AMORES:
an Architecture for MObiquitous REsilient Systems

Christian Artigues, Yves Deswarte
Jérémie Guiochet, Marie-José Huguet
Marc-Olivier Killijian, David Powell
Matthieu Roy
LAAS-CNRS, France
Université de Toulouse, France
{firstname.name}@laas.fr

Emmanuelle Anceaume
Sébastien Gambs
Gilles Guette
Michel Hurfin
IRISA - INRIA
France
{firstname.name}@irisa.fr

Christophe Bidan, Nicolas Prigent
Supelec
France
{firstname.name}@supelec.fr

Frédéric Schettini
MobiGIS
France
{name}@mobigis.fr

ABSTRACT

We present the AMORES project, which aims to provide an architecture for the provision of privacy preserving and resilient collaborative services in “mobiquitous” (i.e., mobile and ubiquitous) systems. The project is built around three use-cases from the area of public transportation: (1) dynamic carpooling, (2) real-time computation of multimodal transportation itineraries and (3) mobile social networking. Four main research tasks are presented in this paper. The first task deals with use-cases, prototypes and privacy assessment. The second task addresses geo-communication primitives: verified positioning, locanyms and geo-services. The third task deals with privacy-preserving communication means such as anonymous routing and geo-cryptography. Finally, the last task is devoted to collaborative behaviors.

Keywords

Mobiquitous, Mobility, Privacy, Geo-privacy

1. INTRODUCTION

The ubiquitous world in which we live is characterized by a high mobility of individuals, most of them wearing devices capable of geo-localization (smartphones or GPS-equipped cars). However, most of the current transportation systems have not yet really used the facilities offered by these geo-located devices to improve the mobility of their users or to propose new transportation means. Situated in this “mobiquitous” context, the AMORES project is built around three use-cases related to mobility, namely (1) dynamic carpooling, (2) real-time computation of multimodal transportation itineraries and (3) mobile social networking. For these three use cases, the AMORES project focusses on the definition and the development of geo-communication primitives at the middleware level that can offer the required geo-located services, while at the same time preserving the privacy of users, in particular with respect to their location (notion of geo-privacy). The geo-primitives refer to the set of services used for data exchange between applications, which are aware of their location and can explicitly take into the geographical context. We focus on the study of geo-located services such as geo-casting, geo-registers, geo-queries and geo-computing. Moreover, to guarantee the authenticity of the location information, we are studying techniques that can be used to verify the positions claimed by the entities. To offer privacy guarantees, we propose an anonymization method based on location data that we refer to as “locanyms”. To offer such features, the geo-communication primitives require some basic functions, such as routing, cryptographics, cryptographic key distribution and management, and location recognition. Thus, privacy must also be considered at the level of these basic functions in order to control the digital traces generated by their use. It is thus also necessary to study the problem of anonymous routing and key generation taking geo-awareness explicitly into account. Each of these services can only work through cooperation between the different entities composing the mobile network. Therefore, we are developing mechanisms to encourage entities to cooperate with each other in a privacy-preserving manner, and to provide services that can detect entities that behave maliciously, such as by deliberately providing fake information.

For each of the previously mentioned use cases, we aim to implement proof-of-concept prototypes based on the primitives developed at the middleware level. Thus, to prove the applicability of our approach, we plan to implement real-time computation of multimodal itineraries and mobile social networking. The underlying middleware will be distributed as open source. The third use case, i.e., dynamic carpooling, will be integrated within the product line of one of the partners. Another important contribution of the project will be the demonstration and delimitation of the real possibilities offered by the proposed approach. A generalization of the expected results in the Toulouse area, in collaboration with Tisséo (the Toulouse public transit company), will nourish our reflection about the future of urban transport systems and the practical applicability of such an approach.

To summarize, the outputs of the project are both conceptual and practical: definition of innovative privacy-preserving geo-communication primitives for mobiquitous systems, implementation of a middleware and some proof-of-concept prototypes and, finally, an impact on next generation public transportation.

2. OBJECTIVES

The AMORES project has two main high-level objectives:
1) Leverage the existence of ubiquitous computing, communication and positioning via small and mobile devices, such as smartphones, in order to provide high-level mobility services targeted at increasing the use of public transportation and reducing CO_2 emissions;
2) Provide a privacy-conscious, geo-aware middleware for the provision of cooperative services in the emerging mobiquitous era of computing.

