Security and Privacy Challenges in Smart Sensor Networks

Cristian Tanas
Dept. Eng. de la Informació i les Comunicacions
Univertsitat Autònoma de Barcelona
ctanas@deic.uab.cat

Cristina Pérez-Solà
Dept. Eng. de la Informació i les Comunicacions
Univertsitat Autònoma de Barcelona
cperez@deic.uab.cat

Jordi Herrera-Joancomartí
Univertsitat Autònoma de Barcelona
jherrera@deic.uab.cat
IN3 - Univertsitat Oberta de Catalunya
jherreraj@uoc.edu

***Abstract*—*Smart sensor networks* fall into a new sensor network paradigm that involve individuals in the sensing data collection process. While prior sensor network paradigms focused on collecting ephemeral data about the surrounding environment by means of a static sensor node topology, smart sensor networks collect and process large amounts of data regarding daily life activities. Being humans the central focus of this new kind of environments, there arise new information security challenges. In addition, the nature of the sensed data results in substantial user privacy threats. In this paper we aim to start a discussion around these critical issues by providing an outline of several important information security and privacy challenges.**

I. Introduction

Nowadays, modern smartphones are practical computing platforms with complex sensor capabilities allowing them to perform multiple sensing tasks such as detecting user location, recording high-quality images or audio, geomagnetic strength, orientation, etc. Due to the increasing popularity of smartphones, a new opportunity raises to develop large-scale sensor networks using cellular network technology and deploy applications on consumer-owned smartphones to collect and report sensor readings back to data collection facilities. Moreover, if end-users are involved in the data collection tasks acting as sensors we will refer to these new kind of sensor networks as *smart sensor networks* (SSN). These sensor networks can help overcome many of the limitations of existing proposals in wireless sensor networks, which require physical deployment and customized node management in addition to complex communication protocols.

Nevertheless, the new opportunities and benefits offered by modern smartphones as sensing devices come at a price. Bringing together geographically and sociologically unrelated individuals to create a community that performs tasks for a greater good brings up to front new challenges and security and privacy issues that might have a strong impact on the overall performance of the network. Sensor network authorities, now have to deal with potential sabotage (intentional or unintentional) from the smartphone users. Great efforts are needed to ensure the sensor network data reliability, and how to derive trust in the sensor readings provided by users becomes an important research question in these environments. Moreover, to engage as many users to participate in the sensor network's sensing tasks is a major challenge since usually, device owners are reluctant to share their precious resources if no direct benefit is perceived.

On the other hand, sensor data often contain GPS positioning information, which reveals real-time accurate knowledge about not only the smartphone, but also the individual using the device. If not handled properly, this information can strongly compromise the user's privacy. Even if users consent this information being transmitted to data collection facilities, sensor network managers must ensure that this data stays safe from third parties.

In this paper, we survey the main security and privacy challenges introduced by these emerging sensing networks and identify some key concepts to deal with them, aiming to incentive further research in this area.

The paper is organized as follows. In Section II, we illustrate the smart sensor network architecture and overview its key features and existing proposals. The security challenges raised in this kind of environments are discussed in Section III. In Section IV we analyze the privacy issues in smart sensor networks. Finally, we draw some conclusions in Section V.

II. Smart Sensor Networks

Sensor networks have become one of the most active areas in networking research over the last decade, providing overwhelming potential for information collection and processing in a wide range of environments. The state of the art approaches in sensor networking include a limited number of static devices, usually wirelessly connected, spanned over a pre-determined geographical area gathering transitory information of the environment around them. We focus on a new generation of sensor networks, those targeting daily life activities of individuals and the environment surrounding them by means of small devices with sensory abilities, carried by individuals in their daily activities, recording continual features of the environment.

This new kind of sensor networks are based on a completely new set of assumption and tradeoffs, but at the same time provide an inexpensive scheme to access information

Acknowledgements: This work has been partially supported by the Spanish Government through projects TSI2007-65406-C03-03 E-AEGIS, CONSOLIDER-INGENIO CSD2007-00004 ARES, TIN2011-27076-C03-02 CO-PRIVACY , TIN2010-15764 N-KHRONOUS.

