Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey

Liang Chen, Sarang Thombre, Kimmo Järvinen, Elena Simona Lohan, Anette Alén-Savikko, Helena Leppäkoski, M. Zahidul H. Bhuiyan, Shakila Bu-Pasha, Giorgia Nunzia Ferrara, Salomon Honkala, Jenna Lindqvist, Laura Ruotsalainen, Päivi Korpisaari and Heidi Kuusniemi

***Abstract*—Internet of Things (IoT) connects sensing devices to the Internet for the purpose of exchanging information. Location information is one of the most crucial pieces of information required to achieve intelligent and context-aware IoT systems. Recently, positioning and localization functions have been realized in a large amount of IoT systems. However, security and privacy threats related to positioning in IoT have not been sufficiently addressed so far. In this paper, we survey solutions for improving the robustness, security and privacy of location-based services in IoT systems. First, we provide an in-depth evaluation of the threats and solutions related to both Global Navigation Satellite System (GNSS) and non-GNSS based solutions. Secondly, we describe certain cryptographic solutions for security and privacy of positioning and location-based services in IoT. Finally, we discuss the state-of-the-art of policy regulations regarding security of positioning solutions and legal instruments to location data privacy in detail. This survey paper addresses a broad range of security and privacy aspects in IoT based positioning and localization from both technical and legal points of view and aims to give insight and recommendations for future IoT systems providing more robust, secure and privacy-preserving location-based services.**

***Index Terms*—Positioning, wireless localization, navigation, Internet of Things, GNSS, vulnerabilities, security, privacy, cryptography, trustworthiness, literature study**

I. Introduction

INTERNET OF THINGS (IoT), which is the concept of pervasive interconnected smart objects operating together to reach common goals [1], has become particularly popular with the rapid development of small low-cost sensors, wireless communication technologies, and new Internet techniques. Typical applications of IoT techniques includes intelligent transportation and logistics, smart home/building, environmental monitoring, medical and heath care, etc. Extensive surveys of architectural elements, features and development tendencies in IoT are provided in [1], [2]. Key applications and, in particular, applications of IoT in industry are reviewed in [3], [4]. Security has often had a low priority for vendors of IoT devices and this has led to a situation where IoT is filled with security vulnerabilities in practice. Hence, also the security and privacy of location information and an IoT enabled Location-Based Service (LBS) are often exposed to attacks.

In IoT systems, context-awareness has been recognized as a significant property. Within all the context sensing information, the location information plays important roles [5]. During the last two decades, researchers and engineers have developed a significant amount of prototypes, systems, and solutions using positioning and localization modules in IoT sensor nodes. For instance, Telit [6] integrates the Global Navigation Satellite System (GNSS) module with Wireless Local Area Networks (WLAN) and Bluetooth Low Energy (BLE) receivers, and other localization enabled IoT systems include Sierra Wireless [7], SOFIA [8], CRYSTAL [9], Carriots [10], Thingworx [11], etc.

The main actors involved in IoT positioning are illustrated in Fig. 1:

- The *IoT device*. The device whose location is determined or used by the system. It can be smart or dumb; smart IoT devices can have a positioning engine on themselves and can support device-centric passive positioning (i.e., without sending their location to the network); dumb IoT devices can be positioned only in a network-centric active approach (i.e., the network computes the device location and it either sends it back to the device or uses it for various location-based or location-aware services).
- The *network* part. The part of the network that is involved in positioning and LBS. It can be further split into two either collocated or distinct parts:
  - The *Location Aggregator (LA)*. This is the network part providing the location information (in network-centric approaches) or the location databases (in device-centric approaches).
  - The *Service Provider (SP)*. This is the network part providing the location-aware or LBS to the end-user/IoT device.

Various positioning technologies can be used in IoT. They can be classified into three main classes, which are affected by different security and privacy threats:

- *GNSS positioning*. This is one of the most privacy-preserving solutions from the end-user's point of view because positioning is done directly in the IoT device without the network or third parties. It works only for smart IoT devices with incorporated GNSS receivers and

L. Chen, S. Thombre, H. Kuusniemi, S. Honkala, M. Zahidul H. Bhuiyan, L. Ruotsalainen, G.N. Ferrara are with Finnish Geospatial Research Institute FGI, National Land Survey, Finland, firstname.lastname@nls.fi

K. Järvinen is with University of Helsinki, Department of Computer Science, Finland, kimmo.u.jarvinen@helsinki.fi

E.S. Lohan and H. Leppäkoski are with Tampere University of Technology, Finland, firstname.lastname@tut.fi

A. Alén-Savikko, S. Bu-Pasha, J. Lindqvist and P. Korpisaari are with Faculty of Law, University of Helsinki, Finland, {shakila.bu-pasha, anette.alen, jenna.makinen, paivi.korpisaari}@helsinki.fi. A. Alén-Savikko, S. Bu-Pasha and J. Lindqvist have the equal contribution to complete Section V.

