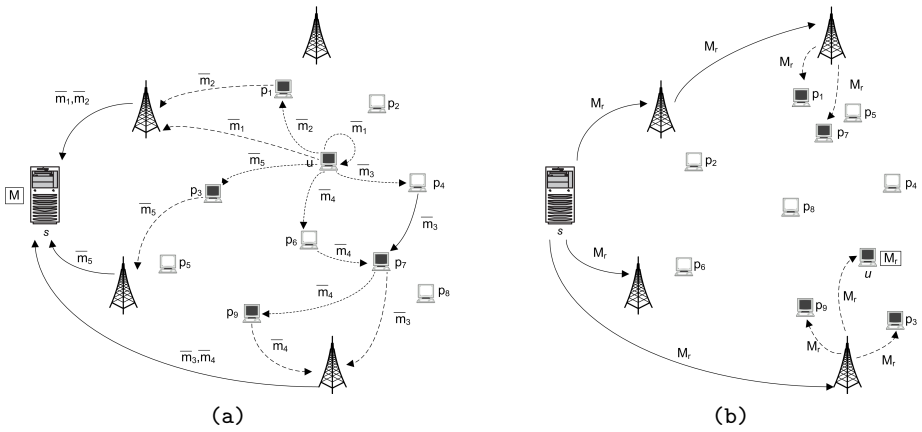

Fig. 8. Example of anonymous request (a) and anonymous response (b)

peer, while black one a peer that sends a packet to s. Requester u defines $k = 5$ and splits the message M in five parts $\{m_1, \ldots, m_5\}$. Packets are then encrypted with symmetric key SK shared between u and s, and mid is attached to each of them. Requester u sends packet $\overline{m}_1$ to s and forwards the other k-1 packets to peers in the communication range. Specifically, packets $\overline{m}_2$ and $\overline{m}_5$ are forwarded to peers p_1 and p_3 that send them to s. Assuming p_4 does not accept to send $\overline{m}_3$, packet $\overline{m}_3$ takes a forwarded path $p_4 \rightarrow p_7$. Packet $\overline{m}_4$ takes a forwarded path $p_6 \rightarrow p_7 \rightarrow p_9$ because, when the packet is received by p_7, p_7 notices that she has already accepted a packet ($\overline{m}_3$) with the same mid, and then forwards $\overline{m}_4$ to p_9. Finally, peers u, p_1, p_3, p_7, and p_9 send a packet to s via o.

Anonymous Response. After the conclusion of the anonymous request process, server s retrieves the original message M and starts the service provisioning, which results in the release of an anonymous response to user u. The communication involves operator o to manage peers mobility and route the response to user u, still preserving her preference k. The anonymous response process works as follow. First of all, server s encrypts response message M_r with secret key SK shared with u. Then, it transmits the encrypted message M_r to the k peers involved in the anonymous request. Server s relies on the cellular network to manage the message delivery and the mobility of the peers. Although all peers receive the message, u is the only peer with secret key SK, and thus, she is the only one able to decrypt the message and benefit of the service.[4]

[4] To further strengthen the protocol, the server could potentially generate k-1 decoy messages, other than M_r. This can be performed by adding a *nonce* to the original

Example 2. Figure 8(b) shows an example of anonymous response to the request in Example 1. Encrypted message M_r is transmitted to all peers used in Example 1, that is, $\{u, p_1, p_3, p_7, p_9\}$. When u receives the message, she can decrypt it with key SK shared with the server. The other peers delete message M_r, since they are not able to open it.

The solution presented provides an *anonymous communication* protocol. In terms of anonymous communication, the message splitting and multi-path communication provide sender k-anonymity against mobile network operators. Also, the solution provides user accountability, since the user's identity is released to the server and can be retrieved by the operator when needed.

It is important to note that a privacy solution, to be practical, should not be invasive, requiring extensive modification of existing network protocols. Considering the solution described above, all the packets are routed regularly through the hybrid network using TCP and reconstructed at the destination server. Only some small changes are necessary and only for specific applications: the message splitting done by requester u, and the packet checks on the mobile ad-hoc network done by the peers.

5 Open issues

We briefly describe some open problems which are important for the future development of privacy-enhanced and anonymous communication infrastructures for mobile networks.

