Participatory Sensing: The Tension between Social Translucence and Privacy

Ioannis Krontiris and Nicolas Maisonneuve

Abstract Participatory sensing is a new research area that emerged from the need to complement our previous efforts in wireless sensor networks. It takes advantage of the emergence of rich-sensor mobile phones and their wide adoption, in order to turn people to producers of sensed data and enable new classes of collective applications. Unavoidably, this raises a lot of privacy concerns, as people are becoming sensors and give out a lot of personal information, like their location. If we choose to protect their privacy by anonymizing the data and completely hiding any identifying information, then the visibility of their contributions to others is lost. However, it is important to maintain this property, in order to support accountability on one hand and allow people gain reputation for their efforts on the other hand. In this book chapter we investigate which of the available technical solutions we need, in order to resolve this conflict and what are the research directions that emerge.

1 Introduction

Over the several past years, there has been a great amount of research on wireless sensor networks, using dedicated embedded devices for data collection, e.g., from the environment or an infrastructure. The deployments of sensor networks have been treated as peripheral networks attached to the mainstream domain of the Internet through a gateway, delivering in this way data to the end-users. However, the initial vision of connecting thousands of sensors that have been randomly disseminated into the environment (“smart dust”) seems to be still far out of reach.

Ioannis Krontiris
Chair of Mobile Business and Multilateral Security, Goethe University Frankfurt, Germany,
e-mail: ioannis.krontiris@m-chair.net

Nicolas Maisonneuve, e-mail: n.maisonneuve@gmail.com

At the same time, the wide adoption of mobile phones in combination with the spread of the Web 2.0 paradigm on the Web recently created the right conditions for a new scope of research, often referred to as *participatory sensing* [1], which comes to complement our previous efforts in wireless sensor networks. Thanks to sensor-rich devices, geo-localised user-generated content can now be created any time, anywhere. Other sensors, besides geo-location chips, such as camera, gyroscope, light sensor or accelerometer started becoming more and more prevalent in mobile devices carried by billions of people, enabling new large-scale practices. So, the vision of a sensor data-sharing infrastructure emerged, where people and their mobile phone devices could provide sensor data streams in accessible ways to third parties interested in integrating and remixing data, enabling new citizen science campaigns [2, 3] and empowering local communities to manage their commons.

Participatory sensing regards end-users not only as consumers, but also as active producers of data and uses the sensors attached to the user as natural source of information.This new direction changes several underlying assumptions of typical sensor networks, as for example urban deployment, no pre-defined sink nodes, more powerful rechargeable nodes,mobility (humans, cars, etc.) and a new variety of sensors, attached closer to human beings and the context around them. With participatory sensing, the research area of sensor networks is moving into a direction, in which sensing networks will be several orders of magnitudes larger than the average existing classical sensor networks and where the short-term real-world impact may be much higher.

In the wireless network research community, participatory sensing is sometimes referred to as people-centric sensing [4], urban sensing [5] or mobile sensing [6]. But while all these terms are close, they emphasize different aspects. *People-centric sensing* focuses on the nature of the data collected, e.g. health data, food consumption or personal noise exposure, and it does not necessary refer to location-related data. *Urban sensing* emphasizes on the environment where the sensing process takes place, i.e., the urban space. *Mobile sensing* emphasizes on the mobility and the nature of the sensor device, i.e. the mobile phone. Finally, *participatory sensing* emphasizes on the participatory nature of some projects, which is the focus of this article.

Indeed, a lot of participatory sensing-related projects target only the individual level. An increasing number of mobile applications deliver self-monitoring services, for instance sensing their daily exposure to pollution, keeping track of their exercise activities, dietary habits, etc. While some of these services, like CenceMe [7], allow to share such information within social networks, they are mainly individual centric. However, in this chapter we focus on sensing projects that also target the community level and in which users sharing commons do not necessary get an individual and direct benefit from offering their sensing capabilities. They are rather motivated by a common cause or interest, similar to the participative paradigm of Web 2.0. Both levels are compatible. For example the NoiseTube [8] project enables citizens to measure their daily exposure to noise in their environment on one hand and report such information to produce a noise map representing the collective exposure experienced by the local people, on the other hand (see Figure 1).