Date of the manuscript: April 13, 2017

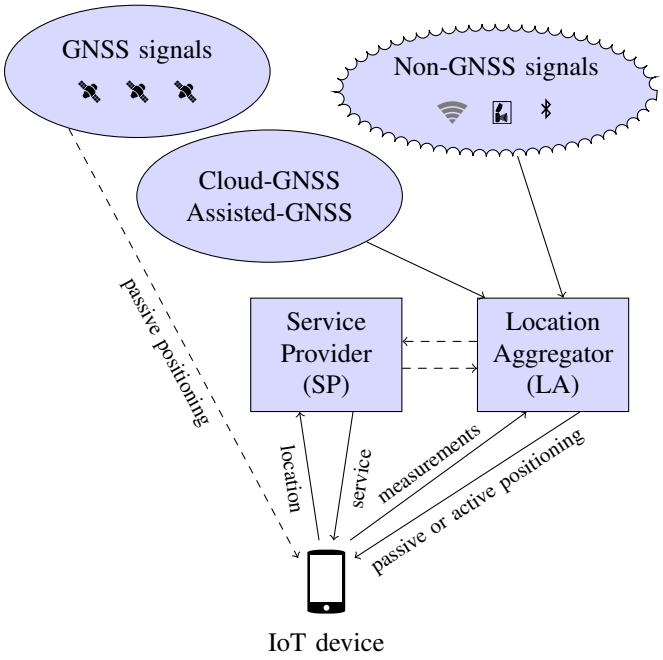


Fig. 1. Block diagram of the main actors in IoT positioning

requires good signal propagation conditions, e.g., outdoor conditions.

- *Assisted-GNSS* and *Cloud-GNSS positioning*. The Assisted-GNSS transmits the assistance data (e.g. the orbital parameters of the GNSS satellites, etc.) though a wireless network, mostly commonly over a cellular data channel [12]. As a result, the Assisted-GNSS significantly improves the startup performance, i.e., time-to-first-fix (TTFF) of a GNSS receiver. The Cloud-GNSS receivers take advantage of cloud computing platforms in computationally demanding applications, such as indoor positioning and multi-constellation processing, etc., or scientific applications which require collecting and processing GNSS signals over different geographical locations [13].
- *Non-GNSS* positioning. This is a wide class of positioning systems without GNSS that encompasses everything from cellular signals to Ultra Wide band (UWB), WLAN, BLE, or Radio Frequency Identification (RFID) signals. Also the signals based on IoT standards, such as enhanced Machine Type Communication (eMTC) [14], [15], NarrowBand IoT (NB-IoT) [16], [17] and LoRa® [18] belong to this class.

In all interactions between the IoT positioning actors illustrated in Fig. 1, there are several sources of vulnerabilities in terms of the robustness, security and privacy of the location solution. The main ones are as follows:

- *Intentional and unintentional system failures*. These can affect all actors in Fig. 1.
- *Intentional and unintentional Radio Frequency interferences (RFI)*. These can affect all actors in Fig. 1, although some interference types may be specific to a certain technology, such as spoofing and jamming in GNSS or interference in ISM (Industrial, Scientific and Medical) bands for systems operating in the ISM bands, e.g., WLAN and BLE.
- *Database-related vulnerabilities*. These typically affect the LA and the IoT device in certain non-GNSS and Cloud-GNSS solutions.
- *Loopholes in privacy-related protection*. These affect mostly the SP.

The rest of the paper explains in more details these vulnerabilities and mitigation methods to deal with them. The paper is organized as follows: Section II discusses robustness of GNSS-based solutions for localization. These include robustness against system level and service level faults, robustness against unintentional interference due to atmospheric conditions and RF transmissions in other frequency bands, robustness against interference due to obstructions, and lastly, security against intentional interference perpetrated through signal jamming and spoofing. Section III addresses security of non-GNSS solutions. This includes discussion about database outlier detectors and malicious nodes detectors, impact of malicious nodes on positioning performance, and interference mitigation in non-GNSS positioning. Section IV describes cryptographic solutions for security and privacy of positioning and LBS. This includes cryptographic techniques for security of location information, secure localization and location verification, IoT-related challenges for implementing cryptography, and discussion about cryptography for privacy-preserving LBSs. Section V discusses legal dimensions of location data, with a focus on data protection law. In addition, intentional interference of GNSS signals, including jamming and spoofing, is discussed with a view on the legal challenges it presents. Legal issues are discussed on a supra-national level, that is, in the framework of the European Union (EU). This section does not discuss other jurisdictions since the focus of legal research is on EU law. The findings and recommendations from these sections is summarized in Section VI with a discussion about the technical and legal requirements for trusted navigation and positioning solutions. We end the paper with conclusions in Section VII.

II. Robustness and Security of GNSS-Based Solutions For Localization in IoT

The possible GNSS threats to IoT positioning are shown in Fig. 2. The solutions to improve the robustness and security of the GNSS based positioning for IoT will be discussed in the following four part, i.e. robustness against GNSS system level failures, robustness against effects of Earth's atmosphere and space weather, security against RF interference and robustness with signal obstructions and indoors.