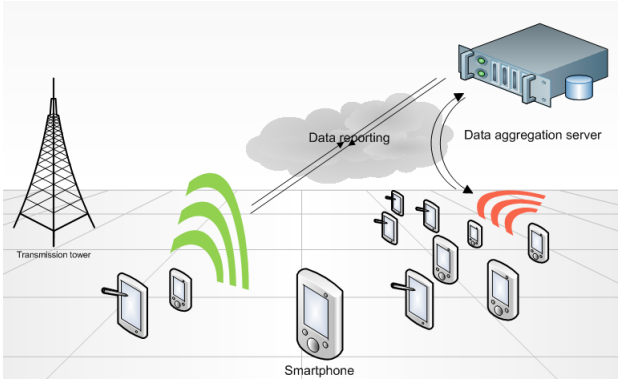

Fig. 1. Typical scenario for smartphone sensor networks

that would otherwise be excessively difficult or expensive to collect, since we rely on a crowd of volunteer individuals for information. Furthermore, technology advances in the mobile phones area allowed manufacturers to build more intelligent and sensing-aware devices, *smartphones*, which, if paired with the crowd, provide a cheap, scalable and effective way to effectively map crowd-based data collection tasks to end-user controlled smartphones. Indeed, modern smartphones besides being sophisticated computing platforms, include a wide range of capabilities, like computing (CPU, data storage,...), communication (UMTS, WiFi, Bluetooth) and sensing (positioning -GPS-, motion -accelerometer-, image -camera- , audio -microphone-).

On the other hand, deployment of such devices is exploding, and competition between Apple and Google expands over 74% of the market share with approximately 110 millions of devices sold during the 4th quarter of 2011 according to Gartner, Inc. [1]. The same advisory company estimates that total smartphone sales in 2011 reached 472 million devices, 31% of all mobile devices sales, up 58% from 2010.

Therefore, we can take advantage of the widespread use of smartphones combined with their sensing capabilities to gather sensory data from the environment and then send the sensed data back to data collection facilities using cellular network technology. This kind of sensor networks are referred to as *smartphone sensor network*. Smartphone sensor networks don't require any human intervention and they rely exclusively on the sensors integrated with the device to infer environmental data. Figure 1 illustrates a typical smartphone sensor network scenario.

On the other hand, it might be useful to have individuals participating in the sensing tasks. Surrounding environment detection, information processing, or great communication skills are just some of the qualities that individuals posses. Therefore, we can take advantage of both available sensors in a smartphone and smartphone's owner intelligence in order to acquire better knowledge on continual features of the landscape. Users can provide additional information to sensor readings, such as natural language description of the environment or location-tagged images, thereby provisioning researchers with a substantial wealth of data. Since now we are relaying on users to act as sensors we could refer to them as *smart sensors*, and we will refer to this new type of sensor networks as *smart sensor networks* (SSN).

A. Benefits

The smart sensor network capabilities can help overcome some of the limitations and challenges raised by traditional wireless sensor networks. The most relevant are next listed:

1) Over-the-air sensor node software distribution and upgrade: Using smartphones to power a sensor network, a large geographic area distribution can be achieved with a huge advantage in the number of nodes attained per unit of cost. Nowadays most used mobile platforms provide a common application distribution mechanism, such as the Apple's *App Store* or the Android's *Android Market*. This way they eliminate any need for a network manager to manually span the nodes over a certain geographical area. The network participants can take part in the sensing tasks of the network by simply downloading the application hosted by their mobile platform distributor.

In addition, this distribution mechanisms allow automatic upgrades of the software applications. Thereby, software improvements and modifications developed after the deployment can be easily transfered to the sensor devices without requiring physical contact with the device.

2) Cost reduction in sensor hardware maintenance: Repairing faulty nodes in traditional sensor networks can be a cumbersome task. Network maintainers have to manually locate, travel to and repair-on-site the nodes. In SSNs, the smartphones' owners have invested in the devices and also these devices are used for quotidian activities such as making phone calls, connecting to the Internet or listening to music. As a result, device owners are inherently motivated to maintain the phone, and therefore maintain the sensors. Moreover, battery life is no longer a problem since users will provide power maintenance for the smartphone to avoid battery deficiency.