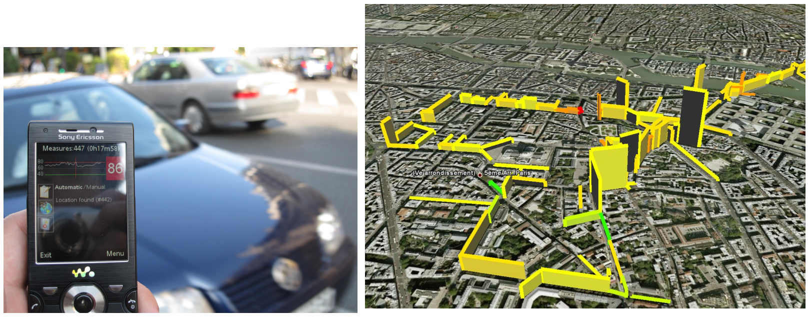

Fig. 1 The NoiseTube project [8]. A sensing project mixing mobile sensing applications with participatory and community building aspects to create a collective exposure map of noise pollution.

Problem Statement and Chapter Organization

In the first part of this chapter, we focus on participatory and accountability-related aspects. Currently, many projects call people to participate with the goal to collect sensor data. But these calls have been only moderately successful. The focus of research should be extended to investigate how we can make people involve more actively in participatory sensing projects. Secondly, like any participatory system, such as Wikipedia, participatory sensing is vulnerable to gaming and spamming. A major challenge, is thus enabling broad user participation by making the system accountable for all data.

To tackle these two issues in the general context of online communities, Erickson and Kellogg [9] proposed to integrate *Social Translucence* features. Social Translucence is a term to refer to “digital systems that support coherent behavior by making participants and their activities visible to one another”. The goal of such feature is to faciliate participation, self-organisation and *accountability*. Such social feature, present in current communities platforms (e.g. Facebook), could provide many benefits to the design of future participatory sensing projects.

At the same time, several research work is focusing on privacy issues of participatory sensing (see [10] for a survey). Indeed, with the mobile devices gathering sensor data from user’s immediate environment and deriving user context, privacy concerns are rightfully raised. In this chapter we focus only on location-related data as they are commonly sensitive. So the goal is to prevent access to location information at all costs, making it tamper-proof against both i) malicious hackers with the desire to intrude on other people’s privacy, and ii) against companies profiling and accumulating users’ location information for profit maximization.

Then the question that we raise in this chapter is: how can we maintain social translucence features to preserve participation and accountability, while preserving privacy at the same time? Indeed, protecting privacy will unavoidably limit the visibility and accountability of user contributions to the minimum.

In the second part of the chapter, to answer this question we explore the use of an anonymity-based approach: all data sent to the service provider do not include any identifying information of the sender. In the context of a social translucence design, we then investigate two related problems:

- In Section 4.2 we discuss about accountability. How to revoke the access credentials of users, who covered behind their anonymity, misbehave against the system?
- In Section 4.3, we discuss about maintening reputation and social recognition. How to enable users to accumulate reputation points and receive recognition for their contributions, even though these contributions were made anonymously?

2 Social factors for participation and accountability

As in many community-based services, a key factor in participatory sensing lies in the leverage of participation in data gathering. Even though the ubiquity of mobile phones makes mass participation feasible, as attempted in [11], it remains questionable how the general public can be motivated to voluntary participate. In most cases, participatory sensing projects call users to volunteer and offer the sensing capabilities of their mobile devices without getting any immediate social benefits. What benefits would they gain that might compensate them for their efforts?

Furthermore like any participatory system, such as Wikipedia, participatory sensing is vulnerable to gaming and spamming. A major challenge, is thus enabling broad user participation by making the system accountable for all data.

