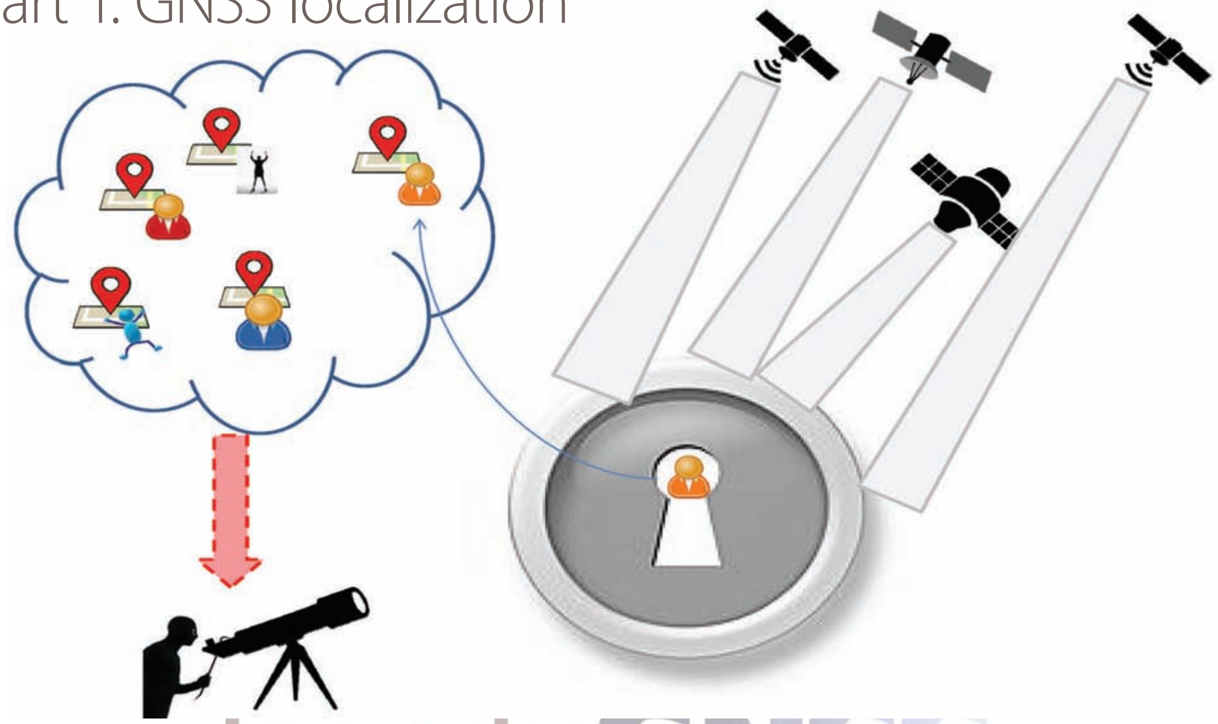
# Location Privacy Challenges and Solutions

## Part 1: GNSS localization



A key vulnerability of Location Based Services is location privacy. Geo-located patterns can lead to the re-identification of individuals and thus risk their right to a private life. This article presents an overview of the location privacy challenges in indoor and outdoor localization and tracking with various wireless technologies. It discusses users' perceptions about the privacy of location information and presents state-of-the-art technical solutions to deal with location privacy in modern GNSS localization technologies. A second article, to be published in the November/December issue of ***Inside GNSS***, will focus on similar issues in non-GNSS localization techniques.

**ELENA SIMONA LOHAN**
TAMPERE UNIVERSITY OF TECHNOLOGY

**PHILIPP RICHTER**
TAMPERE UNIVERSITY OF TECHNOLOGY

**VICENTE LUCAS-SABOLA**
UNIVERSITAT AUTONOMA DE BARCELONA

**JOSÉ A. LÓPEZ-SALCEDO**
UNIVERSITAT AUTONOMA DE BARCELONA

**GONZALO SECO-GRANADOS**
UNIVERSITAT AUTONOMA DE BARCELONA

**HELENA LEPPÄKOSKI**
TAMPERE UNIVERSITY OF TECHNOLOGY

**ELENA SERNA SANTIAGO**
TAMPERE UNIVERSITY OF TECHNOLOGY

Positioning (or localization) is a key component in many wireless devices and a key enabler and optimizer of many mobile applications, including transportation, smart cities, and ambient assisted living. For example, mobile wireless devices relying on a location component can be used as mobile assistants and wearable devices for the elderly, sick, or disabled, for traffic and environment monitoring, for green mobile crowd sensing, in crisis scenarios, for wildfire risk prediction, etc. (see I. Maglogiannis *et alia* and L. Skorin-Kapov *et alia* in Additional Resources). When the time dimension is added to the positioning information, we talk about user or device tracking.

To enable a large-scale uptake of the location-based and location-aware applications, one of the main barriers to overcome is finding solutions to the current vulnerabilities in wireless positioning. Such vulnerabilities exist with respect to the privacy, security, positioning reliability, robustness, and availability, especially in indoor environments, and to the acceptability and safety of tracking devices. Users are indeed, slowly, becoming aware of the potential vulnerabilities in making their minute-by-minute position known to the external world and legislation efforts all over the world are dedicated to build the legal frameworks covering tracking and location privacy (see L. Chen *et alia* and K. Pomfret). Operators and mobile manufacturers are collecting location-based data and possibly geo-tagged context information en masse from our mobile devices for the purpose of network and service optimization. Crowdsourcing, mobility sensing, and cloud storage processing are becoming default options. Many mobile devices can now be used as identifiers, and digital wallets and biometric data play a crucial role. Location is a key component in all of these aspects. A known location, or being able to fake a current location, could mean, in the near future, higher vulnerability to theft, privacy invasion, and increased stalking. Geo-located patterns can lead to the re-identification of individuals and thus could pose a risk to the right to a private life. All these vulnerabilities with respect to the acquisition, storage, and misuse of the users' geospatial information are long-overlooked factors which need to be addressed in a systematic and dedicated manner. The promising potential of future prosperous wireless markets relying on some form of localization and geo-spatial information, such as Internet of Things (IoT), Industrial IoT (IIoT), 5G, Device-to-Device (D2D), or Vehicle-to-Anything (V2X) communications, means that the security, privacy, and transparency aspects in mobile positioning need to become a high priority in the world of mobile computing.