To the best of our knowledge, no such geo-communication oriented middleware yet exists. We strongly believe that, in a mobiquitous setting, with numerous interacting mobile nodes, mobility and geographical distribution should be explicitly taken into account. Indeed, centralized architectures cannot scale to the situation where billions of mobile nodes need to interact with each other, looking for local services. We believe that the highly innovative geo-primitives that we envision will help application designers to implement geo-aware services for the mobiquitous setting. These primitives include: (1) verified positioning, which can verify the location claimed by a node, (2) locanyms, which can be used to address a node by its location and not by its identifier while still providing strong properties like accountability and non-repudiation, and (3) higher-level geo-services for communication (geo-casting), data storage (geo-registers, geo-btrees, etc.), search (geo-queries) and computation (geo-measurements).

The mobiquitous environment, in which devices are mobile and geo-located and where services are location-based, raises several privacy issues due to the fact that geo-located devices usually belong to an individual (or a group of persons such as a family) and as such their locations correspond to the locations of their owner(s). Among the various items of Personal Identifiable Information (PII) that may be revealed, the location of an individual is one of the greatest threats against his privacy. For instance, the spatio-temporal data of an individual can be used to infer the location of his home and workplace, to trace his movements and habits, to learn information about his center of interests or even to detect a change from his usual behavior. Therefore, the preservation of location privacy is a major concern when leveraging the possibilities offered by the mobiquitous setting to provide efficient and trusted geo-services. We intend to assess the privacy risks of each use case and then follow the privacy-by-design principle to develop a geo-service middleware that is publicly (and politically) acceptable and trustworthy.

Being able to communicate anonymously is a necessary (but not sufficient) condition for preserving privacy. It implies the ability to perform anonymous routing, which constitutes a difficult research challenge. Existing approaches either require, for two nodes that wish to communicate, to know their respective location [11, 12], or deeply rely on a trusted authority. These two limitations prevent the use of their solutions in the applications envisioned within the AMORES project, especially for mobile social networking. To avoid the need for a trusted central authority, we will therefore study distributed mechanisms to generate cryptographic keys that are tied to a specific location (we call them “geo-keys”). Once the geo-keys have been generated, they can be used for authentication purposes as well as for ensuring the confidentiality of communications. Finally, to encourage nodes to cooperate in a trustable and private manner, we intend to use digital reputation. Digital reputation has been proven efficient to handle the first challenge. However, because it demands a certain measure of control over the revelation of personal information and its distribution across networks, digital reputation seems to conflict with values of free expression and many business models. On the other hand, if, as for anonymous voting in elections, the feedback collected by reputation mechanisms is anonymous, we might be confident that it should potentially encourage trustfulness by guaranteeing secrecy and freedom from any influence (fears of retaliation or reciprocation). Although such anonymous feedbacks can be exploited by untrustworthy feedback providers (through ballot stuffing and bad mouthing strategies), we are convinced that the benefit brought for honest parties would be considerable: their privacy would be respected and thus they would be protected from any strategic manipulation.

3. PROJECT STRUCTURE

The AMORES project aims to develop privacy-preserving middleware for cooperative mobiquitous systems. The development of the project is guided by a top-down approach within the area of public transportation.

3.1 Use-cases and privacy risks

This task forms the substrate of all the other technical tasks. It will investigate concrete application scenarios that will serve for defining security and privacy requirements of the project, as well as for identifying the technical challenges, and threats to these requirements. First, we will study a set of three use-cases that are relevant to AMORES and identify for each of them the fundamental primitives that are needed and the main challenges to be addressed. Then, we will define and analyze the high-level privacy and security requirements linked to the mobiquitous setting. The final subtask is devoted to prototyping activities, dissemination of the developed middleware, production of proof-of-concept prototypes, and integration of prototypes on real platforms.