3) Powerful smartphone processors and high level programming APIs: Most of the smartphones available on the market have very competitive processing capabilities allowing raw data collection and data processing in levels that were previously impractical in traditional sensor nodes. For example, higher-resolution images can be obtained, offering greater details about the environment under study.

Furthermore, modern smartphones operating system and high level programming languages enable developers to write software that is more loosely-coupled to the underlying hardware and focus only on domain-specific parts of the sensor software. Many modern mobile platforms, such as Android or iOS, allow a development model based on reusing and aggregating components into new applications, empowering the reuse of third-party components, such as advanced video decoding libraries or map visualization modules, for task completion.

4) Availability of standard and flexible network infrastructures: Many available smartphones support different standard

network infrastructures, both ad hoc protocols (such as Bluetooth), and direct Internet connections (3G or WiFi). This flexibility doesn't force the utilization of complex ad hoc wireless communication schemes, like in traditional WSN, but allows a device to dynamically specify the protocol in use based on high-level decisions regarding communication range, speed, battery usage, etc.

5) Human populations mobility monitoring: In order to measure certain characteristics inherent to mobile human populations, a large number of nodes dispersed in a large geographical area are required. Stimulating cooperation among smartphone owners to perform sensing task can inquire in a much greater sensor mobility. Indeed, in busy locations where many smartphones are traveling a reduced number of devices can provide equal coverage relative to a fixed location sensor network. Since mobility in an inherent property of smartphones, larger areas can be covered and these smart sensor networks are more suitable for sensing task where mobile, largely dynamic, and unpredictable properties have to be measured.locations, disaster relief worker tracking, measuring air quality, or measuring noise pollution levels.

B. Existing proposals

Smart sensor networks have a large number of potential applications. However there are just a few proposals that leverage the idea of having sensing tasks relayed to consumer-owned smartphones, and the majority were developed for experimental purposes.

The SSN application spectrum ranges from CO_2 emission monitoring [2] to patient health monitoring systems where smartphones are used in combination with wireless (bio) sensors to monitor a patient's vital signs [3], passing through a longer list of location-based services, such as traffic accidents detection and situational awareness provisioning to first responders [4], traffic conditions monitoring [5], or real-time trail network update for hikers and mountaineers [6].

Furthermore, smart sensor networks can provide support in emergency scenarios or environmental disaster as A. Gahran explained in an article on how citizens living in the Gulf Coast region could use their smartphones sensors, such as GPS and cameras, to enter data on the ecological impact of the Gulf oil spill, providing specialists with first hand information of this disaster [7]. This information was latter used to generate impact analysis and provide recommendations.

III. Security Challenges

Motivating smartphone owners to yield their resources and collaborate in a smart sensor network provides clear advantages and performance improvements over traditional wireless sensor networks. However, it also raises several concerns and problems, specially when dealing with network security and privacy protection.

Security issues posed by recent sensor networks paradigms represent a rich field of research problems. Although sensor nodes are exposed to sensor node compromise, eavesdropping or Denial-of-Service (DoS) attacks, these are common to all sensor networks paradigms and networking applications, and there are on-going research lines dealing with these concerns. On the other hand, deriving trust in data contributed by a crowd of anonymous volunteers or stimulating individual participation in the sensor network's tasks are specific challenges associated with smart sensor networks. An in-depth analysis of these challenges will be the scope of the remainder section.

A. Key issues regarding smart sensors

Consumer owned smartphones come along with a new set of complex, emergent system properties, and context-dependent characteristics that difficult the task of sensor network managers to ensure that the chosen system architecture, protocols, and policies will work as expected and meet the desired objectives of the sensing tasks. The following key issues have a direct impact on the sensor network's performance and must be taken into account when deploying crowd-based sensor networks.