In traditional positioning approaches, such as those purely based on Global Navigation Satellite Systems (GNSS), the user device is a purely passive device, thus fully preserving the user's privacy. Modern localization solutions, including those evolved from GNSS such as Cloud GNSS (C-GNSS) and Assisted GNSS (A-GNSS) involve smart processing of cloud-gathered data, inter-connectivity, and exchange of information between different stakeholders in the localization chain, and possibly geo-tagged content de-identification. Therefore, these are vulnerable to privacy breaches, whereas the user position is fully private in GNSS as its receiver acts only as a passive (receiving) device. This article sheds light on the challenges related to location privacy, emphasizing current user perception of location-based mobile applications, and discusses future research directions and solutions that can benefit the community at large.

## Is Location Privacy Something We Should Worry About?

In order to better understand users' concerns with regard to their location privacy and how much users would be willing to pay for preserving their location privacy, a Webropol web survey (see Additional Resources) was conducted from January to May 2017. The survey was initially built in English and then translated to Finnish and Romanian. The survey link was distributed on different social media channels (e.g., LinkedIn, Twitter, Facebook) and through various mailing lists in order to reach a wide audience with variable backgrounds. In total, 327 answers from respondents across 38 countries in four continents were obtained. 8.8% of the respondents did not answer the question about the country of residence. There were 208 answers in English, 79 in Finnish, and 40 in Romanian. The overall gender distribution is quite balanced: 46.3% male respondents, 49.4% female respondents, and 4.3% declined to state. The age and country distribution of respondents are shown in Figure 1, with Finland, Romania, and UK being the countries of residence for most of the respondents, and the majority of respondents being between 36 and 45 years old.

Figure 2 shows how the respondents

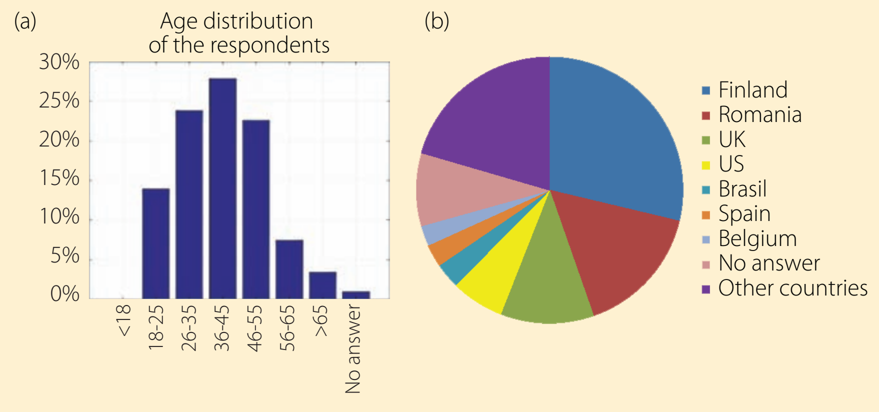


FIGURE 1 a) Distribution of respondents per age group; b) Distribution of respondents per country. For clarity reasons, only the top 7 countries are shown (in terms of number of respondents).

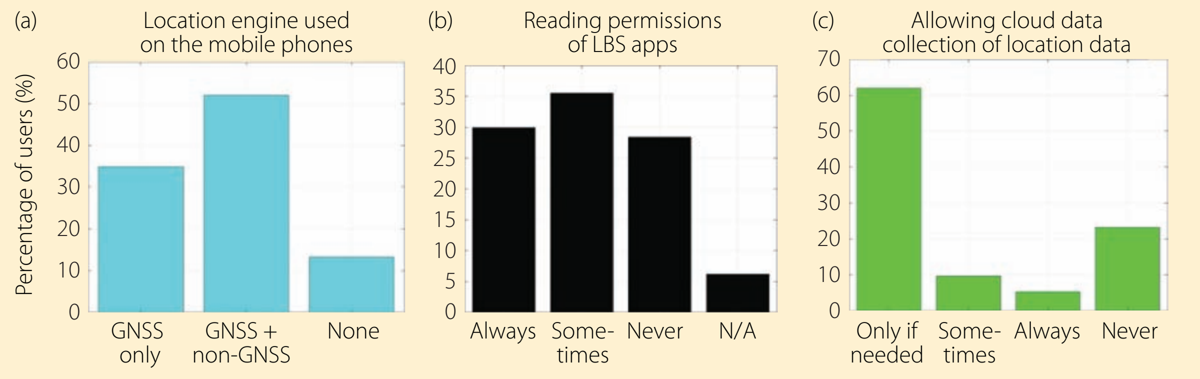


FIGURE 2 Survey results in terms of: a) typically used location engine (if any) on the mobile device; b) how often the users are reading the permissions when installing a new location-based app on their mobile; c) how often the users allow the location-based app to collect their location data and send it to a cloud server.