3.1.1 Use-cases

The chosen application domain is public transportation, which, in our opinion, is a good setting for providing location-based services on top of mobile ad hoc networks. We chose this application domain for several reasons. First, in a public transportation system, the architecture is hybrid since most entities (users, buses, cars, trains, etc.) are mobile but some are fixed (train/bus/bicycle stations, highway toll stations) and can be used as gateways to an infrastructure or as anchors for positioning purposes. Second, the application domain itself is by essence concerned with mobility, proximity and similar notions. It should thus benefit greatly from the geo-aware middleware that we want to build within AMORES. Finally, privacy is of paramount importance in such a setting as users move between places but their mobility patterns should be kept private from other entities (even from other mobile users that they periodically meet and cooperate with) as they generally do not know them and therefore cannot blindly trust them. The three candidate use-cases that we have identified are:

• *Dynamic carpooling*: this service dynamically matches together car drivers with passengers from suburban to urban journeys or intra-urban journeys. The dynamic carpooling service needs to implement algorithms for dynamic vehicle routing problems, where multiple vehicles may candidate to pick up passengers that are themselves potentially moving on a network. To implement this functionality, we intend to leverage both the mobile social network and the available infrastructure.

• *Multi-modal itineraries in real-time*: this service computes in real-time the optimal multimodal (bus, subway, train but also bicycle, walking or carpooling) itinerary by taking into account the up-to-date spatial and temporal information of the various entities. If multimodal shortest path algorithms are now well studied in static networks, they remain challenging in a dynamic network. For instance, given two passengers moving on a network, finding optimal meeting points according to various criteria (e.g., cost, time or preferred locations) and the associated multimodal itineraries is a complex and difficult issue.

• *Mobile social networking*: all mobile users using the public transportation system form a mobile social network at the scale of a city. In the AMORES project, we envision to use explicitly the mobile social network to implement services such as discovering if a friend is located in one's vicinity (e.g., in the same train) or is currently moving towards the area where one is staying and could potentially pick one up on his way. Apart from these social functionalities, we also want to rely on the possibilities offered by this mobile ad hoc network to develop trust mechanisms giving for instance more important roles to close friends.

3.1.2 High-level privacy concerns

The objective of this subtask is to evaluate and assess the privacy risks incurred for the different use-cases, and to show how these risks are dealt with by the mechanisms developed in AMORES. In this subtask, we will:
1) Apply a classic risk assessment process starting from a definition of system usage based on UML interaction models for the three use-cases.
2) Identify relevant incident scenarios, including identification of threats, vulnerabilities, affected assets, and consequences to assets. This work will be carried out using collaborative methods commonly used in the safety domain (such as preliminary hazard analysis). A scale describing the magnitude of potential consequences and their likelihood of occurrence (for instance depending on potential benefits or ease of attack) will be proposed. This scale will be used to quantify the risks of the previously identified hazards.
3) Evaluate the risk acceptability (based on the previous estimation) to decide if a reduction of this risk is needed. In particular, the impact of/on geo-primitives developed in other tasks, which can be viewed as risk reduction strategies, will be investigated.

3.1.3 Prototyping

Various prototypes will be developed, which will have different levels of maturity. First, a proof-of-concept prototype of use-cases 2 and 3 will be developed, on top of the ARUM mobile robot platform previously developed at LAAS [21], to evaluate whether the middleware geo-primitives (and their associated properties) are adequate or not. Then, at a later stage, the middleware will be integrated in the MobiGIS integration platform and use-case 1 will be developed on top of it. We are also planning to have on the MobiGIS platform a hybrid dynamic/static carpooling prototype. For instance, when a user is planning a journey, he will first search locally using the dynamic version of the tool; if he fails to find a carpool partner, he will switch to the static (and already existing) version of carpooling.

3.2 Geo-communication Primitives

This task will provide geo-communication primitives enabling geo-aware design of the use-cases while preserving privacy (for instance, by limiting the dissemination of location) through architectural and algorithmic solutions. Within the course of the project, we want to study specifically the following three geo-primitives (it is worth noting that the former two, Verified Positioning and Locanyms are the described in details in [16]):

• *Verified positioning.* A fundamental geo-primitive we want to provide is verified positioning through which a mobile node can prove its current location to other nodes in a secure and distributed manner. This primitive is necessary to build other more advanced building blocks such as locanyms and geo-services. More precisely, we will (1) explore how the use of mobile base stations (such as buses or other itinerant nodes) [6] can be used to implement more robust mechanisms for location verification, (2) pursue the line of research recently introduced by [7], which adopts a non-standard cryptographic model called bounded retrieval in order to solve the verified positioning problem which they proved to be impossible to solve in the general model, (3) investigate how "collusion attacks" may be mitigated through mobile social network information [26] and related trust mechanisms.