A. Robustness against GNSS system level faults

A number of incidents have shown the possibility of faults on the GNSS system level. Single GPS satellite faults have occurred several times in the past including failures of the satellite clock [19], [20], and signal deformations caused by failures in the transmission hardware [21]. In terms of multiple satellite faults, a failure in the GNSS control segment can cause problems that affect multiple satellites simultaneously.

TABLE I
SOLUTIONS TO IMPROVE ROBUSTNESS IN SYSTEM AND SERVICE LEVEL FOR GNSS SECURITY POSITIONING

Methods	Advantages	Disadvantages	Recommendation to IoT based positioning
Receiver Autonomous Integrity Monitoring (RAIM) [25]	Applying statistical detection excludes single satellite faults effectively	Requires sufficient satellite visibility for redundancy	Low complexity, suited for IoT devices
Space Based Augmentation Systems (SBAS) [26], [27]	Quick alerts in case of satellite faults, also improves accuracy via differential corrections	Need to receive and process SBAS satellite signals. Service coverage area is limited	Low complexity and cost. Augmentation information can also be accessed over the Internet
Multi-GNSS	Multiple independent GNSS constellations provide redundancy	Increased receiver complexity	High complexity, but common in current low-cost receivers. Well suited for IoT considering the price-performance ratio
Advanced RAIM (ARAIM) [28], [29]	Excluding multiple faults, no external service obligatory	Requires multi-GNSS, no well-established implementations exist yet	Moderate complexity, possibility to be applied to in future IoT smart receivers where high integrity is required

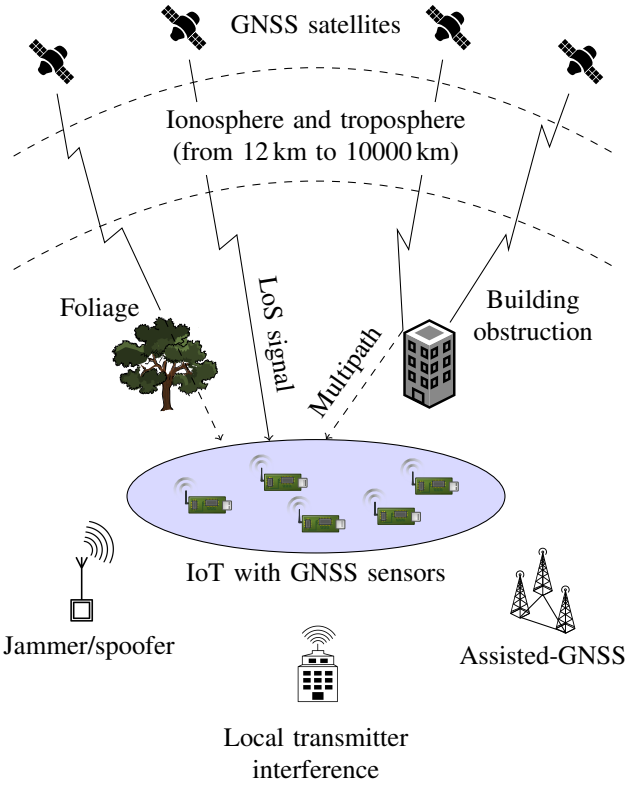


Fig. 2. Block diagram of GNSS threats to IoT positioning

The GLONASS system experienced such a fault in April 2014, when incorrect satellite positions were transmitted by the entire constellation for up to 10 hours [22]. Moreover, some GPS-GLONASS dual-constellation receivers failed to exclude the erroneous GLONASS measurements and make a transition to stand-alone GPS positioning [23]. Another control segment mishap affected GPS in January 2016, when an anomaly in the time signal caused disruptions in GPS-based timing systems worldwide [24].

Solutions to the threat of single satellite faults have been addressed in the civil aviation domain, where integrity and continuity are critical. It should be noted that methods which have been developed for critical civilian applications, are also feasible for IoT applications. The corresponding mitigation methods are summarized in Table I.

B. Robustness against effects of Earth's atmosphere and space weather

The GNSS signals travel more than 19000 km from the satellite to receiver on the Earth. The different factors affecting GNSS signals during the travel are well documented.

- Solar flares [30] and coronal mass ejections (CME) result in electromagnetic energy [31] reaching the Earth's outer atmosphere [32], [33], which increases the thickness and free electron content of the Ionosphere [32], [34], [35].
- While passing through the Ionosphere, GNSS signals experience refraction and diffraction effects, effectively degrading the signal to noise ratio and phase cohesion, and introducing a spatially variable delay component. This is called ionospheric scintillation (IS).
- The Troposphere, and specially its contents of pollutants and aerosols coupled with varying temperature and humidity [35] also contribute to degradation in GNSS signal quality, and introduces its own spatially variable delay.