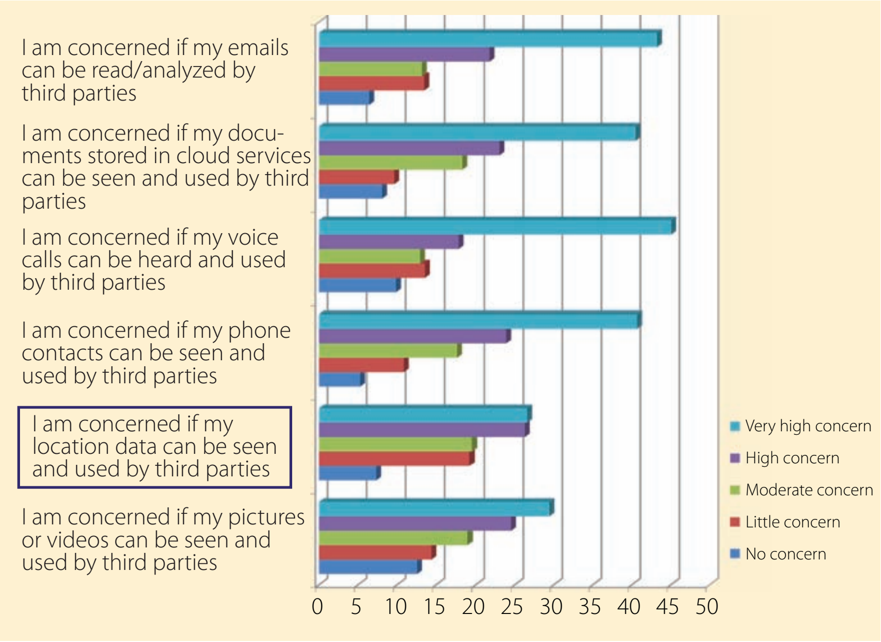


FIGURE 3 User's concerns with respect to their location privacy in comparison with privacy of other data types.

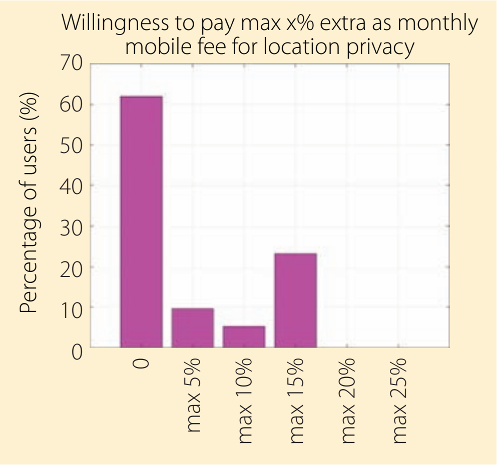


FIGURE 4 Willingness to pay for location privacy

are using their mobile phone's navigation capabilities and Location Based Services (LBS) on their mobile devices. The left plot shows that the vast majority of users (86.6%) are using some form of navigation on their phone, among which 52% typically activate both the GNSS and the non-GNSS (e.g., WiFi and cellular) positioning engines on their phones when navigating. The center plot of Figure 2 describes how often a user reads the permissions before installing an LBS application on his/her phones. These permissions are more or less intrusive in terms of privacy, depending on the application provider and reading them already denotes some minimal concern with regard to the privacy of mobile data. The survey shows that 30.0% of the respondents always read the permissions, 35.49% only occasionally read the permissions, and 28.4% never read the permissions. A small amount of respondents (6.2%) did not know about these permissions.

The right plot of Figure 2 shows how many of the respondents allow the LBS provider to collect their location data. The vast majority of respondents (61.9%) allow their location information to be collected only if they cannot use a particular service otherwise, as is the case with many LBS providers, such as Google maps and HERE maps. 5.2% of respondents always allow the location application to collect the user location data and 9.6% of respondents allow the location application to collect such data from time to time, independently of whether or not the LBS application could have been used in "private" mode (i.e., no data collection). 23% of respondents answered that they had never allowed an application to collect their location data. However, one could also infer that it might be unclear for some users whether or not a certain LBS application collects location data and sends it to the cloud. This comes as a conclusion when comparing the left plot of Figure 2, where only 13.6% of the respondents wrote that they do not use any location engine on their phone, with the right plot of Figure 2, where 23% of respondents say that they never allow an application to collect their location data. Nevertheless, one has to keep in mind that the vast majority of current LBS mobile applications cannot run unless the user allows the application to collect his/her location data.

Figure 3 compares the level of concern of users with respect to their location privacy with other types of personal digital data, such as emails, documents, calls, phone contacts, or images/videos. If we look at the "Very high concern" bars, clearly the users are much more concerned with protecting the privacy of all other types of personal digital data than protecting the location privacy. However, "High" and "Moderate" concerns bars are rather similar for different types of data, which shows that users have significant concerns regarding the privacy of all their personal data, location data included. As for the "No concern" bars, privacy of pictures and videos are least worrisome to those in the survey, with 12.6% having no concern for the privacy of these items. For location privacy, 7.3% had no concern, 14.4% had little concern, 19% moderate concern, 24.5% high concern, and 29.4% very high concern.

How these concerns translate also in a willingness to pay extra for location privacy can be seen in Figure 4. Clearly, the vast majority of users (61.9%) are not yet ready to pay anything extra for a privacy-preserving location engine. It is interesting to see that, among those who are interested in paying something (23.2% of the total respondents), the majority (60.9% of the respondents willing to pay something) would opt to pay up to 15% more compared to their current monthly mobile fee, and no respondent opted to pay more than 20% of the current monthly fee.