• *Locanyms.* As a second middleware geo-primitive, we plan to develop the concept of locanyms, a geo-located version of pseudonym that is tied to a particular geographical area. We believe that it is possible to define locanyms that provide advanced properties such as accountability and non-repudiation. For instance, in the carpooling use-case, the use of locanyms seems sufficient to authenticate the various parties while trying to establish a relationship (e.g., looking for potential candidates to connect for a trip). Once a relationship is established and the parties physically meet, locanymity (location anonymity) can be lifted and identities exchanged as the users meet face-to-face anyway. The accountability property can be important to prove to a third party (such as the administration of the city) that an entity has effectively participated in a carpooling activity, in order to get a discount on his or her public transport subscription for instance. The non-repudiation property, which can be obtained through a combination of locanyms and digital signatures, will ensure that an entity cannot deny having participated in a geo-service to which he had previously given his explicit consent. This property can be essential for billing purposes or to provide cooperation incentives.

• *Geo-services.* Both verified positioning and locanyms are geo-primitives focusing on providing individual properties and services (such as the verified positioning of one entity or a locanym). Beyond these, broader geo-primitives aimed at providing fundamental distributed services such as communication, storage, search and computation need to be developed. Regarding *geo-communication*, we will design a geo-located variant of group communication, which is a fundamental mechanism in classical distributed systems. One of the challenges of group communication deals with the consistency of the group membership views (i.e., who currently belongs to the group), and how nodes join and leave the group. We want to create a service such that, at the moment of the group creation, nodes geo-located in the same vicinity or within a particular delimited area communicate with one another to create the original group structure [20]. We believe that a privacy-aware notion of geo-groups (or geo-cast) can be a very useful building block for higher-level geo-primitives. Moreover, we also want to develop an anonymous variant of geo-cast. Concerning *geo-storage*, we plan to introduce an abstract object, called a geo-register that can associate a value to a geographical location. A geo-register is defined by a geographic area; nodes located within this area participate in the maintenance of the geo-register and can use it (i.e., by read and write operations). We believe that such a basic geo-primitive can be further extended to provide richer primitives such as geo-counters or more advanced structures such as geo-binary trees that could help to speed up other functionalities (e.g., searching). *Geo-search* deals with queries that are bound to a specific geographical area, such as finding the nearest pizzeria for example. A naive implementation of a geo-search could be built on top of locanyms, geo-casting, and anonymous routing. For instance, the requesting node, authenticated by its locanym, issues a search by geo-casting its query (e.g., where is the nearest bus stop); an answering node will then reply using anonymous point-to-point communication. Better strategies will be investigated to optimize the communication resources needed and to obtain better privacy guarantees. Finally, a *geo-computing* primitive could be used to evaluate in real-time some node-dependent property of the zone, such as the density of nodes, or the mean waiting time of users present at a given bus stop.

3.3 Basic communication components

This task will focus on the necessary basic privacy-preserving communication components for the provision of the geo-primitives. Many of these basic components will come directly from the state-of-the-art, such as positioning techniques, anonymous Medium Access Control or standard cryptographic techniques. In AMORES, we will specifically work on the following two basic privacy-preserving components: a privacy preserving routing layer and geo-cryptographic primitives for generating and managing cryptographic keys linked to a geographical place.

Ad hoc routing is particularly suitable for handling communication in mobiquitous networks because of their evolving and dynamic aspect. Many ad hoc routing protocols have been proposed to establish communication between nodes without the support of any fixed infrastructure or central administration. Unfortunatly, the information that is used to build the routing tables and that each node is supposed to disclose (e.g., the MAC and/or IP addresses) generally allows unambiguous identification of the nodes, making anyone able to identify and track any node that collaborates in the routing service. Moreover, by looking for transiently nearby nodes, an attacker can guess which users were located in the same area and can deduce potential social interactions from this physical proximity. Furthermore, if the attacker knows the geographical position of certain nodes, it becomes possible for him or her to track the time-varying relative positions of the other nodes. Finally, an attacker can also quite easily track the occurrence of communications between any pair of nodes.