Well known Web 2.0 success stories such as Flickr, YouTube or Wikipedia prove that it is possible to actively involve people in community projects with no self-reflective benefits. The question is then, can we transfer online social practices from the digital world to the real world via mobile technology?

3 Social Translucence Design for Participatory Sensing

In the context of online communities, Kollock outlines three motivations that do not just rely on altruistic behavior on the part of the contributor: anticipated reciprocity, increased recognition and sense of efficacy [12]. Indeed, as pointed out in [13], the Web 2.0 phenomenon contradicts many predictions regarding the form of cooperation and community building that were encouraged by the founders of the Web. As shown in studies of bloggers or Wikipedia [14], the motivations of contributors do not fit into a single category. They are not either utilitarian, targeting to maximise personal interest or just altruistic, motivated by a desire to volunteer and be part of a community. Users generally first have individualistic motivations when they begin to make visible personal production (e.g. blog posts). Such tendency to get social recognition and attract attention by making their contributions public appears to develop a greater number of interpersonal relations than expected, although the links between individuals are weak. From such dense interaction emerge opportunities of cooperation, transforming user goals from individual interest to more collective.

A *social translucence* design has been proposed by Erickson and Kellogg [9] to make participant's contributions and activity visible to the community. Social Translucence is a term to refer to "digital systems that support coherent behavior by making participants and their activities visible to one another". Designing social infrastructure aims at supporting *mutual awareness and accountability* and thus facilitating participation and collaboration. Interpretation and understanding of those actions can influence the direction of public decision making [15], influence reputations [16], notions of expertise [17], as well as other aspects of collaboration.

4 The Tension between Privacy and Social Translucence

In the previous section we saw that visibility is a crucial requirement to sustain participation and accountability. However we speak of socially translucent systems rather than socially transparent systems, because there is a vital tension between privacy and visibility [9]. Indeed, sensing from a cellphone for collecting information from the environment and tagging them with time and GPS data, could be used to infer a lot of personal information, including the user's identity. This problem is often termed *location privacy*. Knowing when a particular person was at a particular point in time can be used to infer the personal activities, political views, health status, and launch unsolicited advertising, physical attacks or harassment. Location information is therefore in many cases a particularly sensitive piece of personal data and people have now started to realize more and more the need for location privacy [10].

In our pessimistic scenario users have strong concerns about privacy, while at the same time we would like to preserve social features as much as possible. What kind of social translucence design can we offer in this context? Is it possible to offer anonymity to the user, who submits sensing data from the physical environment, while at the same time we maintain properties connected to the translucence of his online identity, like reputation and accountability? So, in a way, while at the previous section we were looking to bring the users from the physical environment closer to the online communities, now we seek ways to maintain these benefits, but also separate their physical identity from their online identity.

In the following sections, we try to answer these questions by showing that indeed, (i) it is possible to revoke access credentials of anonymous misbehaving users and also (ii) award reputation points to anonymous users submitting data. In the latter case reputation values would be public, appearing on the user public profile in the community to express the degree of his/her contribution and receive attention.

4.1 System Architecture

As it turns out, it is not a trivial task to provide anonymity for pervasive contributions of sensor data, as many actors are involved in the process, who could potential harm the privacy of the users. Let us assume that any identifying information has been removed from the data, so it includes only the sensing information, the GPS value and the time of measurement. This is not enough to provide anonymity to the user, if we do not first of all protect identifying information at the network layer. Network identifiers can be used, either to reveal the identity of the user directly or link several reports back to the same user and therefore build a location profile of that user.

Figure 2 depicts the communication paths between the two communication ends in a generic participatory sensing architecture: the mobile users and the application provider. There are (at least) two network access possibilities for the user: through a data telecommunications service, like GSM or UMTS and through a (possibly open) WLAN access point. Providing anonymity at the first hop of communication, i.e. between the user and the mobile operator or the Wi-Fi hotspot, is a problem that falls outside the scope of this chapter. Here we consider attackers, who are able to observe the traffic over the Internet between the access point and the service provider. At this level the goal is to provide communication anonymity, which means hiding the network identifiers in the network layer (i.e., IP addresses).