Together these layers of the atmosphere affect different satellite signals differently because of the spatial diversity of their penetration. The effect of the atmosphere on the GNSS receivers [36], [37], [38] can thus be profound – introducing delay errors [39] and hence degradations of tens of meters [40] in positioning accuracy. High precision receivers using carrier phase-based positioning are especially vulnerable to cycle slips, loss of tracking lock, and even complete outage (unavailability of positioning, navigation and timing (PNT) solution) for tens of seconds [33], [41], [42].

A number of solutions have been recommended over the years to improve positioning robustness against atmospheric and space weather effects and they are listed in Table II.

C. Security positioning against RFI

RFI is a disturbance generated by an external source that affects the signals in the radio frequency spectrum of the interest [45]. In consideration of RFI to GNSS signals, the

TABLE II
SOLUTIONS TO IMPROVE ROBUSTNESS AGAINST INFERENCE FROM EARTH'S ATMOSPHERE AND SPACE WEATHER

Methods		Advantages	Disadvantages	Recommendation to IoT based positioning
Applying corrections to compensate for errors	Applying broadcast error corrections with Ionosphere models and Troposphere models [34], [40]	Corrections available through the GNSS navigation message	• Corrections based on approximations, limited accuracy • Results in residual errors	Low complexity and easy to implement in IoT solutions as no additional resources (hardware, software, energy) are necessary
	Applying differential corrections: SBAS/GBAS, reference networks, commercial services [34], [33], [43]	• Locally relevant corrections computed with greater density of grid points • Augmentation systems can provide additional ranging signals and system integrity information	• Need to communicate the corrections to the target receivers • In case of severe interference and complete loss of PNT solution, both target and reference receivers equally affected	• SBAS capability does not add significantly to receiver complexity or cost • Using commercial services for correction data can be costly
Receiver's signal tracking architecture	• Code-phase based tracking, FLL-assisted PLL [32] • Vector Tracking Loops [31]	• Improves robustness and sensitivity of receivers at low SNR • Quick reacquisition of satellite signal after event has passed	• Improved robustness at the cost of degraded accuracy • Substantial fault in one of the vector-tracking channels can infect other tracking channels	• Code-phase based FLL-assisted PLL tracking is a low complexity commonly employed tracking loop mechanism • relatively higher computational and implementation complexity in Vector Tracking Loops
	Data-less signal tracking [32]: • Predicting the navigation data bits • Using modernized GNSS signals containing data-less signal components	Improves robustness of carrier-phase based against cycle slips even in adverse interference conditions	• Need for additional resources to implement the database of a-priori predicted data bits. • Using modernized signals may require a multi-frequency receiver depending on the signals being used	• Higher complexity and need for additional resources if data bit prediction is used • Lower complexity if modernized signals are employed • However, may require additional RF processing chain for any additional RF frequency
	Dual-frequency receiver [33], [43], [32]	High accuracy of Ionospheric error compensation (lower residual errors)	• Need to use mathematical models for compensating Tropospheric errors • Need for additional radio frequency hardware to process additional frequency band	• May require additional RF processing chain for any additional RF frequency. High implementation cost for mass-market applications • Dual-frequency receivers consume more battery power
External aiding of the GNSS receiver with additional sensors [34], [31]	Inertial sensors (accelerometers, gyroscopes), visual sensors, etc	High degree of robustness to short term external signal interference	• Additional hardware and software necessary • Sensors in themselves cannot provide PNT solution	Moderate implementation complexity. Applicability to IoT applications depends on the cost and quality of the sensor
Receiver-based integrity monitoring [31], [44]	RAIM and A-RAIM	• Effective way to assess integrity of GNSS signals, especially in safety-critical applications • Provides fault-detection (and possibly exclusion) in GNSS environment • A-RAIM provides the capability to detect multiple (even system-wide) faults	RAIM availability is dependent on the visibility of at least 5 satellites. Exclusion of the faulty satellite requires atleast 6 visible satellites	• RAIM algorithms can be implemented in software and do not substantially add to the computational complexity or resource burden of a receiver • A-RAIM is primarily targeted for aviation users and therefore not applicable for IoT
Other techniques [34], [33], [32]	• Alternate PNT infrastructure e.g. eLoran • Record and replay validation of receivers	These solutions are ground-based and therefore, not affected by atmospheric effects. eLoran transmissions are at higher power than GNSS, and can penetrate indoors	Require additional signal processing capability in the receiver	These solutions are out of scope for IoT applications

interference sources can be classified as intentional (e.g. jamming, meaconing and spoofing) and unintentional [45], [46]. For the unintentional RFI, the sources are mainly from the following aspects [47], [46], [48]:

- Energy leakage of out-of-band signals. For example, the harmonic interference from audio and video wireless broadcasting system, which occupy the FM, Ultra-High Frequency (UHF) and Very High Frequency (VHF) frequency spectrum, the narrow band signals generated by VHF Omnidirectional Radio-range (VOR) and Instrument Landing System (ILS) for approach landing systems, VHF communication system for Air Traffic Control (ATC) communications and amateur radio
- Interference due to band's approximate, e.g. wideband inference to GPS and Galileo signals from SATCOM band, which occupies the spectrum from 1626.5-1660MHz.
- In-band interference, which mainly caused by the pulse signal from distance measurement equipment (DME) and tactical air navigation system (TACAN), or wind profile radars, of which the frequency spectrum ranges from 962-1213 MHz, constituting a potential threat to GNSS signals of Galileo E5 and GPS L5 band.