- **Density**. When deploying a SSN, the node density in the target area is difficult to determine *a priori* since the number of individuals willing to participate in the sensor network's data collection tasks is unknown to the network managers. Node density has a clear impact on the system's success or failure taking into account that a context-dependant minimum density of participating sensor nodes must be assured in order to guarantee the sensory data collected is meaningful.
- **Availability**. The availability of sensor nodes is highly unpredictable as the devices might appear or disappear from the sensor network in a manner dictated by its owner. Moreover, energy constraints, GPS coverage and the intermittent Internet connectivity can severely affect node availability since they could incapacitate the device from collecting information or transmitting it.
- **Mobility**. Mobility is an inherent property of human population and influences to a great extent the node availability and the number of sensor nodes present in the target area at a given instant of time. Sensing applications must take into account that there is a limited amount of time a sensor node can query information about its surrounding environment dictated by the individual's trajectory and velocity.
- **Identity**. In common smart sensor networks scenarios the data collection tasks are relayed to a crowd of anonymous volunteers, making network control mechanisms extremely difficult and expensive. Moreover, protected by their anonymity, individuals may have a certain predilection to misbehaviour, exposing the sensor network to data forgery attacks.

B. Data reliability

To deliver up-to-date, accurate and reliable information is the main goal of a sensor network. Since in a SSN-based service data is collected by means of a crowd of anonymous volunteers, a data evaluation process is required to assess the reliability of the data and ensure that wrong data is

not entered into the database. In this kind of collaborative environments, it is not reasonable to assume that the collected data is correct or valid since some network participants could intentionally undermine the sensor network data by sending false information back to the data storage facilities.

1) Control mechanisms: There are mainly three approaches or control mechanisms that can be used to validate sensor readings:

- **In site data validation**. The first approach is to have sensor network managers traveling to the location of the sensor node and verifying that the sensor readings provided correspond to reality. However, it is obvious that this method is infeasible since it would incur a great loss in time and money. Moreover, sensor readings may have changed up to the arrival of the network maintainer.
- **A measure of user trustworthiness**. Another approach is to have trustworthy users identified in the sensor network and thereby consider any information proceeding from them as valid. A trustworthy user can be a user that benefits from high credibility within a community or a user that receives economic benefits for the provided services. Nevertheless, it is not straightforward to determine one individual's credibility. Reputation system could provide a quantification method where a high reputation value could determine the individual's credibility or trustworthiness. However, determining a threshold reputation value beyond which a user can be considered as trustworthy or providing a robust process through which users increase their reputation are still open problems in reputation systems related research.
- **Rating of data on the same object**. Collective knowledge and confirmations of the collected information from different users can be used to derive a measure of data reliability. As stated by F. Sayda [6] the method can be summarized with the following sentence: *"If enough users say that an object presents a certain property, it is likely that it really is a property of the object"*. A simple approach would be counting the number of sensors reporting the same information and validating this information if a predefined number of sensors have reported it. The problem is the exact meaning of *"enough"* in this context. Again, there are no studies proposing a model to quantify the minimum number of confirmations required to validate a sensor reading, and how this model can be complemented with the sensor density information.

C. User selfishness

A smart sensor network is formed by a collection of end-user controlled smartphones with wireless communication capabilities. These devices can suffer from energy constraints or limited bandwidth making their owners reluctant to offer their resources in an altruistic manner. By nature, humans are selfish. A selfish smart sensor withholds to spend its resources (e.g. battery) since it implies an energy cost and has no revenue. Instead, it will be encouraged to participate when the network tasks maximize the individual's own profit. A user could benefit from the information provided by the sensor network (noise pollution levels, map of cellular coverage), but refuse to provide sensed data to avoid battery consumption.

If no measures are implemented to promote and stimulate cooperation, it is very easy for a user to behave selfishly and stop participating in the data collection tasks or the sensed data forwarding process. Moreover, the detection of this kind of misbehavior is a very challenging task due to the unreliable nature of the wireless environment, which can lead to frequent communication failures, or the energy constraints, which can lead to battery exhaustion. Nevertheless, selfish behavior is critical for the performance of the sensor network up to the point that sensing activity could not take place.

