INFORMATION SECURITY OF LOCATION ESTIMATION – INCREASING TRUSTWORTHINESS

Heidi Kuusniemi(1), Elena Simona Lohan(2), Kimmo Järvinen(4), Päivi Korpisaari(3), Sarang Thombre(1), M.H. Zahidul Bhuiyan(1), Helena Leppäkoski(2), Liang Chen(1), Shakila Bu-Pasha(3), Anette Alen-Savikko(3), Jenna Mäkinen(3), Laura Ruotsalainen(1), Stefan Söderholm(1), Robert Guinness(1), Giorgia Nunzia Ferrara(1), Salomon Honkala(1)

(1)Finnish Geospatial Research Institute, Geodeetinrinne 2, FIN-02430 Kirkkonummi, Finland
Email:{heidi.kuusniemi, sarang.thombre, zahidul.bhuiyan, liang.chen, laura.ruotsalainen, stefan.soderholm
robert.guinness, giorgia.ferrara, salomon.honkala}@nls.fi

(2)Tampere University of Technology, Korkeakoulunkatu 3, FIN-33720 Tampere, Finland
Email: {elena-simona.lohan, helena.leppakoski}@tut.fi

(3)University of Helsinki, P.O. Box 4 (Yliopistonkatu 3, 00014 University of Helsinki
Email: {paivi.korpisaari, shakila.bu-pasha, anette.alen, jenna.makinen}@helsinki.fi

(4)Aalto University, Otakaari 1, FIN-02100 Espoo, Finland
Email: {kimmo.jarvinen}@aalto.fi

ABSTRACT

Vulnerabilities of GNSS (Global Navigation Satellite Systems) or non-GNSS based localization include (1) unintended disruptions of the position or timing solution, (2) malicious attack on the physical or virtual infrastructure of the localization engine, (3) theft of information from the localization engine or its associated modules, and (4) loopholes in the policy framework supporting the legal creation and exploitation of location-based applications jeopardizing the privacy of the individual. This paper gives a brief overview to the state-of-the-art in vulnerabilities in localization, including in its technology, security, robustness, privacy, and policy aspects. It discusses the requirements for enhancing the trustworthiness of localization as to overcome a majority of the vulnerabilities. The paper addresses in particular the question of what are the constraints of ensuring continuous logistics of a localization solution and potential solutions. Thus, this paper presents firstly a brief state-of-the-art analysis of vulnerabilities in localization and then focuses on the requirements for enhancing the trustworthiness.

INTRODUCTION

Positioning and navigation technologies include satellite-based systems, i.e. Global Navigation Satellite Systems (GNSS), as well as non-GNSS techniques for determining the position of a person or an object of interest. Many navigation systems are also capable of providing precision timing. Such systems are increasingly being used in safety- and/or security-critical applications such as aviation, autonomous vehicles, and emergency services, as well as synchronization within communication systems, financial infrastructures, power grids, etc. This makes navigation technologies not only an obvious target for malicious attacks but also a critical point-of-failure in case of unintentional disruption. The growth in vulnerabilities has far outpaced the spread in public and authorities' awareness, as well as development of mitigation techniques.

Virtually every segment of society and industry would be negatively impacted, if positioning systems, such as the Global Positioning System (GPS) or the European Galileo, were to face widespread disruptions. The segments of society that would be affected include: emergency services, civil protection authorities, the financial industry including stock markets, transportation (including road transport, maritime, aviation, and rail), communications, power distribution, and logistics, just to name a few areas. What many people fail to realize is that GNSSs provide not only positioning services but also precision timing services. While both are critically important in modern society, the importance of timing services to critical infrastructures, such as power distribution systems, is even more severely overlooked. Furthermore, threats to the security and reliability of navigation systems are not limited to GNSS technologies alone. Alternative positioning systems based on cellular signals, WiFi signals, or other radio-frequency signals, as well as peripheral technologies, are subject to various vulnerabilities, such as database attacks, false emitters, or mal-use of individual Medium Access Control (MAC) addresses. In many cases, a location information service provider or location aggregator [1] collects user data for the positioning purpose and also maintains various location databases used for location estimation. This exchange of information between actors introduces many potential privacy and security vulnerabilities. Moreover, these vulnerabilities should not be addressed only from a technological perspective. In many cases, legislation surrounding these issues is not keeping pace with the advances of technology, resulting in inadequate legal protections. Lastly, the security of location information should be considered not just on a macroscopic societal scale but also on a personal level. The rising use of disruptive devices such as personal privacy devices (PPD) is rooted in the increased concerns over personal privacy regarding location tracking technology. The threat of unwanted interception of location information impacts the personal safety of individuals, and there are many reported criminal cases where location information has either been maliciously intercepted or unintentionally revealed.