- *Performance.* A key aspect for the success of privacy solutions in mobile networks is the performance and reliability of communications. The overhead in terms of end-to-end latency, the increase in the data transmission including both bursty and average bandwidth utilization should then be carefully evaluated. In addition, maintaining low power consumption is still an important performance metric for mobile and handheld devices with limited power. Finally, the performance evaluation should consider the adversarial and threat model and its impact on the performance metrics.
- *Malicious and uncooperative peers.* A complete and comprehensive privacy solution for mobile communications should consider malicious and uncooperative peers, which try to attack the system by modifying, dropping, injecting, or even replay received packets. An adversary

message M_r before encrypting it with secret key SK. The cellular network sees k different response messages and it is not able to associate the response to the request.

model including malicious and uncooperative peers should then evaluate failure probability, that is, the probability to disrupt a communication given the rate of malicious peers in the environment surrounding the users. Finally, a complete model should evaluate the possibility of synchronized attacks, where malicious peers send a sequence of fake requests to neighbor peers trying to make their battery low.

– *Malicious mobile network operators.* The definition of untrusted mobile network operators is the most important paradigm shift with respect to traditional solutions developed for wired and mobile ad-hoc networks. An interesting research direction consists in exploring a solution which considers the possibility of malicious operators that modify, drop and replay received packets to expose communication anonymity and breach users' privacy.

– *Multiple rounds of communications.* An important aspect in the protection of the communication anonymity is the possibility of communications involving multiple rounds of request-response. In this case, intersection attacks can be used by an adversary to successfully expose the communication anonymity and link the user to a service request. Especially in the case of mobile networks, where users can move fast, randomly, and in a short time, intersection attacks become likely to be successful against anonymizing techniques. A strong solution should then provide countermeasures in case multiple rounds of request-response are needed for a service release.

– *Traffic accountability.* Traditionally, one main factor limiting the adoption of privacy solutions is the lack of a mechanism that makes the system accountable for the generated traffic and the operations at the server. In fact, servers are often reluctant to adopt privacy solutions that can be abused due to the lack of user accountability [47], or lack economic incentives. The problem is even worse when privacy solutions (e.g., anonymity techniques) completely hide the users. In addition to that, given the mobile scenario discussed in previous sections, a fundamental requirement is to provide the operators with the ability to distinguish genuine vs malicious traffic, detect malicious users, and keep them out of the network.

– *Participation in anonymizing networks.* An important aspect for the success of anonymizing networks is to foster users participation in them. A suitable solution should then provide automatic incentives, that is, the more a user collaborates in providing anonymity to other peers, the more protected is her communication.

- *Integration with anonymous services.* Solutions that provide communication anonymity against mobile network operators and mobile peers should maintain a level of integrability with existing solutions providing sender k-anonymity against the servers.
- *Multiparty computation.* In mobile networks, most of the existing privacy solutions and anonymous routing algorithms heavily rely on multiparty computation and cryptographic mechanisms. An important requirement for the success of these solutions consists in reducing the impact of multiparty computation on the end to end communication and on the power consumption.
- *Adversary knowledge.* A key aspect to be considered in the definition and development of a strong privacy solution in mobile networks is the effect of the adversary knowledge on the ability of an adversary to link a user to her services. For instance, personal information of users in an anonymity set can bring to situations in which the real requester is identified and associated to the service request.

6 Conclusions

In this chapter, we discussed and analyzed different aspects related to the protection of communication privacy for contemporary mobile networks. We discussed privacy issues in different applications and scenarios, focusing on: *i)* communication anonymity in wired and mobile networks; *ii)* preserving the privacy of wireless traffic through privacy-enhanced and anonymous routing protocols for MANET and VANET; and *iii)* protecting the privacy and anonymity of users that interact with untrusted LBSs. For all these areas, we presented the main solutions, and pointed out their peculiarities and open problems. Furthermore, in the context of mobile hybrid networks, we identified a promising research direction and a novel privacy-preserving scheme based on k-anonymity and multi-path communication, which aims at preserving privacy of users against mobile network operators. Finally, we brought forward some open problems that warrant further investigation.