Protocols to foster cooperation can be categorized as *reputation-based* and *credit-based* according to Marias *et al.* [8]. The former are based on reputation building and the later are based on economic incentives (i.e. money or token-based) to stimulate cooperation. Reputation-based schemes place more weight on sensing data received from the most reliable nodes, that is the nodes with a higher reputation value. The reputation of a node increases when it collaborates in the data collection tasks. On the other hand, credit-based schemes can model the sensor data collection as a service that can be valued and charged. These models incorporate a form of virtual currency to regulate the dealings between sensor nodes and sensor network managers. The obtained currency can be later used to access additional services.

H. Rifà [9] states another way of grouping cooperation protocols, namely policy model, according to the relation that will be established between SSN nodes. Cooperation models can be further categorized as *cooperation enforcement* and *cooperation incentive* protocols. The former consider cooperation as mandatory and attempt to force a balanced participation among those users who have enough energy and bandwidth resources. The later, on the other hand, promote voluntary and generous donations letting users decide if they wish to participate and in what extent.

Reputation-based schemes can follow any of the two stated policy models. However, the combination of a credit-based scheme with an enforcement policy model it is not feasible. Indeed, if the policy model states that the cooperation is mandatory, there is no need to design a credit exchange mechanism to control the incomings or what a user consumes, because this rating is not correlated with the user's duty to cooperate.

IV. Privacy Challenges

Involving users in data collection tasks introduces many challenges on designing privacy preserving SSN, in addition to those already existent on wireless sensor networks. Sensor data readings available from smartphones (for instance, positioning, motion, or audio) together with real time data provided by users involved in the collection process, constitute sensitive data which disclosure has to be carefully made in order not to invade user's privacy. Designing privacy preserving SSN is a

challenging task that we start by identifying the problems and attacks that can be conducted on SSN data.

Privacy threats that SSN will have to deal with depend on the specific adversary model defined for each scenario. Different adversaries have different resources on their power, and thus different levels of data access. Moreover, distinct adversaries may also have several divergent goals in mind when attacking SSN. In general, adversaries can be classified depending on their capabilities and their view of the network. Privacy literature usually classifies adversaries depending on their spatial scope (global vs local), their temporal scope (short term vs long term), their ability to interact with the network (active vs passive) and their target scope (individual vs mass).

The architecture of the SSN has to be taken into account in order to assess the possible adversaries that may attack the network, together with the privacy threats that they involve. While totally centralized architectures are susceptible to global adversaries that can observe all the traffic of the network, decentralized architectures may be more concerned by the threats that malicious users can suppose to the network.

Typical adversaries that may attack a SSN are:

- SSN software provider: the SSN software provider is the entity that develops smartphone applications to be used as sensors in the SSN. Having access to all communications in the network, this global, long term, passive attacker, usually targeting a huge amount of users, is one of the most powerful attackers in centralized architectures.
- Network provider: the network provider is also able to monitor all traffic that goes through a centralized architecture, but unlike the software provider, it may not be able to see the contents of the messages that go through the network. The network provider is also a global, long term, passive attacker.
- Third party service providers: smartphone applications often make use of third party services in order build all the functionalities of their applications. Map embedding is one of the most usual features that make use of third party services. By using these services, the SSN leaks information to the 3rd party provider, which can potentially become a long term, passive attacker.
- Eavesdropper: an adversary that gains knowledge of the network by listening to communications between nodes or between nodes and the central server is a local, short term, passive attacker.
- (Other) users: users of the network can also take the role of an attacker by either trying to attack the network itself or either attempting to compromise other users in the network. This kind of attacker is a local, short term but active attacker, usually focused on a single target.

Many privacy threats arise from the usage of smart sensor networks. Some of these threats also affect other data release scenarios and are thus already identified in the literature. Disclosure attacks on information about individuals are usually classified in attribute disclosure or identity disclosure attacks [10], and have been widely studied in the past:

- **Attribute disclosure:** Attribute disclosure attacks are focused on learning new information (attributes) from a user or a set of users.
- **Identity disclosure:** Identity disclosure attacks are focused on linking a record in the released data with a subject.

Identity disclosure often leads to re-identification of an individual, and thus ends up in attribute disclosure. However, attribute disclosure may take place both with and without re-identification.