3.4 Cooperation incitation

This task will address the different aspects needed to promote cooperation among unknown users and devices. One aspect relates to the quality of service observed during interactions between nodes. Another aspect is how to efficiently, securely and anonymously collect observations of these interactions over the hybrid network. The last aspect is the evaluation of a reputation score according to the collected observations and their credibility.

4. RELATED WORK

In this section, we briefly describe the current state of the art in the main scientific themes addressed by the AMORES project: privacy-preserving geo-aware middleware, anonymous routing and communication in MANETs, and cooperation incitation.

4.1 Privacy-preserving geo-aware middleware

The field of middleware for mobile/mobiquitous systems is by itself relatively recent [2, 33, 21]. One essential feature in these settings is context awareness, and more particularly geo-location awareness. Early works try to address new primitives for data-sharing or communication on top of mobile systems, see, e.g., geo-registers [27], asynchronous shared memory [24], or tuple-spaces [32, 14]. Other research has focused on online reconciliation of offline transactions based on partial representations [23, 29]. Peer-to-peer is one of the most used paradigms when researchers try to deal with the mobility aspect. This is quite relevant since, when considering information flow from the low layers (routing) to the upper layers (application), access to classic servers can never be guaranteed when a node is mobile [18, 9].

To the best of our knowledge, there has been no previous work specifically targeting the issue of privacy in middleware for mobiquitous systems. Geo-privacy seeks to prevent an unauthorized entity from learning the past, current and future locations of an individual [3]. Indeed, learning the location of an individual is one of the greatest threats against his privacy [15]. An adversary can combine some auxiliary knowledge with this location information to gain additional knowledge. For example, if the adversary has access to the social network of an individual, he can determine when the person is visiting a given friend.

In a mobiquitous setting, the identity of an entity is not (only) defined in the usual sense by its name, its physical characteristics or its public key but rather according to its location and mobility behavior. One fundamental issue is therefore to be able to verify the location claimed by an entity in a secure manner. Indeed, if a location is used as a form of credential and a malicious entity can cheat with its location, this opens the way to a panoply of attacks on the geolocated services that could go as far as creating multiple identities, each claiming to be at a different location (this corresponds to a geolocated variant of the Sybil attack [10]). Brands and Chaum [4] were among the first ones to design a distance-bounding protocol using the notion of time-of-response to verify the location. For an entity, proving its location generally requires interactions with several verifiers. The verifiers send challenges (i.e., messages) to the prover, using for instance a medium such as radio waves (which travel at the speed of light), and measure the time taken to receive a response. Depending on the time taken, the verifiers can identify and certify collectively the location of the entity. Several protocols found in the literature [28, 5] are based on this cooperative approach between verifiers for ensuring secure positioning. However, a recent work [7] has shown that these techniques are sensitive to a "collusion attack" (in such attacks, several provers collude together to convince the verifiers that they are talking to a single prover located at a fake location). Providing a geo-aware communication middleware with verifiable locations while preserving geo-privacy is one of the challenges addressed by AMORES.

4.2 Anonymous routing and communication

In MANETs, routing protocols can be broadly classified as proactive (e.g. OLSR [8]) or reactive (e.g. AODV [25]). In proactive routing protocols, nodes update their routing tables periodically by exchanging information about the network's topology and connectivity, while in reactive routing protocols (also called on-demand), the source searches for the route only when it has to send a message. During the design of all these protocols, the focus has been so far on performance, scalability, energy consumption and some security issues (mainly confidentiality, authenticity, integrity and availability) whereas privacy seems at first glance to be antagonistic with the very principles of ad hoc routing. To address this problem, some seminal works have proposed privacy-preserving variants of ad hoc routing protocols. Most of these protocols (e.g., MASK [34], ARM [30]) are reactive and consist in (1) using cryptographic primitives to generate pseudonyms during route requests and (2) by hiding communication between two nodes through anonymous communication networks such as mixnets or non-routing relays. Recently, Al Defrawy and Tsudik have proposed two location-based ad hoc routing protocols ([11, 12]) that address partially privacy issues. In these protocols, a node A decides to communicate with another node B depending on where B is located at the present time.