Since mixes were proposed in 1981 [18] as a solution for achieving anonymous communication, multiple other protocols appeared in the literature in order to provide anonymity over the Internet. In particular, low-latency anonymous overlay networks seek to provide, from the user's point of view, a reasonable trade-off between anonymity and performance. Some of the most prominent low-latency approaches include Crowds, Tor, Jap, and Onion Routing. Still, only a few of these anonymizing networks have been tested for the mobile Internet scenario and it is an area that only lately attracted research interest [19]. Even though it is not hard to adapt protocols like Tor to conform to the mobile internet constraints, other more lightweight solutions remain to be investigated [20]. Nevertheless, in the rest of this book chapter, we will assume that a suitable anonymous overlay network is applied to offer the desirable protection at the communication level.

Let us note however that the interconnection of users through online communities creates a different setting for the evaluation of the performance by anonymous communication networks in our scenario. Here, an attacker, besides her observations at the network layer, has also knowledge from the application layer, i.e., the identities of the users that participate in the system and how they are related, through their profiles in the social group. Users organize themselves into a community with a common goal, and these users are expected to send measurements for the corresponding campaign. There is an *a priori* knowledge of user profiles and associations that can be combined with data gathered by traffic analysis of the mix-based network.

Diaz et al. studied the problem of measuring anonymity based on profile information [21] and social networks [22] and showed that user profile information does not *necessarily* lead to a reduction of the attacker's uncertainty. The assumptions in

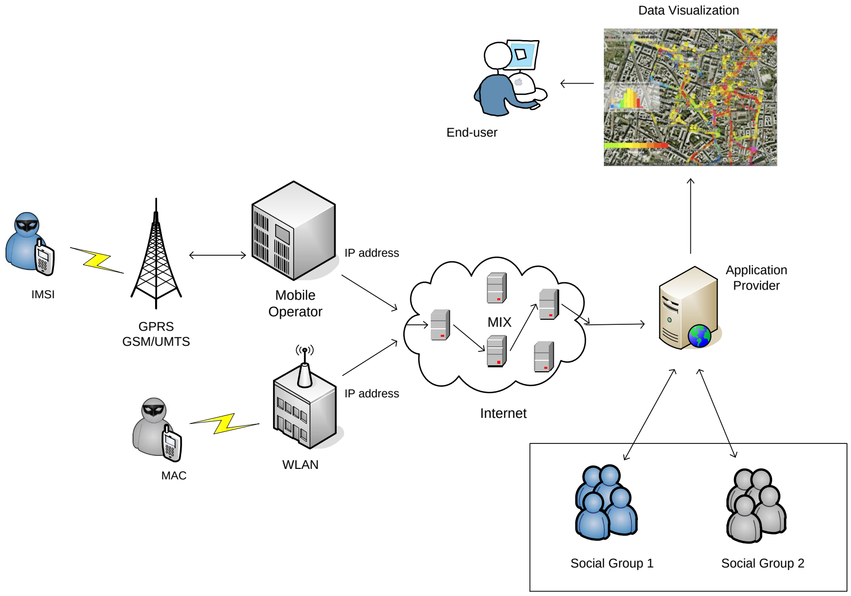

Fig. 2 A generic system model for a participatory sensing system, where users preserve their location privacy by submitting de-identified data. However, the network layer contains many identifiers that can be used to identify the users. Also the knowledge of the social group that an anonymous user belongs to, could reduce the offered anonymity.

this work include a 1-to-1 communication paradigm, where individuals communicate with each other directly, as well as a global passive adversary model, where the attacker can observe all the inputs and outputs of the anonymous communication network. Generalizing the first and relaxing the second assumption certainly creates an interesting but also challenging problem.