Other privacy threats arise from the context information appearing in user's queries. Although many context data can be used by an attacker, researchers have focused on studying the impact on location and time in user's queries. Location privacy attacks identified for services using location data also concern SSNs:

- **Presence disclosure:** Presence disclosure attacks are focused on discovering if a given user or a set of users are present at a given location at a given time [11], [12]. Presence disclosure attacks may have several privacy implications. Just knowing if a user has been at a given location can already disclose sensitive information. Take for example a sensor network application that requires the sensor's location to compute a map for cellular network coverage. The sensor's and implicitly the user's location is needed for accurate coverage calculations; however an adversary might infer restricted information from the available context: if Alice participates in the data collection process and her location matches the location of a given political party headquarters, an attacker could infer her politic ideals. Moreover, knowing the exact time when Alice was at the specified location can also reveal compromising information: if a radical cell of the political party is meeting at a specific time, knowing that Alice was there at that time is more compromising.
  Generally, the attacks which goal is to discover the whole sequence (or a partial sequence) of places where the user has been are called **tracking** attacks, whereas attacks focused on retrieving a single position (at a single instant) are known as **localization** attacks [11].
- **Absence disclosure:** On the contrary, absence disclosure attacks have as their goal to learn if a given user is not at some location at a given time [11], [13]. A typical absence disclosure attack happens when Alice goes on holiday: disclosing that she is not going to be at home for a long period of time can be exploited by an adversary to commit robbery. Some initiatives such as the *Please Rob Me* website [14] have been made in order to increase people's awareness of absence disclosure attacks. Nevertheless, the absence of a smart sensor can prove itself essential for the SSN since it implies that no more sensor readings will be available from that sensor.
- **Meeting disclosure:** The goal of meeting disclosure attacks [12], also referred as co-location attacks in the literature [15], is to reveal physical proximity between users.

By knowing that multiple users were on the same location at a the same time, an attacker can infer information of the existing relationship among those users. Inferring information of the frequency of those encounters, the number of users involved or the location and time where the meetings took place are some of the attacks that fall into this category.

- **Aggregated presence attack:** Aggregated presence attacks aim to discover the number of users that are present at a given location at a given time, regardless of who are those users [12]. Although this kind of attack is less intrusive than the three attacks described above, aggregated presence information can be used to collect statistical information about the density of users at a given location, disclosing the best place to launch a chemical attack, for example.
- **Identification:** The goal of identification attacks is to discover the real identity of a user or a set of users [11]. Identification attacks do not only appear in relation to location privacy. However, re-identification attacks with anonymous location information have been done by linking users with sensitive places such as home or work [16], [17], [18] or by analyzing mobility patterns [19].

Note that although these attacks are presented as different problems that arise when dealing with location data, some of these attacks are in fact closely related. For instance, tracking attacks usually end up with the identification of the subjects.

Finally, in addition to privacy threats already existing in individual data release and location data scenarios, smart sensor networks introduce another privacy threat that can be categorized as **behavioral profiling**. Attacks focused on collecting longitudinal data about personal activities [20], [21], fall into this category. Behavioral profiling is usually done to modify user experience based on those activities. Depending on the scope and functionalities of the SSN applications deployed, behavioral attacks can also be a threat that SSN users may have to deal with.

V. Conclusions

In this paper we acknowledge the increasing interest in human-centric sensor networks where sensing task are relayed to end-users in possession of a smartphone. Such scenarios exhibit undeniable security and privacy challenges which must be resolved if these systems have any intentions to take full advantage of their potential. Data reliability and user selfishness have been identified as two major security issues specific to smart sensor networks. Moreover, sensor readings available from smartphones, such as positioning or motion, combined with real time data provided by end-user lead the way to user's privacy intrusion. Sensitive data disclosure and location privacy have been identified as two major drawbacks towards privacy preserving smart sensor networks development. We hope this paper will encourage further discussion and research in this field, and open a path for researchers to develop new methods and protocols to deal with the security and privacy challenges present in this new kind of environments.

References

[1] "Press Release. Gartner Says Worldwide Smartphone Sales Soared in Fourth Quarter of 2011 With 47 Percent Growth," *Gartner Newsroom*, Feb. 2012, http://www.gartner.com/it/page.jsp?id=1924314 (last access 26 Mar. 2012).