4.3 Cooperation incitation

Most of the services addressed by AMORES critically depend on cooperation to be effective. This raises new concerns related to the willingness of parties to collaborate, the establishment of trust among parties, and incentives for fair participation. These concerns are exacerbated by the fact that all these services propose to take advantage of both autonomous rational parties (users/humans) and deterministic altruistic ones (buses, trams, subway trains). Two main approaches exist to enforce fair cooperation among almost or completely unknown parties: currency-based and reputation-based mechanisms. Currency-based mechanisms either rely on the presence of a centralized entity in charge of trading credits [35] or on the propensity of participants to exchange currency (usually a virtual one). This centralized approach is incompatible with the very nature of the applications we consider, the underlying networks, as well as with the preservation of privacy. Moreover, paying nodes for their willingness to collaborate may not be tractable at all levels of our architecture [19]. The recent emergence of e-commerce in open large-scale distributed marketplaces has shown that digital reputation systems stimulate interactions among strangers and encourage them to behave in a trustworthy manner, while discouraging them in presence of deviant parties. Similarly to real world reputation, a digital reputation mechanism expresses a collective opinion about some target entity by collecting and aggregating feedback about the past behavior of that entity [22]. Because of their strong impact on reducing the risks of collaborating with strangers, these mechanisms have been studied from the viewpoint of them being efficient, scalable, accurate and robust against undesirable behaviors ([1, 13]). On the other hand, none of the current distributed implementations of reputation mechanisms have addressed privacy concerns. Deducing user profiles (i.e., combining all the contexts in which a user has been involved in, such as the communities or people with whom that user has recently interacted, the frequency of these interactions, his satisfaction, his irritation) may be of high interest and a promising target for collectors of private data [17], or worse for retaliation arguments. In any case, this is clearly in contradiction with the user's right to privacy [31].

5. CONCLUSION

In this paper, we presented the AMORES project, which aims to provide an architecture for the provision of privacy-preserving and resilient collaborative services in mobiquitous systems. The project, started in October 2011 and running for 42 months, is built around four tasks and three use-cases in the area of public transportation. The first task deals with the use-cases, the prototypes and privacy assessment. The second task addresses geo-communication primitives: verified positioning, locanyms and geo-services. The third task deals with privacy-preserving communication means such as anonymous routing and geo-cryptography. Finally, the fourth task is devoted to cooperation incentives.

6. ACKNOWLEDGMENTS

This work was partially supported by LAAS, CNRS, Aerospace Valley and ANR French national program for Security and Informatics (grant #ANR-11-INSE-010).

7. REFERENCES

[1] E. Anceaume and A. Ravoaja. STORM: A secure overlay for p2p reputation management. In *IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO 2007)*, 2007.

[2] P. Bellavista and A. Corradi. *The Handbook of Mobile Middleware.* Auerbach Publications, 2006.

[3] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. *IEEE Pervasive Computing*, 3(1):46–55, 2003.

[4] S. Brands and D. Chaum. Distance-bounded protocols (extended abstract). In *EUROCRYPT'93*, pages 244–359, 1993.

[5] L. Bussard. *Trust establishment protocols for communicating devices.* PhD thesis, Eurecom, 2004.

[6] S. Capkun, M. Cagalj, and S. M. Secure localization with hidden and mobile base stations. In *Proc. of IEEE INFOCOM, 2006*, 2006.

[7] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky. Position based cryptography. In *CRYPTO'09*, pages 391–407, 2009.

[8] T. Clausen and P. Jacquet. Optimized link state routing protocol (OLSR). IETF mobile ad hoc networking Working Group, RCF 3626, 2003.

[9] L. Courtès, O. Hamouda, M. Kaaniche, M. Killijian, and D. Powell. Dependability evaluation of cooperative backup strategies for mobile devices. In *13th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC'07)*, 2007.

[10] J. Douceur. The sybil attack. *Peer-to-peer Systems*, pages 251–260, 2002.

[11] K. El Defrawy and G. Tsudik. Alarm: Anonymous location aided routing in suspicious manets. In *Proc. of the 2007 IEEE International Conference of Network Protocols (ICNP'07)*, 2007.