The survey findings show that there is already a reasonable awareness about location privacy challenges and that such awareness could be capitalized upon to

| Location granularity | Possible attacks | Description of attacks | Useful LBS applications |
|---|---|---|---|
| Hundreds of km (town- or country-level granularity) | House burglary<br>Car theft | An attacker able to know when a family is on holiday or far from home (e.g., in another town or country) can try a house burglary or a car theft. | Location-based weather forecasts |
| Few tens of km (district-level granularity) | Stalking<br>Unwanted advertising and location-based scams | A stalker can get important information about the social habits, hobbies, social network, and relationships and living habits of someone, just by knowing his/her approximate location for a certain duration in time (e.g., a few weeks or months). | Location-based district-level advertising (e.g., shows, museums, etc.)<br>Location-based socializing and chatting |
| Few tens of meters (block-level or building-level granularity) | Unauthorized use of tolled highways<br>Attacks of crowded regions of people<br>Disclosure of unwanted personal information<br>Loss of social reputation | An attacker able to steal the location identity of another user can freely ride the automatic toll highways, as the bill would be sent to another user. Also, an attacker able to access the location information from many mobile devices simultaneously can easily create a 'heat map' of the most crowded regions in a city at any point of a day and can enable various attacks upon crowded areas. Knowing someone's location with building-level granularity can also lead to public disclosure of unwanted information, such as how often an employee who is supposed to work is taking coffee breaks, how often a husband is visiting other places than those he informed the wife about, or the religious and political affiliations of a person (based on the gatherings and places he/she is attending), etc. (M. Li *et alia*). In extreme cases, an eavesdropper which finds out private personal information based on location patterns can also resort to blackmailing and produce economical losses and/or social reputation losses. | Automatic tolls<br>Coarse tourist guidance<br>Social marketing<br>Find your friend<br>Public transportation information<br>Town surveillance applications<br>Geofencing |
| Few meters (room-level granularity) | Enabling identity thefts | Location information leakage can help in identify theft attacks, as shown by S. Mascetti *et alia*. | Accurate tourist guidance<br>E-health solutions<br>Proximity-based offers/ rewards/vouchers<br>Gaming and gamification<br>Social networking<br>Emergency services and alerts<br>Home surveillance |
| Few centimeters (professional GNSS and 5G-level granularity) | Decreased traffic safety in unmanned and automated vehicle applications | An adversary who is eavesdropping on the location of a smart vehicle can act in such a way to decrease the driving vehicle's safety and provoke collisions and accidents as shown by D. Henrici and P. Muller (Additional Resources). | Automatic driving<br>Navigation aids for the visually impaired<br>Item tracking |

**Table 1** Examples of possible attacks, according to the granularity of knowing the user location.

some extent in business, by offering users more privacy-aware location solutions. The next sections will focus first on some aspects regarding granularity of location estimation, and then on GNSS location technologies categories, and will point out if and how such technologies can better support location privacy.

## Granularity of Location Estimates for Various LBS

When talking about location privacy, one refers to the capacity of preventing any third parties to learn anything about a device location in space and time. There is thus a quadruplet $(x, y, z, t)$ characterizing the location, where $x, y, z$ are the spatial coordinates of the mobile device and $t$ is the time at which that location is valid. When time is also known, we often talk about the user or device tracking.

There are two ways of defining the granularity of a location estimate: one is from the point of view of an attacker and it refers to the accuracy level at which the attacker can detect the location information; the other is from the user's point of view, and it refers to the Quality of Service (QoS) received from a Location Service Provider (LSP), knowing that there is an inherent tradeoff between preserving his/her own location privacy via, for example, some cloaking or obfuscation mechanisms, and the QoS of the LBS. For example, let's assume that the user's true position at time $t$ is $(x, y, z)$, but the location information sent to the LBS and/or accessed by an attacker is $(x + \Delta x, y + \Delta y, z + \Delta z)$. Then, the location granularity $g$ in this case is defined as

$$g = \sqrt{\Delta x^2 + \Delta y^2 + \Delta z^2},$$

which is basically the distance uncertainty in the location estimate.

**Table 1** gives examples of how an attacker can make use of the user location, if the user location is known with a certain granularity. The last column also shows positive examples of how the location information of a certain granularity can serve the user. Typically, the location needs to be known at several moments in time, ranging from a few hours to several months, in order for an attacker to be able to act upon the knowledge, but sometimes even the knowledge of as little as four different locations in time can lead to personal identification (see De Montjoye *et alia* in Additional Resources). As shown in Table 1, while one may be completely unconcerned if his/her location is known within a kilometer of error, this might be enough for an attacker to establish if a family is away from their home and to organize a house burglary. The examples of attacks shown in all rows above the current row are also applicable to the current row. For example, if the location is known within a few tens of meters from the actual position, house burglary, car thefts, or stalking are also potential threats, in addition to terrorism or disclosures of unwanted personal information, which are enabled by a more precise location known to an attacker.

## Location Privacy in GNSS-Based Positioning

### Cloud GNSS

In the coming years, the development of new GNSS-based applications will play a leading role in the context of urban environments, i.e., Smart Cities, where almost every object or device such as urban furniture or wearable items can be connected between themselves, i.e., Machine to Machine (M2M) or D2D, and to the internet. In this sense, IoT applications have triggered the use of GNSS technologies for retrieving the Position, Velocity, and Timing (PVT) of the devices. Nevertheless, GNSS was designed for outdoor applications, and its performance gets truncated in urban working conditions. Moreover, IoT devices cannot implement advanced computational tasks due to constraints on low energy consumption, thus hindering the use of GNSS in harsh working conditions such as urban canyons, indoors, etc. Computational constraints are not only circumscribed to GNSS-based IoT devices, but also to conventional GNSS receivers providing advanced features such as multi-constellation processing, signal authentication, or threat detection (e.g., interference or propagation effects such as multipath or NLOS).