This paper originates from a research project named INSURE (Information Security of Location Estimation and Navigation Applications) and is organized as follows: first, the layers of information security in location estimation are presented. Secondly, a short review of vulnerabilities in localization is introduced followed by discussion on the requirements for enhancing the trustworthiness. Finally, potential countermeasures are addressed to improve the robustness of location estimation and its overall information security in all domains with identifying steps to be taken.

LAYERS OF INFORMATION SECURITY

Apart from a small cadre of experts, few people have given serious consideration to the effects that would be posed to society if positioning systems, such as the GPS or Galileo, were to face widespread disruptions. Such threats are not a matter of mere possibility or imagination. They have already surfaced on many occasions, although the impacts have thus far been mostly local in nature. For example, during 2009 and 2010 the US Federal Aviation Administration (FAA) attempted to deploy a GPS augmentation system at Newark International Airport that would allow GPS-based precision landings. However, repeated episodes of intentional jamming of the GPS signals caused extensive delays of the testing and commissioning of this system. Although it took months to identify the source of the radio-frequency interference, ultimately it was traced to the use of so-called "personal privacy devices" (PPD) on a nearby highway, which jam the GPS frequencies and render nearby GPS receivers useless [2].

The motivation for using such devices can range from relatively benign (avoiding tracking of employees) to extremely malicious. For example, GPS jammers have been used by criminals in many robberies of vehicles to render automatic alarm systems useless [3]. Also location information from the mobile phones has been used by malicious apps to launch location-based attacks or malware [4] or to build an accurate profile of the user and thus expose him/her to possible identify thefts or other attacks [5].

As mentioned above, threats to the security and reliability of navigation systems are not limited to GNSS technologies alone. Alternative positioning systems based on cellular signals, WiFi signals, or other radio-frequency signals, as well as peripheral technologies, are subject to various vulnerabilities, as outlined in Figure 1, which illustrates the main actors involved in localization. These include the Location Information Service (LIS) provider, the LBS (Location Based Service) provider and the end-user. The LIS offers the actual technology to position the user. In many cases, it collects user data for the positioning purpose, and it also maintains various location databases used for location estimation. This exchange of information between actors introduces many potential privacy and security vulnerabilities.

Lastly, the security of location information should be considered not just on a macroscopic societal scale but also on a personal level. The rising use of disruptive devices such as PPD is rooted in the increased concerns over personal privacy regarding location tracking technology. The threat of unwanted interception of location information impacts the personal safety of individuals, and there are many reported criminal cases where location information has either been maliciously intercepted or unintentionally revealed [6].

Trustworthy localization implies that the application using these technologies can rely on a steady, uninterrupted, and uncompromised flow of positioning (or timing) information for as long as the application is operational. At the innermost core of different layers of requirements for trusted navigation and localization systems are the requirements of a robust electronics and communication system, including the localization engine, sensor modules, and antennae, etc. Next layer consists of requirements of cyber-security of the information highway, including data, network busses, databases, user- and internet-interfaces, etc. The third layer includes requirements for pre-empting vulnerabilities in the local environment, for example, presence of spoofing, jamming, multipath, and unavailability of GNSS signals (due to urban canyon, foliage, or moving indoors), etc. The fourth layer presents requirements with regards to the vulnerabilities of the positioning infrastructure; including the GNSS signal structure, WiFi access points, and cameras (in case of visual-aided infrastructure-less positioning), etc. The fifth and outermost layer deals with requirements to overcome the vulnerabilities in the legal framework. While the requirements of the innermost layer are well-documented and form a significant part of any positioning solution hardware, the requirements from the rest of the layers are typically less discussed. Figure 2 depicts the layers identified.

Although the security threats associated with location technologies are not widely known to the general public, there are several groups researching these topics internationally. For example, researchers from the University of Texas demonstrated how easily the satellite navigation signals used at sea can be spoofed to disorient a ship's navigation system and force the auto-pilot to change course [7]. The US Department of Homeland Security has been investing heavily in research and development to detect and mitigate GPS jamming [8]. Similarly in Europe, especially the UK, authorities have strongly invested in interference monitoring initiatives through, for example the GAARDIAN [9] and SENTINEL [10] projects. The STRIKE3 EU H2020 project [11] is on the other hand a new initiative aiming at standardising the systems, processes and interfaces for GNSS interference reporting and receiver testing.