4.2 Revocation of Misbehaving Users

For most participatory sensing applications it is essential to enforce access control in order to prevent service abuse and to protect against malicious attacks. Access to services for users offering the data should be granted only based on pre-established trust between users and the service provider. Given that we also want to preserve anonymity, this leads to a chicken-and-egg conundrum. On one hand, a user has to be authenticated before accessing a service; on the other hand the users ID can serve as a unique identifier that can be used to track the users whereabouts and actions.

In response to this problem, a lot of research work has focused on anonymous user authentication that targets user privacy while maintaining access security. The basic idea has been to verify the users right to access a service, while at the same time the users identifying information remains secured. This immediately creates an important requirement: the support of *user revocation*. The anonymous access to a service offers users a high degree of privacy and along with it the license to misbehave without the fear of punishment. Therefore we want to be able to deanonymize misbehaving users and limit their access to the system.

An approach for enhancing anonymous authentication is to use *group signatures* [23], where a vast amount of research is being carried out worldwide. These technologies can be used to verify whether or not a user is allowed access, without actually identifying the user. This is achieved by allowing a member of a group to sign a message on behalf of the group, without revealing which member produced the signature. Group signature systems can support revocation, where group membership can be selectively disabled without affecting unrevoked members.

In order to apply group signatures for mobile phones and users belonging to highly dynamic communities, we need to address a number of problems that come with this solution. For example, in online communities members continuously come and go and a solution to change and re-distribute fresh certificates to all members each time is not a viable solution. This problem has been addressed by anonymous credential systems that support dynamic membership revocation [24, 25].

Existing group signature solutions are based on a trusted third party (TTP), which has the ability to revoke a user's privacy at any time. This becomes problematic, since users can never be assured that their privacy will be maintained by that TTP. To eliminate the reliance on TTPs, certain "threshold-based" approaches such as e-cash [26, 27] and k-Times Anonymous Authentication (k-TAA) [28] have been proposed. In these schemes, no one, not even an authority, can identify a user who has not exceeded the allowed number of k authentications or spent an e-coin twice.

However misbehavior in participatory sensing applications is not defined as overusing a service. In our case, we are interested in revoking users who upload data, which after a specific process are judged as "inappropriate". When they have been judged to have repeatedly misbehaved at least d times, they should be revoked by the system. This problem has been addressed recently by Tsang et al. [29], who proposed a d-strikes-out revocation scheme for blacklisting misbehaving users, without relying on a TTP. Unfortunately the computational and communication overhead of the protocol is not attractive for power-limited devices such as mobile phones, especially as the size of the blacklist grows.

4.3 Anonymous Reputation

As we discussed above, offering reputation points to people submitting data can form a sort of recognition to their efforts. These reputation points are collected when submitting data to the service provider and then they are publicly displayed in the profile that the user maintains in the community. The challenge to comply with the privacy properties that we also described above should now be obvious. A direct process of acquiring reputation points for a given report and display them on a public profile would clearly compromise the anonymity of the submitter. So, we need to provide a protocol that satisfies the following two properties:

- The process of acquiring reputation points is independent from the process of updating the reputation value on someone's public profile.
- The process of acquiring reputation points for two successive reports should be unlinkable with each other, in order to maintain the unlinkability of reports.

One way is to base the solution on Chaum's eCash [18]. An electronic cash system aims at emulating regular cash and offers anonymity properties: an adversary cannot link a spending to a withdrawal. In our system, the whole process takes place in two independent phases: First a user U communicates with the service provider under a randomly chosen one-time pseudonym P_U to submit the data. The user obtains an e-coin from the bank for each report submission, each one corresponding to a reputation point. In the second phase, the user logs-in using his regular public profile and redeems the e-coin to get a reputation point and increase his total reputation. E-coins can be spend only once, and cannot be transferred to other users.

However we cannot solve the problem of a secure reputation system just by using an eCash scheme. E-coins are anonymous, but linkable, which in turn leads to the linkability of the reports submitted in order to acquire these e-coins. The use of other cryptographic tools are required as well, such as blind signatures [30]. For an example of how these cryptographic tools can be combined to build a reputation system for anonymous networks, we refer the reader to the recent work of Androulaki et al. [31]. One of the drawbacks of this protocol is that negative reputation is not supported. That is, users can only increase their reputation and eventually the system will reach a final state, where all users have the maximum reputation. After this point, no user has the incentive to collect new reputation points.