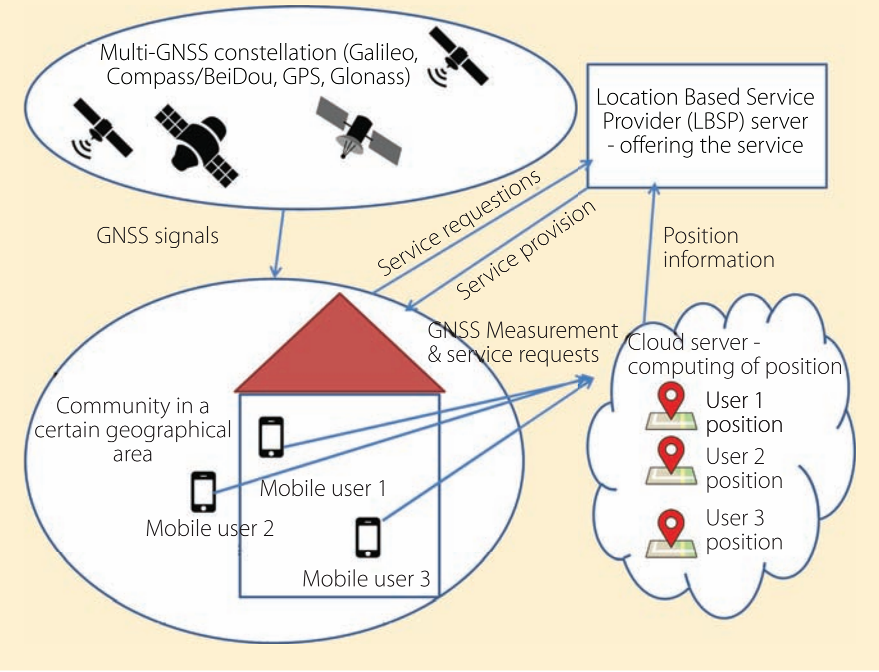

Multi-GNSS constellation (Galileo, Compass/BeiDou, GPS, Glonass)
Location Based Service Provider (LBSP) server - offering the service
GNSS signals
Service requestions
Service provision
Position information
GNSS Measurement & service requests
Cloud server - computing of position
User 1 position
User 2 position
User 3 position
Community in a certain geographical area
Mobile user 1
Mobile user 2
Mobile user 3

FIGURE 5 Cloud GNSS concept illustration.

To overcome this hurdle, the Cloud GNSS concept has recently been proposed as a disruptive approach for solving most of the current limitations of conventional GNSS receivers (see Additional Resources). In this paradigm, the GNSS signal processing tasks traditionally carried out in on-chip GNSS modules at the user terminal, are now relocated in a cloud server, as illustrated in Figure 5, where on-demand scalable computing capacity in terms of data storage and processing power is available. Thanks to this availability, the energy consumption and computational power required by the user terminal is significantly reduced, since its main function is now to gather raw GNSS samples and transfer them to the cloud. Thanks to the computing capacity provided by the cloud, sophisticated GNSS signal processing techniques can easily be performed, thus providing a wider range of use cases where the GNSS sensor can effectively operate. For instance, Cloud GNSS can be used in liability-critical and safety-critical applications, where the use of conventional GNSS receivers faces some limitations due to the stringent requirements imposed on the user terminal in terms of integrity, continuity and, in the future, authentication.

The transfer of information from the user terminal to the cloud may raise some concerns on the potential vulnerabilities of cloud GNSS signal processing in terms of privacy and security. From a high-level perspective, we can identify three different categories of vulnerabilities, explained below: i) at the user-to-cloud communication link; ii) on the cloud storage of personal digital data, such as identifiers or GNSS raw samples; iii) on the computation, and therefore knowledge, of users' location by third-parties, for example at the Location Based Service Provider (LBSP) side.

### User-to-Cloud Communication

During the transmission of raw GNSS samples from the user's device to the cloud server, personal data may eventually be intercepted by attackers. Location may also be known by the service provider of the network infrastructure due to the identifier each device holds, e.g., IP or MAC address or International Mobile Station Equipment Identity (IMEI). However, communication privacy and security is already provided by wireless infrastructures through secure communication protocols and standards, e.g., user access authentication implemented in Long Term Evolution (LTE) or Narrow Band Internet of Things (NB-IoT). Hence, the security and privacy of the user-to-cloud communication link is achieved with state-of-the-art wireless communication standards. Besides that, some cloud providers also offer secure platforms to connect users' devices with the cloud. For instance, Amazon Web Services (AWS) offers an IoT platform, which already provides traffic encryption over Transport Layer Security (TLS) by using different cryptography standards such as X.509 or the Signature Version 4 Signing Process (SigV4).

### Cloud Storage of Personal Digital Data

Customers may worry about the security involving the raw GNSS samples and personal digital data they upload to the cloud, due to the possibility of it being read or analyzed by third-parties (or attackers) and thus being used in an unauthorized manner. Nine critical threats to cloud security are identified by the Top Threats Working Group (Additional Resources): data breaches, data loss, account hijacking, insecure APIs (Application Program Interface), denial of service, malicious insiders, abuse of cloud services, insufficient due diligence, and shared technology issues. To prevent many of these threats, current cloud providers such as AWS, Microsoft Azure, and Google Cloud provide high-security systems with ISO 27001 certification, thus assuring confidentiality, integrity, and availability. With regard to the stored data, cloud platforms do not distinguish between personal data and any other type of data. Therefore, by using certified cloud platforms, the security of personal data, which in this case would be the raw GNSS samples file, the device location and any other stored personal data, would be guaranteed. Users shall realize that the security policies of a cloud service may change depending on the legislation of the country in which the cloud server is allocated, and hence personal digital data may be accessed by the government.