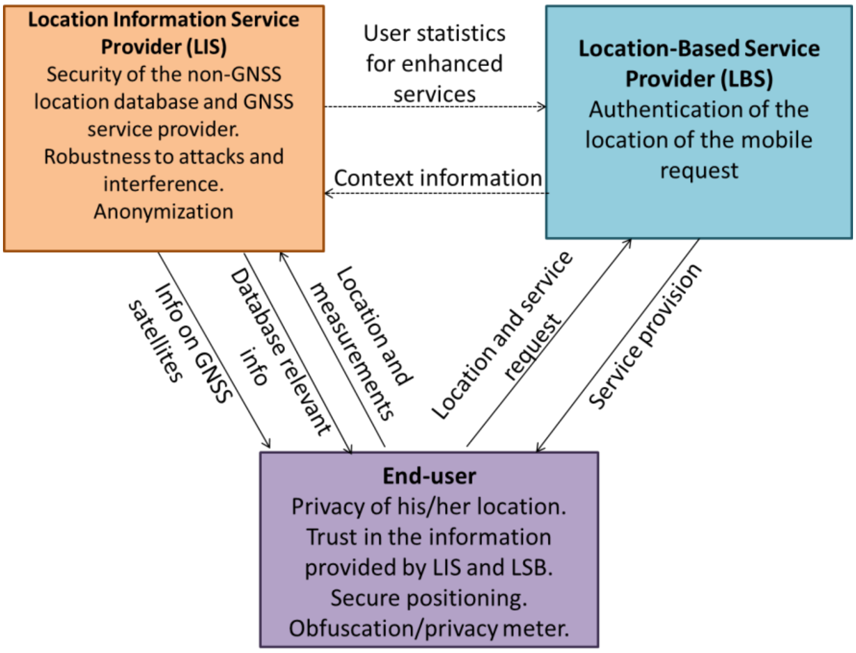
Location Information Service Provider (LIS)
Security of the non-GNSS location database and GNSS service provider.
Robustness to attacks and interference.
Anonymization
User statistics for enhanced services
Context information
Location-Based Service Provider (LBS)
Authentication of the location of the mobile request
Info on GNSS satellites
Database relevant info
Location and measurements
Location and service request
Service provision
End-user
Privacy of his/her location.
Trust in the information provided by LIS and LSB.
Secure positioning.
Obfuscation/privacy meter.

Figure 1. Interactions between the three major actors in localization and the security issues

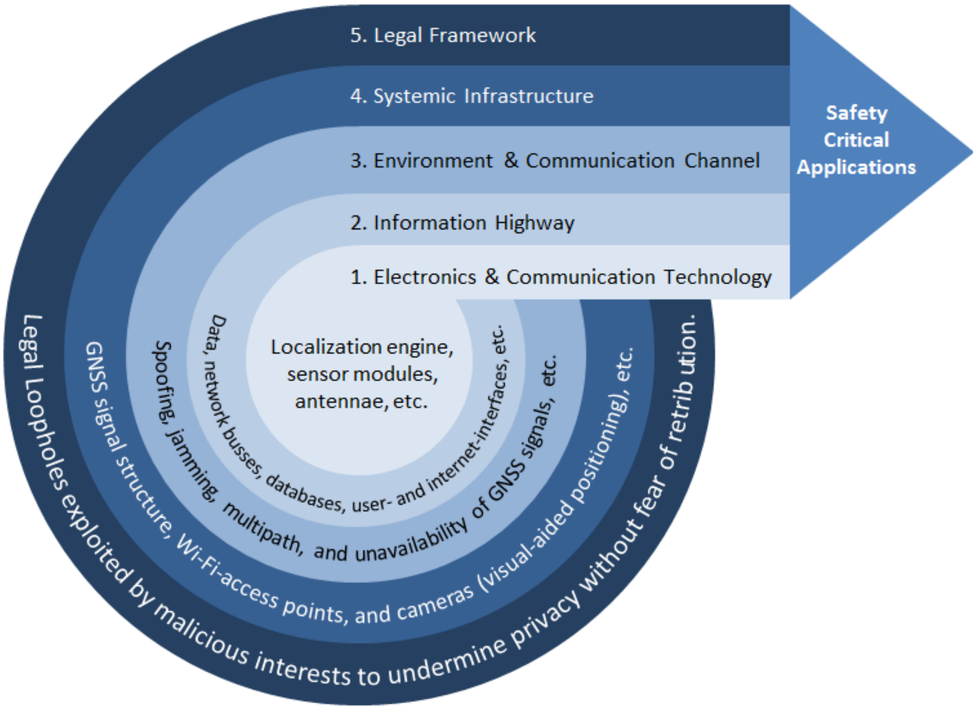
5. Legal Framework
4. Systemic Infrastructure
3. Environment & Communication Channel
2. Information Highway
1. Electronics & Communication Technology
Safety Critical Applications
Localization engine, sensor modules, antennae, etc.
Data, network busses, databases, user- and internet-interfaces, etc.
Spoofing, jamming, multipath, and unavailability of GNSS signals, etc.
GNSS signal structure, Wi-Fi-access points, and cameras (visual-aided positioning), etc.
Legal Loopholes exploited by malicious interests to undermine privacy without fear of retrib ution.