Intentional RFI, which is deliberate interference to GNSS, includes mainly jamming and spoofing. Jamming is the transmission of signals in the GNSS frequency bands with the intent of disrupting the system operation, whereas spoofing is the transmission of counterfeit GNSS-like signals with the intent of fooling the receiver to use false information for positioning calculations.

The effects of (un)intensional RFI on GNSS receiver are assessed and analyzed in [45], [46], [49], [50], [51], [52], which includes the impact on different stages and observables in the GNSS receiver, including the frond-end, acquisition stage, tracking stage and the estimation of signal-to-noise ratios.

The methods to suppress RFI, especially the intentional RFI (e.g. jamming and spoofing) are needed to preserve the accuracy and guarantee the integrity of the GNSS-based solution in IoT systems. These techniques can be divided into four categories: techniques based on signal processing, antenna configuration, sensor integration and system deployment. A summary of the mitigation techniques is provided in Table III.

D. Robust localization in signal obstructions and indoors

GNSS positioning is degraded in urban areas and forests, where buildings and foliage, respectively, obstruct the signal propagation and cause multipath. Furthermore, conventional GNSS positioning is unavailable indoors and inside tunnels. Therefore, research and development has been active for decades for finding methods enabling the position computation in these challenging GNSS environments. These methods may be divided into four categories based on the equipment used for position computation: High-sensitivity GNSS (HGNSS) receivers, GNSS pseudolites, fusion of GNSS receiver with other data, and use of non GNSS radio signals for computing the position solution independent of GNSS. An overview of the three first ones is given in Table IV. Section III will discuss more on the fourth category.

III. Security of Non-GNSS Solutions for Localization

The main security and privacy-related threats in non-GNSS positioning for IoT devices are summarized in Table V. Typically, a non-GNSS positioning solution is either based on a two-stage approach (offline training database creation and on-line estimation with inputs from the training database) or based on a one-stage approach involving some timing or angle estimates. The first category is mostly encountered in the Received Signal Strength (RSS) solutions. This approach is often called location fingerprinting. Recent and good overviews of RSS-based localization can be found, e.g., in [83], [84], [85], [86]. The second category of one-stage approaches typically relies on Time Of Arrival (TOA), Time Difference of Arrival (TDOA), Angle of Arrival (AOA) or Phase Difference of Arrival (PDOA) techniques, explained, e.g., in [87], [88], [89], [90].

The IoT positioning methods relying on a training database have to cope with the possibility of database corruption and malicious nodes attacks (e.g., access points transmitting random or fake information). All non-GNSS positioning methods are vulnerable to various RF interferences, both wideband and narrowband. The non-GNSS positioning methods relying on signals in the ISM spectra are more vulnerable to interferences than those relying on signals in licensed bands. Also, all these non-GNSS methods have to rely on the network side (on LA, on SP or on both), and thus the issue of the trustworthiness of the network components is also an important one to be addressed.

A. IoT non-GNSS technologies for positioning and related security threats

The main non-GNSS technologies for positioning are illustrated in Table VI, together with their vulnerabilities. WLAN or WLAN-based positioning is by far the most widespread non-GNSS positioning technology in smart IoT devices [86], [91], [92], [93]. Other signals of opportunity, such as BLE [94], [93], [95], RFID [96], digital TV [97], [98] or UWB [99] can also offer positioning solutions, especially indoors. Wireless Sensor Network (WSN) based positioning is also used in a variety of sensor applications [100].

Several threats are related to the training database in RSS-based localization. The database includes information about the Access Nodes (AN), i.e., the static nodes of the network. In its simplest version the information is just the location of the AN and its unique Media Access Control (MAC) address [101], [102] while the more sophisticated versions include also information about signal propagation environment, such as coverage areas of ANs [103] or location dependent information on the probability distribution of the RSS from each of the MAC addresses [104], [105]. The later category of databases is usually based on extensive data collection. However, the database can also be generated automatically from AN locations and taking into account the signal propagation properties of the environment, e.g., floor and wall attenuations obtained from path-loss models and map or floor plan information [104], [106].