### User's Location Calculation by Third-Parties

Device anonymization is needed when the user's location is known to a third-party, either when the location is calculated by the cloud GNSS platform or when it is used by some LBS. If not, the cloud and the LBS server might know who the devices' owner is, and use the personal data and location for their own benefit. For LBS, a k-anonymization model to deal with location privacy is presented by B. Gedik and L. Liu. In this approach, an anonymity server decrypts the data transferred from the device to the LBS and removes all the related identifiers (e.g., IP or MAC address, device, or customer identifier). Next, the location information is disrupted by means of spatio-temporal cloaking (i.e., hiding the true location information in a wide spatio-temporal area), and finally, the anonymized location is sent to the LBS server. Note that this approach may perturb the quality of service, and thus a tradeoff between the QoS and location privacy is faced.

Another alternative is to assign a random identifier to every device, which is then changed after a fixed time such as minutes, hours, or days depending on the application, in order to facilitate the anonymization. In this context, hash-based ID variation (see Additional Resources) can be used for enhanced location privacy. This process is often accomplished through two different and independent entities, the first one (e.g., a certification body) being in charge of randomly assigning identifiers to users, and the second one (e.g., the LBSP) being in charge of the exploitation of the randomized data. This scheme guarantees that the entity making use of the data has no access to the mechanism whereby the identifier was generated and assigned to the user. In this manner, users have a time-varying identifier with limited lifetime that thus cannot be tracked for a long period of time. Clearly, the shorter the identifier lifetime, the better the user privacy, since we prevent inferral of user identification via behavior pattern analysis.

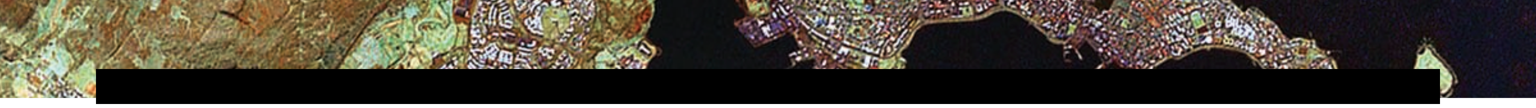
In conclusion, there are many protection schemes that can be used to solve the potential vulnerabilities of cloud GNSS positioning in terms of location security and privacy. When it comes to strengthening the privacy requirements of the user's location, this often translates into a tradeoff between privacy and QoS.

### Assisted GNSS

In order to position itself using the signals from navigation satellites, the GNSS receiver needs to know the precise time and orbital parameters to compute the positions of the satellites. The GNSS satellites broadcast this information in their navigation messages. However, decoding the orbital information from navigation messages takes 30 seconds in good signal conditions, which is a significant Time-To-First-Fix (TTFF), i.e., delay in the starting of positioning. This time may be much longer in environments dense with buildings or foliage where these obstacles attenuate the satellite signals. If the signal power decreases further, the receiver cannot decode the navigation data even if it is still able to make the ranging measurements. In this case, without information on satellite orbits and precise time, the measurements are useless for the receiver and it cannot compute its position.

In A-GNSS, the functionalities of a GNSS receiver are enhanced through terrestrial communication networks to shorten the TTFF and to improve the sensitivity of the receiver, i.e., to allow positioning with weaker satellite signals (J. Syrjäinne; F. Van Diggelen, Additional Resources). In A-GNSS, the missing information is provided to the receiver by a server that is connected to the receiver that has good visibility to the satellites (**Figure 6**). In addition to the orbital information and time, the A-GNSS can also deliver the Differential GNSS (DGNSS) corrections which allow improvements of positioning accuracy even to the one meter level.

Two architectures were proposed for A-GNSS where the roles of the user terminal (mobile station, MS) and the server in the network are different. In MS-based A-GNSS (MS-Based Network-Assisted) the user receives



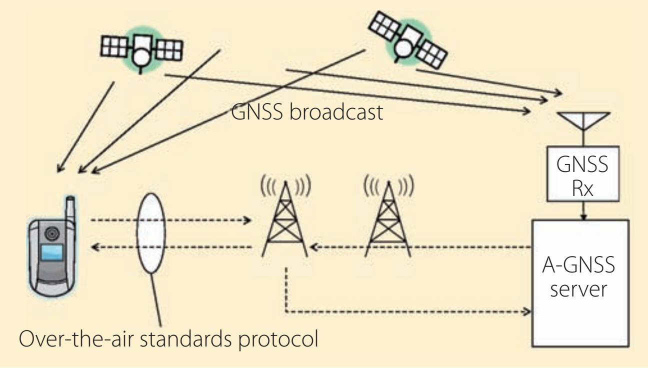


FIGURE 6 A-GNSS Diagram

assistance data from the server and makes the ranging measurements, possible DGNSS corrections, and positioning calculations by itself. In MS-assisted A-GNSS (MS-Assisted Network-Based) the user terminal makes the ranging measurements and sends them to the server. The server applies the possible DGNSS corrections to the measurements, computes the position, and sends it back to the user. To assist the user terminal in the positioning measurements, the server sends a small set of assistance data to the user to enable fast signal acquisition.