[2] J. Froehlich, T. Dillahunt, P. Klasnja, J. Mankoff, S. Consolvo, B. Harrison, and J. Landay, "UbiGreen: investigating a mobile tool for tracking and supporting green transportation habits," in *Proceedings of the 27th international conference on Human factors in computing systems*. ACM, 2009, pp. 1043–1052.

[3] P. Leijdekkers and V. Gay, "Personal heart monitoring and rehabilitation system using smart phones," in *Proceedings of the International Conference on Mobile Business*. Citeseer, 2006, p. 29.

[4] C. Thompson, J. White, B. Dougherty, and D. Schmidt, "Optimizing mobile application performance with model-driven engineering," in *Proceedings of the 7th IFIP Workshop on Software Technologies for Future Embedded and Ubiquitous Systems*, 2009.

[5] G. Rose, "Mobile phones as traffic probes: practices, prospects and issues," *IEEE Spectrum*, vol. 38, no. 1, pp. 90–91, 2001.

[6] F. Sayda, "Involving LBS users in data acquisition and update," in *Proceedings of the AGILE 2005, Conference on geographic information science*, 2005.

[7] A. Gahran, "Reporting on the gulf oil spill from your cell phone," Jun. 2010, http://articles.cnn.com/2010-06-11/tech/oil.spil.app_1_cell-phones-apps-geotagged?_s=PM:TECH (last access 26 Mar. 2012).

[8] G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation enforcement schemes for MANETs: A survey," *Wirel. Commun. Mob. Comput.*, vol. 6, no. 3, pp. 319–332, 2006.

[9] H. Rifà-Pous, "Securing Ad Hoc Networks. Mechanism and Techniques," Ph.D. dissertation, Universitat Politècnica de Catalunya, Barcelona, Jun. 2008.

[10] D. Lambert, "Measures of disclosure risk and harm," *Journal of Official Statistics*.

[11] R. Shokri, J. Freudiger, and J. P. Hubaux, "A unified framework for location privacy," in *Proceedings of the 9th International Symposium on Privacy Enhancing Technologies (PETS'10)*, 2010, pp. 203–214.

[12] R. Shokri, G. Theodorakopoulos, J. Le Boudec, and J. Hubaux, "Quantifying location privacy," in *Security and Privacy (SP), 2011 IEEE Symposium on*, may 2011, pp. 247 –262.

[13] D. Freni, C. Ruiz Vicente, S. Mascetti, C. Bettini, and C. S. Jensen, "Preserving location and absence privacy in geo-social networks," in *Proceedings of the 19th ACM international conference on Information and knowledge management*, ser. CIKM '10. New York, NY, USA: ACM, 2010, pp. 309–318.

[14] "Please rob me." [Online]. Available: http://pleaserobme.com

[15] C. Ruiz Vicente, D. Freni, C. Bettini, and C. S. Jensen, "Location-related privacy in geo-social networks," *IEEE Internet Computing*, vol. 15, no. 3, pp. 20–27, May 2011.

[16] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in *Proceedings of the 7th International Conference on Pervasive Computing*, ser. Pervasive '09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 390–397.

[17] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Enhancing security and privacy in traffic-monitoring systems," *Pervasive Computing, IEEE*, vol. 5, no. 4, pp. 38 –46, oct.-dec. 2006.

[18] J. Krumm, "Inference attacks on location tracks," in *Proceedings of the 5th international conference on Pervasive computing*, ser. PERVASIVE'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 127–143.

[19] Y. De Mulder, G. Danezis, L. Batina, and B. Preneel, "Identification via location-profiling in gsm networks," in *Proceedings of the 7th ACM workshop on Privacy in the electronic society*, ser. WPES '08. New York, NY, USA: ACM, 2008, pp. 23–32.

[20] E. Toch, Y. Wang, and L. F. Cranor, "Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems," *User Modeling and User-Adapted Interaction*, vol. 22, no. 1, pp. 203–220, Apr. 2012.

[21] N. F. Awad and M. S. Krishnan, "The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization," *MIS Quarterly*, vol. 30, no. 1, pp. pp. 13–28, 2006.