Figure 2. Different layers of requirements of trustworthy localization

However, not enough attention has been paid to information security in positioning and navigation applications, nor to the related legislation. Security issues are encountered at all levels of the stakeholders involved in a localization process: end-user privacy, security of the localization solution offered by the localization provider, and authentication and trust issues from the LBS provider's point of view. The growing processing capacity of mobile devices (e.g. smartphones) as well as the possibilities enabled by cloud computing facilitate innovative solutions that have not been feasible before. For example, the ability to process and analyze raw GNSS signal measurements on a smartphone has only recently become a possibility.

CURRENT VULNERABILITIES IN LOCATION ESTIMATION

Vulnerabilities of localization as for example the ones described in [12-18] include unintended interference of the position or timing solution, deliberate attack on the physical or virtual infrastructure of a localization system, theft of information from the localization system or its related segments, and gaps in the policy framework supporting the legal creation and exploitation of location-based applications potentially risking the privacy of the individual.

GNSS vulnerability is becoming more real and the risk is ever increasing. Failure of safety and mission critical location-based systems, such as power systems, military operations, aircraft systems and high value transport systems as well as governmental systems such as road user charging or commercial structures such as pay-as-you-go services, can have a shattering impact on infrastructure, economic stability, crime prevention and national security. Unintentional threats are those where unintended interference from some other source affects location estimation performance (e.g. other radio systems such as mobile phone networks etc. to GNSS). Deliberate/malicious threats include those incidents where the threat is a direct attack on a specific object. Intentional interference may take a number of forms such as:

- **Jamming**: Broadcast of an interference signal to prevent a GNSS receiver from acquiring and tracking GNSS satellites
- **Spoofing**: Broadcast of synthetic GNSS signals to try to trick a GNSS receiver into using the false signals and obtaining an incorrect position or time
- **Meaconing**: Re-broadcast of real satellite signals after a brief delay in order to create errors in the GNSS receiver

The reasons for intentional interference may be crime, terrorism, or deliberate mischief without clear understanding of the consequences. The recent increase in the use of PPDs is an example of deliberate interference towards GNSS that is occurring more and more without the actors actually having broader harming intentions – just unawareness of the risks and more extensive affects. Reasons for using the personal privacy devices may include incentives such as fraud and privacy concerns, and may be in response to e.g. road charging or offender tracking processes.

Regarding vulnerabilities in non-GNSS, the WiFi signals or other signals from the ISM (industrial, scientific and medical) band that can be used for in particular indoor localization are also highly vulnerable to radio interferences as ISM bands are freely shared by many signals and applications [19].

REQUIREMENTS FOR ENHANCING TRUSTWORTHINESS

Localization is becoming an increasingly crucial part of modern communication systems, such as Internet of Things (IoT) and 5G cellular communications. As such, the location trustfulness and the ability to identify and authenticate correctly the three actors in localization (see Fig. 1) are very important issues. There are currently very few metrics to define the location trustworthiness, and the majority of the research in wireless localization is focused towards accuracy and availability of the positioning solution. We define here the following trustworthiness metrics:

- **Proximity metrics**: only a certain geo-spatial region could be allowed for a LIS provider, LBS provider or end-user when receiving information from the other actors in Fig.1. For example, a user device located in Helsinki, Finland could reject all database information or all service providers which are not tagged in Helsinki region (or in a smaller defined geographical region). Both distance proximity and temporal proximity metrics could be envisaged [20]
- **Authentication metrics**: the signals used for positioning could have authentication keys embedded within them, so that un-authorized or fake signals are automatically rejected. Similarly, the LBS provider can offer services only to authorized users, identified through certain authentication procedures
- **Similarity metrics**: if the LIS or LBS providers have access to the location information of many users, some similarity patterns between users located in close proximity to each other can be checked and the outliers can be thus detected and removed. Also similarity patterns with past user geo-location information, when such information is available, can be used for an increased trustworthiness of the user location data from the network side
- **Privacy metrics**, such as the location uncertainty related to a particular user or the linkability of location information to the user who generated it [21]

COUNTERMEASURES AND PREPAREDNESS

Though development and preparedness for threats have increased in recent years in systems relying on location, there are still much to do regarding reliability. Developing countermeasures have been very active in the past few years in particular in GNSS receiver design and also non-GNSS based localization systems are more and more equipped with robustness features for failures.

GNSS

Most of the GNSS jammers encountered are based on a pulsed chirp-generator with varying period and frequency - these are easier and cheaper to produce and are effective because GNSS receivers generally lack protection against such attacks. Interference countermeasures can be implemented in all stages of a GNSS receiver, the acquisition, tracking and navigation stages. Reliability monitoring and outlier detection are also crucial in threat risk analysis. In addition, anti-attack methods utilizing inertial sensors or vision to augment the GNSS signal processing in the presence of unwanted radio frequency signals harassing the GNSS processing increase information security.