TABLE III
MITIGATION METHODS AGAINST RFI

	Methods	Features	Recommendation to IoT based positioning
Signal Processing	Wavelet transform [53]	• Transformed domain techniques implementation is computationally demanding and makes them unsuitable for real-time applications • Variable resolution (Wavelet transform) • Good performance for high power jammers (Hilbert-Huang)	Due to higher complexity, the implementation of transform-domain mitigation methods are not well-suited for IoT
	Hilbert-Huang transform [54]		
	Karhunen-Loéve [55]		
	Adaptive notch filter [56], [57]	• More computationally efficient than the transformed domain methods • Very good performance against any intentional or unintentional narrow-band jamming • Adequate mitigation performance for chirp-like jammers	A good choice for IoT localization considering the price-performance ratio
	Pulse blanking [58]	• Very low complexity • Sample-by-sample operation • Suitable for real-time implementations	Very well suited for IoT applications because of simple real time implementation
	Signal quality monitoring [59], [60], [51]	• Low complexity algorithm based on measurements at the correlators output able to detect distortion in the correlation function • Capable to protect against spoofing attacks with relatively matched power to the authentic signal [60]	Suitable for detection of GNSS jamming/spoofing/blockage, and hence, could trigger alternative methods for IoT localization
Antenna arrays	Post-despreading [61]	• Based on comparison of the estimated Angle of Arrival (AoA) of authentic and spoofing PRNs after they are fully tracked • Very computationally heavy	Not suitable for IoT due to heavy computational burden
	Pre-despreading [62]	• Before acquisition and tracking stage • Not heavy computational load imposed to the receiver • Might not perform well when spoofing signals are transmitted from multiple antennas	
Sensor integration	Integration with INS [63]	• Measurements from INS are not affected by jamming or spoofing • The performance suffers from measurements biases that accumulate in large position errors with time • Adequate for short-time jamming	Well suited for IoT localization in case of short GNSS outage due to signal blocking/ jamming/ spoofing
	Integration with visual sensors [64], [65]	• Feasible instruments for constricting the growth of INS errors • Improved robustness of the position accuracy when jamming is not only momentary	Suitable, only if visual sensors are already integrated in IoT sensors; otherwise, visual-based localization might seem expensive considering the price-performance ratio
System deployment	Multi-frequency multi-GNSS [66]	To change the frequency band of signals processed from one that is being interfered to another not being disrupted	Well suited for IoT applications that require integrity and robust navigation solution
	Cooperative ITS [66]	Use of vehicles as floating sensors and of existing road side equipment to monitor the environment cooperatively	Very well-suited for IoT localization

Both in the generation and in the maintenance phase of the database, several unintentional events may generate errors that affect the localization reliability. The locations of the AN or RSS entries may be estimated poorly, and if the location input requires user input, human errors can produce errors to the database. In crowdsourcing-based database generation or maintenance human errors are more probable than in cases when the persons are trained to do the data collection. In crowdsourcing, it is also possible that someone intentionally provides wrong locations, if they are entered manually as they often are at least indoors. Wrong RSS values can enter into the database if it is generated automatically and the map information includes errors. In data collection the poor RSS values can enter into the database if data is collected with a device that measures or reports the RSS unusually inaccurately. Again, this happens more likely in crowdsourcing where non-dedicated devices may participate. Once generated, the database requires maintenance, as the signal or propagation environment may change if ANs or obstacles such as walls, furniture, or vegetation, are moved, removed or added. In device-centric localization, possible communication line errors may corrupt the database during its transfer from the database

TABLE IV
ROBUST LOCALIZATION IN SIGNAL OBSTRUCTIONS AND INDOORS

Methods		Features	Recommendation to IoT-based localization
High-sensitivity GNSS [67]		• Combining the process of coherent and non-coherent integration • Able to acquire weak signals, e.g. GALILEO signals even below 10 dB-Hz after 5 seconds integration	• Complexity slightly high, possibly applied in high integrated IoT receivers • High expectations for GPS L5 and GALILEO E5 wideband signals for indoor localization [68]
GNSS pseudolite [69], [70], [71]		• Transmitting GNSS-like signals and able to provide a position solution indoors • Accuracy of the position may be very good, depending on the density of the transmitters and methods	• Suitable for IoT receivers • The transmitters should be well designed so as not to interfere GNSS signals
Fusion GNSS with other data	Loosely coupled [72]	Measurements obtained are computed independently from GNSS and sensors and then fused	• The performance of the fused system suffers from sensor measurement biases that accumulate to large position errors with time [73] • With the improvement of the accuracy of low cost INS sensors and also the computation capability of the IoT sensor nodes, these techniques are promising to be applied in IoT
	Tightly coupled [74]	Fusing GNSS pseudorange and pseudorange rate observations with measurements from the self-contained sensors	
	Deeply-coupled [75], [76], [77], [78], [79], [80]	Integrating information obtained from the inertial sensors to aid the GNSS and enhances system's robustness	
	Shadow matching [81], [82]	• Fuses GNSS ranging by 3D mapping with the GNSS shadow matching technique • Comparing the measured signal availability and strength with predictions made using a 3D city model	Suited for IoT with cloud computing techniques, where the 3D maps are restored in cloud or the server side