In MS-based A-GNSS, in good signal conditions the user terminal can also position itself without assistance from the server. That is to say, the network connection is not necessary. In MS-assisted A-GNSS, the positioning of the user terminal always requires two-way communication with the server. The best achievable accuracy in both A-GNSS modes is defined by the DGNSS, which allows accuracies on the level of one meter (see Additional Resources). However, both modes are susceptible to multipath and NLOS, and therefore the accuracy is not always as good as in clear LOS. Actually, in an MS-based approach, the positioning accuracy may deteriorate to hundreds of meters when assistance is needed due to bad signal conditions. When the satellite signal levels drop very low, e.g., in underground settings, the user devices also cannot make the measurements, and both A-GNSS modes fail.

While both MS-based and MS-assisted architectures require point-to-point communication, either in the control plane of a cellular network or in the user plane of a wireless internet, only in MS-assisted approach does the user terminal reveal its accurate position to the server. The functionalities of the current Cloud GNSS are very similar to MS-assisted A-GNSS, therefore the privacy threats are also similar. For A-GNSS, secure architectures exist (L. Wirola et alia), e.g., the Open Mobile Alliance Secure User Plane Location Protocol (OMA SUPL) which provides security and authentication services using Generic Bootstrapping Architecture (3GPP GBA) (please see Additional Resources).

## Conclusions

Our studies shed more light on users' perception of their location privacy and on the privacy threats and solutions in modern wireless localization. We learned that, in general, users are not yet particularly aware of location privacy threats and most would not be willing to pay much or anything for private or passive positioning. In addition, privacy of localization is not yet fully solved in many state-of-the-art GNSS localization systems, such as Cloud GNSS and Assisted GNSS.

## Acknowledgements

The authors express their warm thanks to the Academy of Finland (Project 303576) for its financial support for this research work.

## Additional Resources

[1] 3GPP TS 33.220 Generic Bootstrap Architecture, http://www.3gpp.org

[2] Chen, L., Thombre, S., Järvinen, K., Lohan, E. S., Korpisaari, P., Kuusniemi, H., Leppäkoski, H., Honkala, S. , Bhuiyan, M. Z. H., Ruotsalainen, L., Ferrara, G. N., Bu-Pasha, S., "Robustness, Security, and Privacy in Location-Based Services for Future IoT," *IEEE Access,* Vol. 5, pp. 8956-8977, 2017

[3] De Montjoye, Y. A. , Hidalgo, C. A., Verleysen, M., and Blondel., V. D., "Unique in the Crowd: The Privacy Bounds of Human Mobility," *Scientific Reports 3,* Article number: 1376, 2013

[4] Gedik, B. and Liu, L., "Location Privacy in Mobile Systems: A Personalized Anonymization Model," *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems, ICDCS,* pp. 620-629, June 2005

[5] Gschwandtner, F. and Schindhelm, C. K., *Spontaneous Privacy-Friendly Indoor Positioning using Enhanced WLAN Beacons,* 2011

[6] Henrici, D. and Muller, P., "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers," *Proceedings of the 2nd IEEE Annual Conference in Pervasive Computing and Communications Workshops,* pp. 149-153, March 2004

[7] Li, M., Zhu, H., Gao, Z., Chen, S., Ren, K., Yu, L., and Hu, S., "All Your Location are Belong to Us: Breaking Mobile Social Networks for Automated User Location Tracking," *Proceedings of MobiHoc, ACM,* pp. 43-52 2014

[8] Lucas-Sabola, V., Seco-Granados, G., López-Salcedo, J. A., García-Molina, J. A., and Crisci, M., "Cloud GNSS Receivers: New Advanced Applications Made Possible," *Proceedings of the International Conference in Localization and GNSS (ICL-GNSS),* pp. 1-6, June 2016

[9] Maglogiannis, I., Kazatzopoulos, L., Delakouridis, K., and Hadjiefthymiades, S., "Enabling Location Privacy and Medical Data Encryption in Patient Telemonitoring Systems," *IEEE Transactions on Information Technology in Biomedicine,* Vol. 13, No. 6, pp. 946-954, November 2009

[10] Mascetti, S., Bertolaja, L., and Bettini, C., "A Practical Location Privacy Attack in Proximity Services," *2013 IEEE 14th International Conference on Mobile Data Management,* Milan, pp. 87-96, 2013

[11] Misra, P. and Enge, P., *Global Positioning System - Signals, Measurement and Performance, 2nd ed.,* Ganga-Jamuna Press, ISBN 0-9709544-1-7, 2006

[12] OMA Secure User Plane Location 1.0, OMA-ERP-SUPL-V1_0-20070615-, http://www.openmobilealliance.org

[13] Pomfret, K., "Geolocation Privacy – Implications of Evolving Expectations in the United States," *Inside GNSS,* September/October 2016

[14] Skorin-Kapov, L., Pripužić,K., Marjanović, M., Antonić, A., and Žarko, I. P., "nergy Efficient and Quality-Driven Continuous Sensor Management for Mobile IoT Applications," *10th IEEE International Conference on Collaborative Computing: Networking, Applications, and Worksharing,* Miami, FL, pp. 397-406, 2014

[15] Syrjärinne, J., *Studies of Modern Techniques for Personal Positioning,* Ph.D. Dissertation, Tampere University of Technology, 2001

[16] Top Threats Working Group, *The Notorious Nine: Cloud Computing Top Threats in 2013,* Cloud Security Alliance, 2013

[17] Van Diggelen, F., *A-GPS : Assisted GPS, GNSS, and SBAS,* Artech House, 2009