Interference detection can be done through monitoring of the AGC (automatic gain control) level, the received signal strength of each tracked satellite and the digitized signal levels [22-23]. In general terms, jamming detection can be defined as the process of revealing the presence of a jamming source within the signal band of interest, as e.g. discussed in [24]. Multiple antennas can also be used to detect an interfering signal by exploiting the spatial properties of signals received from satellites and from a jammer respectively (i.e. they arrive from different directions). Such a detector was, for example, proposed in [25], where the phase difference between two receive antennas was estimated and used to detect a spoofing. Interference can also be detected based on correlation with other sensor, as e.g. discussed in [26].

Interference mitigation methods can be divided into techniques based on signal processing, antenna configuration, sensor integration and system deployment. More information can be found e.g. in [18, 27-30]. With regards to interference mitigation the following are some of the most prevailing approaches:

- Interference mitigation using signal processing techniques
- Using antenna configurations for example, antenna arrays
- Sensor integration with inertial navigation systems and visual sensors
- Techniques related to system deployment e.g., use of multi-GNSS receivers and use of cooperative systems

Non-GNSS

Many indoor localization solutions nowadays rely on two phases, the training phase which collects data from indoor spaces and the estimation phase, when the actual mobile positioning is done. The collected data can take various forms, such as signal fingerprints, coverage areas, timing information, and so on. The data gathered in the training phase is stored at a location server in huge databases. In the on-line estimation phase, parts of this data are transferred to the mobile to enable it to calculate its location. Many indoor localization technologies nowadays, such as WiFi, Bluetooth, RFID, etc, which rely on Received Signal Strength (RSS) measurements for positioning purposes, are highly vulnerable to location jamming, spoofing and location database manipulation attacks. Solutions to deal with the vulnerabilities in non-GNSS localization solutions include:

- anonymity zones to preserve the anonymity of message destination in positioning-based routing of messages, for example in mobile ad hoc networks [31]
- improving the secrecy capacity of the Primary User (PU) channel by sharing the channel with secondary users (SU) [32]
- using Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP) scheme for mobile devices that allow the co-located users to mutually prove their location history while still protecting the anonymity and location privacy of individual users [33]
- time, RSS, amplitude and angle discrimination methods [34]. For example, jumps in amplitude, RSS and/or signal-to-noise ratio of the navigation signal can be used to identify possible attacks; also a big clock offset during a short time or fast phase changes may be good indicator for an attack
- consistency cross-checks [35], for example, cross checking the consistency of the data from the inertial sensors and the localization results from the wireless signals can provide more information about the trustfulness of a location estimate
- database protection (e.g., through watermarking) and attack-proofing in crowdsourced positioning
- integrity monitoring solutions [36]

Cryptography

Cryptography is crucial for ensuring information security and, hence, it will be important also for increasing the trustworthiness of location estimation. Typical use cases of cryptography include providing confidentiality, integrity, and authenticity for data in communication or storage (see, e.g., [37]):

- Confidentiality ensures that the data can be accessed only by authorized entities. Typically this means that an entity encrypts the data with a strong encryption algorithm (e.g., with AES [38]) that allows decryption only by entities who possess the secret key used in the algorithm
- Integrity ensures that an entity is able to verify that the data has not been tampered. This can be achieved, for instance, by computing a cryptographic check sum with a hash function (e.g., with SHA-256 [39])
- Authenticity provides proofs that an entity is the one that it claims to be (e.g., with cryptographic access control or challenge-response protocols) or that data truly comes from an entity it is claimed to come from (e.g., with digital signatures)

All above aspects can have importance also in location estimation and handling of position data. Despite the severity of security threats in location estimation, information security has had a low priority in designing these systems and they include only little use of cryptography [40]. In military GPS, cryptography restricts access to more precise location information (although the specifics are classified) [41]. There are plans to include cryptography even for civilian use in future GNSS systems such as in the Galileo commercial service, e.g., using strong cryptographic authentication would prevent the threat of fake satellites. However, cryptography cannot prevent all attacks in GNSS, such as replay attacks/meackoning where a signal from a legitimate satellite is replayed by an adversary [42].

Cryptography can play a role also in location estimation itself. Cryptographic distance-bounding protocols (e.g., [43]) are protocols to derive a strict upper-bound for the distance between two entities. They derive this bound by utilizing the fact that signals cannot travel faster than the speed of light and prevent cheating in the protocol by using cryptographic commitments and authentication [43]. Such protocols can be used, e.g., for secure positioning in wireless networks without relying on external positioning services (such as GNSS) [40,44].

Cryptography has significance also in ensuring privacy. Contemporary location based services rely on a user releasing his/her location data to the service provider which is an obvious privacy concern. Cryptographic techniques would allow, e.g., proximity testing so that the exact locations are not revealed (e.g., [45]). This kind of applications are mostly still in their infancy but can be expected to play a role in the future when people become more aware of privacy aspects of location based services.