Acknowledgments

This work was supported in part by the EU, within the 7th Framework Programme (FP7/2007-2013) under grant agreement no. 216483 “PrimeLife”.

References

1. Barkhuus, L., Dey, A.: 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)
2. D'Roza, T., Bilchev, G.: An overview of location-based services. BT Technology Journal **21**(1) (January 2003) 20–27
3. Loopt. `http://www.loopt.com/about/privacy-security` (December 2008)
4. Zander, C.: Cia Cell Tower Monitors Local Internet Users' Wireless Transmissions. (September 2007) `http://www.send2press.com/newswire/2007-09-0911-003.shtml`.
5. Chicago Tribune: Rental firm uses GPS in speeding fine. July 2nd, p9. Associated Press: Chicago, IL, 2001.
6. Lee, J.W.: Location-tracing sparks privacy concerns. Korea Times. http://news.naver.com/main/read.nhn?mode=LPOD&mid=etc&oid=040&aid=0000016873, 16 November 2004.
7. Giannotti, F., Pedreschi, D., eds.: Mobility, data mining and privacy - Geographic knowledge discovery. Springer (2008)
8. Kaufman, C., Perlman, R., Speciner, M.: Network security: Private communication in a public world. Prentice Hall (2003)
9. Reiter, M., Rubin, A.: Crowds: Anonymity for web transactions. ACM Transactions on Information and System Security **1**(1) (1998) 66–92
10. Ciriani, V., De Capitani di Vimercati, S., Foresti, S., Samarati, P.: k-Anonymity. In Yu, T., Jajodia, S., eds.: Secure Data Management in Decentralized Systems. Springer-Verlag (2007)
11. Samarati, P.: Protecting respondents' identities in microdata release. IEEE Transactions on Knowledge and Data Engineering **13**(6) (2001) 1010–1027
12. Ardagna, C., Stavrou, A., Jajodia, S., Samarati, P., Martin, R.: 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 (October 2008)
13. Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM **24**(2) (1981) 84–88
14. Onion Routing. `http://www.onion-router.net/`.
15. Reed, M., Syverson, P., Goldschlag, D.: Anonymous connections and onion routing. IEEE Journal on Selected Areas in Communications **16**(4) (May 1998) 482–494
16. Reed, M., Syverson, P., Goldschlag, D.: Proxies for anonymous routing. In: Proc. of the 12th Annual Computer Security Applications Conference, San Diego, CA (December 1996)
17. Dingledine, R., Mathewson, N., Syverson, P.: Tor: The Second-Generation Onion Router. In: Proc. of the 13^{th} USENIX Security Symposium. (August 2004)
18. Perkins, C., Royer, E.: 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 (February 1999)
19. Johnson, D.B., Maltz, D.A.: Dynamic Source Routing in Ad Hoc Wireless Networks. Volume 353. Kluwer Academic Publishers (1996)
20. Boukerche, A., El-Khatib, K., Xu, L., Korba, L.: 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 (October 2004)