[12] K. El Defrawy and G. Tsudik. Prism: Privacy-friendly routing in suspicious manets (and vanets). In *Proc. of the 2008 IEEE International Conference of Network Protocols (ICNP'08)*, October 2008.

[13] M. S. Fallah and M. Mouzarani. A game-based sybil-resistant strategy for reputation systems in self-organizing MANETs. *The Computer Journal*, 2011.

[14] E. Freeman, S. Hupfer, and K. Arnold. *JavaSpaces: Principles, Patterns, and Practice.* Addison-Wesley, 1999.

[15] S. Gambs, M. Killijian, and M. Prado Cortez. Show me how you move and i will tell you who you are. In *ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS*, 2010.

[16] S. Gambs, M.-O. Killijian, M. Roy, and M. Traore. Locanyms: Towards privacy-preserving location-based services. Technical Report 12032, LAAS-CNRS, 2012.

[17] E. Gudes, N. Gal-Oz, and A. Grubshtein. Methods for computing trust and reputation while preserving privacy. In *Proceedings of the 23rd Annual IFIP WG 11.3 Working Conference on Data and Applications Security XXIII*, pages 291–298, 2009.

[18] H. Hsieh and R. Sivakumar. On using peer-to-peer communication in cellular wireless data networks. *IEEE Trans. Mobile Comput.*, 3(1):57–72,, 2004.

[19] S. Kamvar, M. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *Proc. of the Int'l Conference on World Wide Web (WWW)*, 2003.

[20] M.-O. Killijian, R. Cunningham, R. Meier, L. Mazare, and V. Cahill. Towards group communication for mobile participants. In *Proc. of Principles of Mobile Computing, POMC-2001*, page 8, 2001.

[21] M.-O. Killijian and M. Roy. Data backup for mobile nodes : a cooperative middleware and an experimentation platform. *Architecting Dependable Systems*, 7, 2009.

[22] S. Marti and H. Garcia-Molina. Taxomany of trust: Categorizing p2p reputation systems. *Computer Networks Journal*, 50(4):472–484, 2006.

[23] C. Mascolo, L. Capra, S. Zachariadis, and W. Emmerich. Xmiddle: a data-sharing middleware for mobile computing. *Int. Journal on Wireless Personal Communication*, 21(1):77–103, 2002.

[24] B. Nitzberg and V. Lo. Distributed shared memory: a survey of issues and algorithms. *IEEE Computer*, 24:52–60, 1991.

[25] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc on-demand distance vector (AODV) routing. IETF mobile ad hoc networking WG, RFC 3561, 2003.

[26] D. Quercia and S. Hailes. Sybil attacks against mobile users: friends and foes to the rescue. In *Proc. of IEEE INFOCOM, 2010*, pages 336–340, 2010.

[27] M. Roy, F. Bonnet, L. Querzoni, S. Bonomi, M. Killijian, and D. Powell. Geo-registers : an abstraction for spatial-based distributed computing. In *OPODIS'08*, 2008.

[28] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *WiSe03*, pages 1–10, 2003.

[29] M. Satyanarayanan, J. Kistler, P. Kumar, M. Okasaki, E. Siegel, and D. Steere. CODA: a highly available file system for a distributed work- station environment. *IEEE Trans. Comput.*, 39(4):447–459, 1990.

[30] S. Seys and B. Preneel. ARM: Anonymous routing protocol for mobile ad hoc networks. In *20th International Conference on Advanced Information Networking and Applications*, 2006.

[31] S. Steinbrecher. Enhancing multilateral security in and by reputation systems. *IFIP International Federation for Information Processing*, 298, 2009.

[32] P. Wyckoff, S. Mclaughry, T. Lehman, and F. D. TSpaces. *IBM Syst. J.*, 37:454–474, 1998.

[33] Y. Yu, B. Krishnamachari, and V. Prasanna. Issues in designing middleware for wireless sensor networks. *IEEE Network*, 1:15–21, 2004.

[34] Y. Zhang, W. Liu, W. Lou, and Y. Fang. MASK: Anonymous on-demand routing in mobile ad hoc networks. *IEEE Transactions on Wireless Communications*, 5(9), 2006.

[35] S. Zhong, J. Chen, and Y. R. Yang. Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In *INFOCOM*, 2003.