Legal Aspects Related to Systems, Devices and Privacy

In the EU and Finland in particular, legal initiatives in order to prevent GNSS jamming and spoofing threats have not received enough attention till today. For its part, Galileo Public Regulated Service (PRS) represents an important addition in the area [16]. The objective of the legal analysis under the INSURE project (www.insure-project.org), that the authors are involved in, is to explore the existing legislation and its suitability to promote system security and location data privacy, and to tackle illegal jamming and spoofing devices. Several legal aspects are relevant in this respect:

1. Personal data protection relating to the collection and use of the location information
2. Risks exposed with using jamming and spoofing devices
3. The right to own, possess, and use devices that interfere with or alter the signals
4. The limits of legitimate activities and consequences for exceeding them
5. The assessment of whether the European, and Finnish, regulation is up to date with regard to this phenomenon

The term ‘spoofer’ and in many cases ‘jammer’ may not be mentioned in the relevant laws, but the use of devices that interfere with radio communications could be illegal in different laws. At EU level, relevant provisions and initiatives are rather scattered: with regard to Galileo PRS, Decision No 1104/2011/EU of the European Parliament and of the Council of 25 October 2011 on the rules for access to the public regulated service provided by the global navigation satellite system established under the Galileo programme (PRS Access rules) [46] is an important legal document. A point of contact must be designated for purposes of reporting electromagnetic interference, which is apt to harm and affect the PRS. It also includes provisions on manufacture and security of receivers as well as export restrictions for technology. Moreover, Decision No 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision) [47] aims at coordination of radio spectrum policy for availability and efficient use while taking into account the interests in avoiding harmful interference, among others. With regard to equipment, the Radio Equipment Directive (RED) 2014/53/EU [48] applies from 13 June 2016 revising the R&TTE Directive 1999/5/EC [49]. Similarly, the Electromagnetic Compatibility (EMC) Directives 2004/108/EC [50] has been replaced by Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility (recast) [51] on 20 April 2016. These legal instruments will be relevant in addressing the legal status of jamming and spoofing devises in particular. In addition, the EU data protection law must be taken into account. The most important piece of legislation dealing with the protection of personal data, including location data, is the Data Protection Directive of 1995 [52] which will be replaced by the General Data Protection Regulation (GDPR) [53] in May 2018. Simultaneously, some provisions of the e-Privacy Directive [54] are relevant to address location privacy in the electronic communications sector. The Finnish legal framework is significant in light of relevant EU law, including amendments made or needed to comply with the requirements. Furthermore, various provisions, including those of criminal law, exist at national level.

Proceeding from the current legal frameworks, the INSURE project analyses current suitability in preserving and improving GNSS system security, in dealing with jamming and spoofing devices and in ensuring the privacy of individuals. The main goal relating to policy aspects of the INSURE legal team is to address the balance between system security and end-user privacy from a legal perspective. The effectiveness and limits of existing anonymization techniques and possibility of using location data in business is of particular interest. Analysis is needed on issues, such as which data is at risk and why, alongside mapping the grey areas of legislation in EU and in Finland.

CONCLUSIONS

This paper addressed aspects of trustworthiness in localization related to the INSURE project: what are the constraints of ensuring continuous logistics of a localization solution, different layers of location information security, requirements and the potential solutions. Firstly a brief state-of-the-art analysis of vulnerabilities in localization was given followed by reviewing the countermeasures in GNSS, non-GNSS, cryptographic techniques and legal aspects all taken into account. The authors’ research in the INSURE project as a whole aims to contribute to a trustworthy localization future – increased trustfulness being the main aim of the INSURE project.

REFERENCES

[1] Cavoukian A., K. Cameron (2011). Wi-Fi Positioning Systems: Beware of Unintended Consequences - Issues Involving the Unforeseen Uses of Pre-existing Architecture, Information and Privacy Commissioner, Ontario, Canada, June 2011.

[2] Gibbons G. (2013) FCC Fines Operator of GPS Jammer That Affected Newark Airport GBAS. *Inside GNSS*. August 2013. Available at http://www.insidegnss.com/node/3676

[3] Warman M. (2012). Organised crime routinely jamming GPS. *The Telegraph*, February 2012. Available at http://www.telegraph.co.uk/technology/news/9096080/Organised-crime-routinely-jamming-GPS.html

[4] Bissmeyer N., K. H. Schröder, J. Petit, S. Mauthofer and K. M. Bayarou (2013). Short paper: Experimental analysis of misbehavior detection and prevention in VANETs. IEEE Vehicular Networking Conference 2013, Boston, MA, 2013, pp. 198-201. doi: 10.1109/VNC.2013.6737612

[5] Seneviratne S., F. Jiang, M. Cunche and A. Seneviratne (2015). SSIDs in the wild: Extracting semantic information from WiFi SSIDs. IEEE 40th Conference on Local Computer Networks (LCN), Clearwater Beach, FL, 2015, pp. 494-497. doi: 10.1109/LCN.2015.7366361

[6] The Wall Street Journal (2010). Stalkers Exploit Cellphone GPS. Available at http://www.wsj.com/articles/SB10001424052748703467304575383522318244234

[7] 'UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea' (2013). Available at: http://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea

[8] Divis D.A. (2014). Homeland Security Researching GPS Disruptions, Solutions. *Inside GNSS*. June 2014.