To address this problem, Schiffner et al. [32] proposed a solution that supports non-monotonic reputation. By allowing negative ratings, the problem that emerges is that ratees cannot be forced to deposit received reputation coins, i.e., the ratee can decide on his own whether he wants to deposit the received rating an of course he would not deposit a negative coin. To overcome this, the authors force the rating of every interaction. That is, the reputation provider keeps account not only of the reputation, but also of the interactions, guaranteeing that each interaction is actual rated, possibly also in a negative way.

5 Conclusion

In this book chapter we introduced the emerging research area of participatory sensing and concentrated on the location privacy challenges. We took the approach of protecting user's privacy by anonymizing their data before submission to the service provider. On the other hand, we argued that offering social translucence to the users is important for the success of future participatory sensing campaigns. As these two goals are contradictory with each other, we looked for social translucence properties that are still possible, even under user anonymity like accountability and reputation.

For the first, we saw that indeed revoking anonymous misbehaving users is possible, even without relying on a trusted third party (TTP), but more work would be needed to improve the performance of such protocols in the pervasive scenario. For the latter, some protocols exists that allow anonymous users to collect reputation points using a combination of e-cash systems and blind signatures. However, they currently do not support more complicated reputation systems that will be needed to support incentive and community building mechanisms of participatory sensing. Finally, it remains an interesting problem to see what other tools we can develop in the future to provide even more social translucence for anonymous users in participatory sensing systems.

6 Acknowledgements

We are grateful to Felix Freiling for the fruitful discussions regarding this work.

References

1. J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava, “Participatory sensing,” in *Workshop on World-Sensor-Web (WSW’06): Mobile Device Centric Sensor Networks and Applications*, pp. 117–134, October 2006.
2. A. Irwin, *Citizen Science: A Study of People, Expertise and Sustainable Development*. Routledge, 1995.
3. E. Paulos, R. Honicky, and B. Hooker, *Citizen Science: Enabling Participatory Urbanism*, ch. 28. 2008.
4. A. Campbell, S. Eisenman, N. Lane, E. Miluzzo, R. Peterson, H. Lu, X. Zheng, M. Musolesi, K. Fodor, and G.-S. Ahn, “The rise of people-centric sensing,” *IEEE Internet Computing*, vol. 12, no. 4, pp. 12–21, 2008.
5. D. Cuff, M. Hansen, and J. Kang, “Urban sensing: out of the woods,” *Communications of the ACM*, vol. 51, no. 3, pp. 24–33, 2008.
6. N. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. Campbell, “A survey of mobile phone sensing,” *IEEE Communications Magazine*, vol. 48, pp. 140–150, September 2010.
7. E. Miluzzo, N. D. Lane, K. Fodor, R. Peterson, H. Lu, M. Musolesi, S. B. Eisenman, X. Zheng, and A. T. Campbell, “Sensing meets mobile social networks: the design, implementation and evaluation of the cenceme application,” in *Proceedings of the 6th ACM conference on Embedded network sensor systems (SenSys ’08)*, pp. 337–350, 2008.
8. M. S. Nicolas Maisonneuve and B. Ochab, “Participatory noise pollution monitoring using mobile phones,” *Information Policy*, vol. 15, pp. 51–71, 2010.
9. T. Erickson and W. A. Kellogg, “Social translucence: an approach to designing systems that support social processes,” *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 7, no. 1, pp. 59–83, 2000.
10. I. Krontiris, F. C. Freiling, and T. Dimitriou, “Location privacy in urban sensing networks: Research challenges and directions,” *IEEE Wireless Communications Magazine*, October 2010.
11. M. Paxton, “Participate: Producing a mass scale environmental campaign for pervasive technology,” in *6 th International conference on Pervasive Computing*, 2008.