TABLE V
SECURITY THREATS AND MITIGATION METHODS IN NON-GNSS BASED LOCALIZATION

Security threat	Description	Mitigation
Database corruption: reference locations	Entering wrong reference locations either intentionally or unintentionally, due to human errors or faults in positioning technology	Outlier detection and database consistency monitoring
Database corruption: wrong RSS	Due to errors in maps, floor plans or other geographical information, erroneous RSS fingerprints are generated when computing them from these sources	Outlier detection and database consistency monitoring
Environment change	RF infrastructure: Addition, removal, or location change of ANs. Propagation environment: Changes in building structure or furniture	Outlier detection and database consistency monitoring
RF interference	Decreases the quality of localization, in extreme cases prevents signal reception and localization. Examples: narrow band interference (jamming) and wide band interference (affects mostly cellular 3G)	Interference detection and warning or mitigation
Malicious nodes	Sends fake or erroneous information, e.g., spoofing	Identification and exclusion
Privacy threat to making the IoT device position known	Identity theft based of IoT device location or other vulnerabilities regarding to the loss of location privacy	Data perturbation or obfuscation methods
Trusted network issue	In network-centric positioning network has full control on positioning information. This can be misused by untrustable networks	Authorised access support

server to the user.

Cellular-based positioning solutions, covering all digital cellular standards from 2G to 4G and beyond, e.g., to the proposed 5G, have been increasingly offering more accuracy and more robustness for the positioning functionality. Most of the cellular-based approaches work in a network-centric mode, where the network, based on the measurements from the IoT device, computes the device location. More recently, standards specifically dedicated to IoT communications, such as LoRa [107], NB-IoT [108], eMTC or other Low Power Wide Area Network (LPWAN) standards [109], support positioning of the nodes to a certain extent. For example, in LoRA, the positioning is supported via proprietary chirp spread spectrum with time stamping of packet arrivals, plus a combination of TDOA, RSS, and Differential RSS (DRSS) estimators. The target positioning error in LoRa is 3 m, with a coverage up to 5 km range urban and up to 15 km range suburban. In NB-IoT and Narrowband Cellular IoT (NB-CIoT) standards, only the basic positioning inherited from LTE/4G is supported, such as Cell-ID and Positioning Reference Signals (PRS)-based. In Machine-to-Machine / Machine Type Communications (M2M/MTC) standards, collaborative positioning methods have been proposed [110], which may introduce an additional layer with possible vulnerabilities, the one of the inter-communication between the IoT devices.

B. Database outlier detectors

Outlier detection methods developed by statistics and signal processing communities [111] can be used to find possible problems in the training database. As the data in databases

TABLE VI
NON-GNSS BASED LOCALIZATION TECHNOLOGIES AND THEIR SECURITY THREATS

	Technology									
Security threat	WLAN	802.11az FPS	Bluetooth	RFID	UWB	WSN	Cellular	LoRa and other LPWAN in ISM bands	NB-IoT / NB-CIoT	M2M (eMTC / LTE MTC)
Database corruption: reference locations	x	x	x	x						
Database corruption: wrong RSS	x	x	x							
Environment change	x	x	x	x	x (RSS)					
RF interference	x	x	x	x	x	x	x	x	x	x
Malicious nodes (affect unlicensed bands)	x	x	x	x	x	x				
Trusted network issue	x	x	x	x	x	x	x	x	x	x

with location dependent RSS information or coverage areas include mutual dependences, the consistency of the database can be analysed by using various outlier detection methods. With simple database including only MAC addresses and location information of the ANs, the consistency checks can be done when RSS measurements are available by comparing simultaneous measurements from multiple ANs and using theoretical coverage or path loss models and the geometry of the AN locations.

For localization based on databases with RSS information, the authors of [112] propose an outlier detection method that is based on non-iterative RANdom SAmple Consensus (RANSAC) to detect ANs from which the measured RSS is severely distorted. A crowdsensing-based management scheme for the training database is proposed in [113] where the coverage and the accuracy of the initial database are enhanced by collaboratively collected user data. Localization system for WSNs that localizes the nodes, uses outlier detection to monitor the quality of the RSS database, and updates the RSS database is proposed in [114]. The authors of [115] propose a localization scheme for RSS fingerprinting where the user's location and the ANs with erroneous measurements are jointly estimated by an online algorithm. For detecting outliers without the RSS information in the database, [116] proposes a method where distance is estimated from RSS and trilateration residuals and hypothesis testing is used.

C. Identification of malicious and fake nodes

Malicious and fake nodes in IoT positioning are those access nodes intentionally sending corrupt or fake information to the training database of the LA. Such corrupt information can be, e.g., the node position or it can affect the RSS values, if the malicious node changes randomly its transmission power, or even the node identity (e.g., if the access nodes are faking or changing their IP address, etc.). A malicious node transmitting incorrect position is of particular threat in applications such as Vehicular Ad Hoc Networks (VANET) [117]. An excellent classification of the malicious nodes mechanisms can be found in [118] in the more general context of IoT communications (not focusing on the positioning part). The types of malicious nodes attacks relevant to IoT positioning can be summarized as follows:

- *Conflicting behavior attack*. The untrustworthy node can transmit partially trustful information (e.g., correct IP address) and partially incorrect information (e.g., faking its position).
- *On-off attack*. A malicious node can transmit erroneous positioning-related information only from time to time, e.g., at random intervals.
- *Sybil attack*. This refers to malicious nodes using two or more IP addresses so that their identification is hindered by the random change in identity.
- *Newcomer attack*. A node previously identified as malicious can change its IP and enter the network again as a new node.