[9] SENTINEL: GNSS Services Needing Trust In Navigation, Electronics, Location & timing, Project report, 2011. Available at http://www.chronos.co.uk/files/pdfs/gps/SENTINEL_Project_Report.pdf

[10] GAARDIAN: GNSS Availability, Accuracy, Reliability anD Integrity Assessment for Timing and Navigation. Available at http://www.chronos.co.uk/index.php/en/gaardian

[11] STRIKE3, Standardisation of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation, EU H2020 project, Available at https://www.gsa.europa.eu/standardisation-gnss-threat-reporting-and-receiver-testing-through-international-knowledge-exchange

[12] Thomas M. (ed.) (2011). *Global Navigation Space Systems: reliance and vulnerabilities*. The Royal Academy of Engineering, March 2011, 48 p. ISBN 1-903496-62-4. Accessible via http://www.raeng.org.uk/publications/reports/global-navigation-space-systems

[13] Volpe J.A. (2001). *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System*. National Transportation Systems Center, U.S. Department of Transportation. Final report, August 2001, 113 p.

[14] Crane R. (2012). Radio Frequency Interference and the Cybersecurity Framework, U.S Remarks. GNSS Vulnerabilities and Solutions Conference 2012, Baška, Croatia. Accessible via http://www.gps.gov/news/2012/05/croatia/

[15] Xu Q., Rong Zheng, W. Saad and Zhu Han (2016). Device Fingerprinting in Wireless Networks: Challenges and Opportunities. In IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 94-104, Firstquarter 2016.

[16] Rügamer A., Kowalewski D. (2015). Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!. FIG Working Week 2015, From the Wisdom of the Ages to the Challenges of the Modern World, Sofia, Bulgaria, 17-21 May 2015.

[17] Sanou, D. and Landry, R. (2013) Analysis of GNSS Interference Impact on Society and Evaluation of Spectrum Protection Strategies. Positioning, 4, 169-182. doi: 10.4236/pos.2013.42017.

[18] Bauernfeind R., T. Kraus A. Sicramaz Ayaz, D. Dötterböck and B. Eissfeller (2012). Analysis, Detection and Mitigation of Incar GNSS Jammer Interference in Intelligent Transport Systems. Deutscher Luft- und Raumfahrtkongress 2012, Hamburg, Germany.

[19] Carvalho E., B. S. Faiçal, G. P. R. Filho, P. A. Vargas, J. Ueyama and G. Pessin (2016). Exploiting the use of machine learning in two different sensor network architectures for indoor localization. IEEE International Conference on Industrial Technology (ICIT), Taipei, 2016, pp. 652-657. doi: 10.1109/ICIT.2016.7474826

[20] Nurse J. R. C., I. Agrafiotis, S. Creese, M. Goldsmith and K. Lamberts (2013). Building Confidence in Information-Trustworthiness Metrics for Decision Support. 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, VIC, 2013, pp. 535-543. doi: 10.1109/TrustCom.2013.6

[21] Ma Z., F. Kargl and M. Weber (2009). A location privacy metric for V2X communication systems. IEEE Sarnoff Symposium, 2009. SARNOFF '09. Princeton, NJ, 2009, pp. 1-6. doi: 10.1109/SARNOF.2009.4850318

[22] Axell, E., Eklöf, F. M., Alexandersson, M., Johansson, M., & Akos, D. M. (2015). Jamming detection in GNSS receivers: Performance evaluation of field trials. *NAVIGATION*, Journal of the Institute of Navigation, vol. 61, no. 1, pp. 73–82, Spring 2015.

[23] Izos, O., Akos, D., Lindgren, T., Sun, C., & Jan, C. (2011). Assessment of GPS L1/Galileo E1 interference monitoring system for the airport environment. In Proc. of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS), Portland, OR, September, 2011.

[24] Borio, D., Dovis, F., Kuusniemi, H., & Presti, L. L. (2016). Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers. *Proceedings of the IEEE*, Vol. 104, Issue 6, pp. 1233 – 1245, June 2016.

[25] Montgomery, P., Humphreys, T., & Ledvina, B. (2009). A Multiantenna Defense: Receiver-autonomous GPS spoofing detection. *Inside GNSS*, vol. 4, nr 2, pp. 40-46, 2009.

[26] Faurie, F., & Giremus, A. (2011). Bayesian detection of interference in satellite navigation systems. In Proc of. IEEE Int. Conf. on Acoustics, Speech, and Signal Process. (ICASSP), Prague, Czech Republic, 2011.