21. Kao, J.C., Marculescu, R.: Real-time anonymous routing for mobile ad hoc networks. In: Proc. of the Wireless Communications and Networking Conference (WCNC 2007), Hong Hong (March 2007)
22. Kong, J., Hong, X.: 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 (June 2003)
23. Wu, X., Bhargava, B.: AO2P: Ad hoc on-demand position-based private routing protocol. IEEE Transaction on Mobile Computing **4**(4) (July-August 2005)
24. Yang, L., Jakobsson, M., Wetzel, S.: Discount anonymous on demand routing for mobile ad hoc networks. In: Proc. of the Second International Conference on Security and Privacy in Communication Networks (SECURECOMM 2006), Baltimore, MD, USA (August-September 2006)
25. Zhang, Y., Liu, W., Lou, W.: Anonymous communication in mobile ad hoc networks. In: Proc. of the 24th Annual Joint Conference of the IEEE Communication Society (INFOCOM 2005), Miami, FL, USA (March 2005)
26. Zhang, Y., Liu, W., Lou, W., Fang, Y.: Mask: Anonymous on-demand routing in mobile ad hoc networks. IEEE Transaction on Wireless Communications **5**(9) (September 2006)
27. Capkun, S., Hubaux, J.P., , Jakobsson, M.: Secure and privacy-preserving communication in hybrid ad hoc networks. (January 2004) Technical Report IC/2004/10, EPFL-IC, CH-1015 Lausanne, Switzerland.
28. Raya, M., Hubaux, J.P.: 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 (November 2005)
29. Dotzer, F.: Privacy issues in vehicular ad hoc networks. In: Proc. of the Workshop on Privacy Enhancing Technologies (PET), Dubrovnik, Croatia (June 2005)
30. Lin, X., Sun, X., Ho, P.H., Shen, X.: GSIS: A secure and privacy preserving protocol for vehicular communications. IEEE Transactions on Vehicular Technology **56**(6) (November 2007) 3442–3456
31. Sampigethaya, K., Li, M., Huang, L., Poovendran, R.: AMOEBA: Robust location privacy scheme for VANET. IEEE Journal on Selected Areas in Communications **25**(8) (October 2007) 1569–1589
32. Ardagna, C., Cremonini, M., Damiani, E., De Capitani di Vimercati, S., Samarati, P.: Supporting location-based conditions in access control policies. In: Proc. of the ACM Symposium on Information, Computer and Communications Security (ASIACCS 2006), Taipei, Taiwan (March 2006)
33. Ardagna, C., Cremonini, M., Damiani, E., De Capitani di Vimercati, S., Samarati, S.: 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)
34. Mascetti, S., Bettini, C.: A comparison of spatial generalization algorithms for lbs privacy preservation. In: Proc. of the 1st International Workshop on Privacy-Aware Location-based Mobile Services (PALMS 2007), Mannheim, Germany (May 2007)
35. Bettini, C., Wang, X., Jajodia, S.: Protecting privacy against location-based personal identification. In: Proc. of the 2nd VLDB Workshop on Secure Data Management, Trondheim, Norway (September 2005)
36. Gruteser, M., Grunwald, D.: 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 (May 2003)
37. Mokbel, M., Chow, C.Y., Aref, W.: 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 (September 2006)
38. Gedik, B., Liu, L.: Protecting location privacy with personalized k-anonymity: Architecture and algorithms. IEEE Transactions on Mobile Computing **7**(1) (January 2008) 1–18
39. Ghinita, G., Kalnis, P., Skiadopoulos, S.: PRIVÈ: Anonymous location-based queries in distributed mobile systems. In: Proc. of the International World Wide Web Conference (WWW 2007), Banff, Canada (May 2007)
40. Hashem, T., Kulik, L.: Safeguarding location privacy in wireless ad-hoc networks. In: Proc. of the 9th International Conference on Ubiquitous Computing (UbiComp 2007), Innsbruck, Austria (September 2007)
41. Cornelius, C., Kapadia, A., Kotz, D., Peebles, D., Shin, M., Triandopoulos, N.: Anonysense: privacy-aware people-centric sensing. In: Proc. of the 6th international conference on Mobile systems, applications, and services (MobiSys 2008), Breckenridge, CO, USA (June 2008)
42. Zhong, G., Hengartner, U.: A distributed k-anonymity protocol for location privacy. In: Proc. of the Seventh IEEE International Conference on Pervasive Computing and Communication (PerCom 2009), Galveston, TX, USA (March 2009)
43. Fujiwara, T., Watanabe, T.: An ad hoc networking scheme in hybrid networks for emergency communications. Ad Hoc Networks **3**(5) (2005) 607–620
44. Sphinx - A Hybrid Network Model for Next Generation Wireless Systems. `http://www.ece.gatech.edu/research/GNAN/work/sphinx/sphinx.html`.
45. Chaum, D.: The dining cryptographers problem: Unconditional sender and recipient untraceability. Journal of Cryptology **1**(1) (1988) 65–75
46. Stavrou, A., Keromytis, A.: Countering dos attacks with stateless multipath overlays. In: Proc. of the 12th ACM conference on Computer and communications security (CCS 2005), Alexandria, VA, USA (November 2005)
47. Borisov, N., Danezis, G., Mittal, P., Tabriz, P.: Denial of service or denial of security? In: Proc. of the 14th ACM conference on Computer and communications security (CCS 2007), Alexandria, Virginia, USA (October-November 2007)