[18] Webropol web survey tool, http://w3.webropol.com/start/

[19] Wirola, L., Laine, T. A., and Syrjärinne, J., "Mass-Market Requirements for Indoor Positioning and Indoor Navigation," *Proceedings of the International Conference on Indoor Positioning and Indoor Navigation (IPIN),* Zürich, Switzerland, 2010

## Authors

**Elena Simona Lohan** received an M.Sc. degree in Electrical Engineering from Polytechnics University of Bucharest, Romania, in 1997, a D.E.A. degree (French equivalent of master) in Econometrics, at Ecole Polytechnique, Paris, France, in 1998, and a Ph.D. degree in Telecommunications from Tampere University of Technology (TUT), Finland, in 2003. Dr. Lohan is now an Associate Prof. at the Laboratory of Electronics and Communication Engineering (ELT) at TUT and a Visiting Professor at Universitat Autonoma de Barcelona. She is leading a research group on Signal processing for wireless positioning. She is a co-editor of the first book on Galileo satellite system (Springer "Galileo Positioning Technology"), co-editor of the 2017 Springer book on "Multi-technology Positioning", and author or co-author in more than 160 international peer-reviewed publications. Her current research interests include wireless location techniques, Location Based Services and privacy-aware positioning solutions.

**Philipp Richter** holds a doctoral degree in telecommunications and works currently as a post-doctoral researcher in the Wireless Communication and Positioning group at the Tampere University of Technology. Before, he was a research associate at the Fraunhofer Institute for Integrated Circuits IIS from 2009-2012. His main research interests are in signal processing, Bayesian inference and machine learning applied to robust multi-sensor data fusion, positioning and tracking.

**Vicente Lucas-Sabola** was born in Barcelona, Spain, in 1990. He received the B.Sc. in telecommunication systems engineering in 2015 and the M.Sc. in telecommunication engineering in 2017, both from Universitat Autonoma de Barcelona (UAB). Since 2015 he is involved in the development of a Cloud GNSS receiver, a project funded by the European Space Agency (ESA). Since 2017 he is pursuing the PhD at the SPCOMNAV group, dealing with topics related to Cloud GNSS signal processing for Internet of Things (IoT) applications.

**Prof. Jose Lopez-Salcedo** received the Ph.D. degree in Telecommunications Engineering from Universitat Politecnica de Catalunya (UPC), Barcelona, Spain, in 2007. He is Associate Professor at the Department of Telecommunications and Systems Engineering, Universitat Autonoma de Barcelona (UAB), where he is also the Coordinator of the telecommunication engineering studies. Jose Salcedo has been involved in more than 30 research projects for private industry and public administrations on topics related to signal processing, wireless communications and global navigation satellite systems (GNSS). He has held several visiting appointments at the University of California Irvine, the Coordinated Science Laboratory, University of Illinois at Champaign-Urbana and the European Commission, Joint Research Centre in Ispra, Italy. His research interests lie in the field of signal processing for communications and navigation, with emphasis on cloud and IoT GNSS signal processing and the convergence of 5G/GNSS systems.

**Gonzalo Seco-Granados** received a Ph.D. degree in telecommunications engineering from Universidad Politècnica de Catalunya and an MBA from IESE, the graduate business school of the University of Navarra. From 2002 to 2005,

he was with the European Space Agency, Netherlands. Since 2006, he has been an associate professor at the Universidad Autònoma de Barcelona, where he coordinates the SPCOMNAV (Signal Processing for Communications and Navigation) group. His research interests include signal-processing techniques for advanced features of GNSS receivers and localization using next-generation wireless communications networks.

**Helena Leppäkoski** received the M.Sc. and Ph.D. degrees from the Tampere University of Technology (TUT), Tampere, Finland, in 1990 and 2015, respectively. She was with Metso Corporation, Helsinki, Finland, from 1990 to 2000. She joined TUT in 2000, where she is currently a Post-Doctoral Researcher. Her research topics have varied from satellite positioning to various methods for pedestrian indoor positioning and machine learning for location related context inference. She is currently involved in a project on information security of location estimation and navigation applications.

**Elena Serna Santiago** was born in Toledo, Spain, on October 23, 1993. She received the B.Sc. degree in Telecommunication Systems Engineering from Polytechnic University of Madrid, Spain, in 2015, and the Master of Engineering degree in Telecommunication Systems from Polytechnic University of Madrid, Spain, in 2017. She worked with Department of Electronics and Communications Engineering of Tampere University of Technology to develop her Master's Thesis in 2017 during her Erasmus programme. Her research interests are in Global Navigation Satellite Systems (GNSS), mobile positioning, radar systems, signal processing and communications engineering.

**Em. Univ.-Prof. Dr.-Ing. habil. Dr. h.c. Guenter W. Hein** is Professor Emeritus of Excellence at the University FAF Munich. He was ESA Head of EGNOS & GNSS Evolution Programme Dept. between 2008 and 2014, in charge of development of the 2nd generation of EGNOS and Galileo. Prof. Hein is still organising the ESA/JRC International Summerschool on GNSS. He is the founder of the annual Munich Satellite Navigation Summit. Prof. Hein has more than 300 scientific and technical papers published, carried out more than 200 research projects and educated more than 70 Ph. D.´s. He received 2002 the prestigious Johannes Kepler Award for *"sustained and significant contributions to satellite navigation"* of the US Institute of Navigation, the highest worldwide award in navigation given only to one individual each year. G. Hein became 2011 a Fellow of the US ION. The Technical University of Prague honoured his achievements in satellite navigation with a *Doctor honoris causa* in Jan. 2013. He is a member of the Executive Board of Munich Aerospace since 2016. IG