[27] Dovis F. (ed.) (2015). *GNSS Interference Threats and Countermeasures*, Artech House, 2015, 216 p.

[28] Daneshmand, S. (2013). GNSS Interference Mitigation Using Antenna Array Processing, PhD thesis, University of Calgary, 2013.

[29] Ruotsalainen, L., Kirkko-Jaakkola, M., Bhuiyan, M. Z. H., Söderholm, S., Thombre, S. & Kuusniemi, H. (2014). Deeply-coupled GNSS, INS and visual sensor integration for interference mitigation. In Proceedings of the ION GNSS 2014, Tampa, FL, USA.

[30] Kirkko-Jaakkola, M., Ruotsalainen, L., Bhuiyan, M. Z. H, Söderholm, S., Thombre, S. and H. Kuusniemi, H. (2014). Performance of a MEMS IMU Deeply Coupled with a GNSS Receiver under Jamming, In Proceedings of the UPINLBS 2014, IEEE, Corpus Christi, TX, USA.

[31] Wu X., Jun Liu, Xiaoyan Hong, and Elisa Bertino (2008). Anonymous Geo-Forwarding in MANETs through Location Cloaking. *IEEE Transactions on Parallel and Distributed Systems*, Vol. 19, No. 10, October 2008.

[32] Zhang H., Tianyu Wang, Lingyang Song, and Zhu Han (2016). Interference Improves PHY Security for Cognitive Radio Networks. *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 3, March 2016.

[33] Wang X., Amit Pande, Jindan Zhu, and Prasant Mohapatra (2016). STAMP: Enabling Privacy-Preserving Location Proofs for Mobile Users. *IEEE/ACM Transactions on Networking*, 2016, DOI: 10.1109/TNET.2016.2515119.

[34] Martinez-Hernandez U., T. Dodd, T. J. Prescott and N. F. Lepora (2013). Active Bayesian perception for angle and position discrimination with a biomimetic fingertip. IEEE/RSJ International Conference on Intelligent Robots and Systems, Tokyo, 2013, pp. 5968-5973. doi: 10.1109/IROS.2013.6697222

[35] Miyazaki T. and M. Okada (2013). Motion pattern design satisfying dynamical consistency and differential relations between position, velocity and acceleration. 2013 Proceedings of SICE Annual Conference (SICE), Nagoya, Japan, 2013, pp. 395-400.

[36] Liu J., B. g. Cai, Y. h. Wen and J. Wang (2014). Integrity monitoring and risk evaluation for BDS-based train positioning using track map database. 2014 International Conference on Electromagnetics in Advanced Applications (ICEAA), Palm Beach, 2014, pp. 554-557.doi: 10.1109/ICEAA.2014.6903920

[37] Menezes A.J., van Oorschot P.C., Vanstone S.A. (1996). *Handbook of Applied Cryptography*. CRC Press.

[38] National Institute of Standards and Technology (2001). Advanced Encryption Standard (AES). FIPS PUB 197, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[39] National Institute of Standards and Technology (2015). Secure Hash Standard. FIPS PUB 180-4, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

[40] Capkun S., Hubaux J.-P. (2006). Secure Positioning in Wireless Networks. *IEEE Journal of Selected Areas in Communications*. 24(2):221-232.

[41] Global Positioning Systems Directorate (2013). Interface Specification IS-GPS-200H. http://www.gps.gov/technical/icwg/IS-GPS-200H.pdf

[42] Papadimitratos P., Jovanovic A. (2008). GNSS-Based Positioning: Attacks and Countermeasures. Proceedings of the 2008 IEEE MILCON Conference.

[43] Brands S., Chaum D (1994). Distance-Bounding Protocols. Advances in Cryptology---EUROCRYPT 1993. LNCS 765, pp. 344-359, Springer.

[44] Singelee D., Preneel B. (2005). Location Verification using Secure Distance Bounding Protocols. Proceedings of the 2005 IEEE International Conference on Mobile Adhoc and Sensor Systems Conference.

[45] Narayanan A., Thiagarajan N., Lakhani M., Hamburg M., Boneh D. (2011). Location Privacy via Private Proximity Testing. Proceedings of the 18th Annual Network & Distributed System Security Symposium (NDSS 2011). The Internet Society.

[46] OJ L 287 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011D1104

[47] OJ L 108 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002D0676

[48] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance, OJ L 153 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014L0053

[49] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, Official Journal L 091, 07/04/1999 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999L0005

[50] Directive 2004/108/EC of the European Parliament and of the Council of 15 December 2004 on the approximation of the laws of the Member States relating to electromagnetic compatibility and repealing Directive 89/336/EEC, OJ L 390.

[51] OJ L 96 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0030

[52] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31.

[53] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (2016) OJ L119/1.

[54] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201/37.