12. P. Kollock, *The Economies of Online Cooperation: Gifts and Public Goods in Cyberspace*, ch. 9, pp. 220–239. 1999.
13. C. Aguiton, D. Cardon, and F. T. R, "The strength of weak cooperation: an attempt to understand the meaning of web 2.0," *Communication & Strategies*, vol. 65, 2007.
14. S. L. Bryant, A. Forte, and A. Bruckman, "Becoming wikipedian: transformation of participation in a collaborative online encyclopedia," in *GROUP '05: Proceedings of the 2005 international ACM SIGGROUP conference on Supporting group work*, (New York, NY, USA), pp. 1–10, ACM, 2005.
15. A. Borning, B. Friedman, J. Davis, and P. Lin, "Informing public deliberation: Value sensitive design of indicators for a large-scale urban simulation," in *In Proc. 9th European Conference on Computer-Supported Cooperative Work*, 2005.
16. P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," *Commun. ACM*, vol. 43, no. 12, pp. 45–48, 2000.
17. D. Mcdonald and M. Ackermann, "Just talk to me: A field study of expertise location," 1998.
18. D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.
19. J. Lenhard, K. Loesing, and G. Wirtz, "Performance measurements of Tor hidden services in low-bandwidth access networks," in *Proceedings of the International Conference of Applied Cryptography and Network Security (ACNS '09)*, pp. 324–341, June 2009.
20. I. Krontiris and F. C. Freiling, "Integrating people-centric sensing with social networks: A privacy research agenda," in *Proceeding of the IEEE International Workshop on Security and Social Networking (Sesoc)*, 2010.
21. C. Diaz, C. Troncoso, and G. Danezis, "Does additional information always reduce anonymity?," in *Proceedings of the 2007 ACM workshop on Privacy in electronic society (WPES '07)*, pp. 72–75, 2007.
22. C. Diaz, C. Troncoso, and A. Serjantov, "On the impact of social network profiling on anonymity," in *Proceedings of the 8th international symposium on Privacy Enhancing Technologies*, 2008.
23. D. Chaum and E. van Heyst, "Group signatures," in *Advances in Cryptology - EUROCRYPT '91*, pp. 257–265, 1991.
24. J. Camenisch and A. Lysyanskaya, "Dynamic accumulators and application to efficient revocation of anonymous credentials," in *Advances in Cryptology—CRYPTO 2002*, (London, UK), pp. 61–76, Springer-Verlag, 2002.
25. D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *Proceedings of the 11th ACM conference on Computer and communications security (CCS '04)*, pp. 168–177, 2004.
26. J. Camenisch, S. Hohenberger, and A. Lysyanskaya, "Compact e-cash," in *Advances in Cryptology—EUROCRYPT 2005*, pp. 302–321, 2005.
27. J. Camenisch, S. Hohenberger, and A. Lysyanskaya, "Balancing accountability and privacy using e-cash (extended abstract)," in *Proceeding of the 5th Conference of Security and Cryptography for Networks (SCN '06)*, pp. 141–155, 2006.
28. I. Teranishi, J. Furukawa, and K. Sako, "k-times anonymous authentication," in *Proceedings of the 10th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT '04)*, pp. 308–322, December 2004.
29. P. P. Tsang, M. H. Au, A. Kapadia, and S. W. Smith, "BLAC: Revoking Repeatedly Misbehaving Anonymous Users Without Relying on TTPs," 2010.
30. D. Chaum, "Blind signature system," in *CRYPTO*, p. 153, 1983.
31. E. Androulaki, S. G. Choi, S. M. Bellovin, and T. Malkin, "Reputation systems for anonymous networks," in *Proceedings of the 8th international symposium on Privacy Enhancing Technologies (PETS '08)*, (Leuven, Belgium), pp. 202–218, 2008.
32. S. Schiffner, S. Clauß, and S. Steinbrecher, "Privacy and liveliness for reputation systems," in *Proceedings of the 6th European PKI Workshop: Research and Applications (EuroPKI '09)*, (Pisa, Italy), 2009.