The authors in [119] proposed an algorithm based on linear regression for the identification of the mobile fake or malicious nodes, which requires a certain observation time interval and knowledge about a certain percentage of trustworthy nodes.

D. Data perturbation and other obfuscation methods

In order to preserve the privacy of the IoT device location or of the access node location, different forms of position information obfuscation methods have been proposed in the literature. The classical methods of obfuscation simply replace the true position information with a fake position information when transmitting this information between the actors in Fig. 1. An alternative way is the data perturbation method, when the true location is embedded in noise and only the noisy location estimates are transmitted. Various types of noise and noise distributions have been used in the literature: e.g., additive or multiplicative noises, correlated or uncorrelated with the location information, and drawn from various distributions. The most used distribution is the multivariate Gaussian; this case is referred to as the simple additive noise perturbation.

A third approach, presented in [120] for vehicle-to-vehicle (V2V) communications combines the obfuscation and power variability in order to form fake point clusters and to decrease the probability that an attacker gets hold inadvertently of the position of the IoT device.

More advanced mechanisms for the location privacy protection have been also presented in [121] (relying on Hidden Markov chains) and in [122] (semantic space translation).

E. Interference mitigation in Non-GNSS positioning

1) Measures against spoofing in Non-GNSS location: Spoofing refers to situations when an attacker sends fake position-related information to the IoT devices. This problem is closely related to the problem of fake or malicious nodes and has been addressed in Section III-C.

2) Measures against jamming in Non-GNSS location: Jamming refers to the narrowband interference of the wireless signals on which the non-GNSS positioning is based, such as narrowband interference in ISM bands (for WLAN and BLE-based positioning) or in the cellular bands (for cellular-based positioning). Examples of mechanisms to deal with jamming attacks in wireless networks are found in [123], [124].

3) Measures against meaconing in Non-GNSS location: Meaconing refers to the situation when an attacker captures a positioning-related signal and re-transmits it with a delay. This terminology is very seldom used in the context of Non-GNSS positioning, as its impact on the positioning accuracy is not so high as in the GNSS case. For example, for a WLAN-based or BLE-based positioning system, transmitting the RSS with a delay would basically have little or no impact on the training database used in positioning. For cellular-based positioning, due to the authentication mechanisms is also almost impossible to meacon the positioning signals. Thus, we can state that meaconing is not a threat in Non-GNSS positioning.

IV. Cryptographic Techniques for Secure and Privacy-Preserving Positioning in IoT

This section surveys cryptographic techniques that can be used for protecting location information and secure localization in IoT. Although work designed specifically for secure IoT localization is still mostly missing, we can utilize existing schemes originally designed for applications that are closely related or included in the IoT framework, such as (military) WSN or RFID. The IoT inherits many of the threats of the previous applications but, e.g., the heterogeneity of devices that are connected into the same worldwide network and the sensitive nature of location information (e.g., persons' movements) handled in applications also set new challenges.

In Section IV-A, we first review standard cryptographic solutions that can be used for securing communication of location information over a public network. Section IV-B reviews cryptographic distance-bounding protocols and secure localization which have been previously used primarily in WSN and RFID applications, but can be used more generally for IoT. The IoT sets strict constraints for cryptographic implementations and these are discussed in Section IV-C. Because IoT handles a lot of users' sensitive location information, localization in IoT also connects to privacy-preserving techniques and Section IV-D discusses certain aspects of privacy-preserving LBSs.

A. Standard cryptography for location information

Assume that a device (e.g., a beacon node or a user's personal device) knows its location (e.g., has a GNSS chip), which it and the network trust to be correct up to necessary precision, and the device wants to share this information with some other devices (e.g., regular nodes or cloud service provider) over the network (i.e., the Internet) in a secure manner. In this case, location information can be treated similarly as any other critical piece of information and standard cryptographic techniques can be used for securing communication [125]. The other devices can trust the correctness of the location information only if they can verify its authenticity and integrity. The former means that the location information was truly sent by the device claimed to be the source and not by a malicious party claiming to be the correct source (spoofing). The latter means that the information has not changed on the way. The former implies the latter, but not vice versa. The authenticity and integrity of location information can be ensured with standard cryptographic techniques. Computing a check sum by using a (cryptographic) hash function (e.g., SHA-256 [126]) gives integrity, but without additional techniques only against transmission errors (i.e., no security). If the parties have a shared secret key, they can use cryptographic message authentication to ensure both integrity and authenticity (see, e.g., HMAC [127]). Digital signature schemes based on public-key cryptography (e.g., (EC)DSA [128]) allow verification of authenticity and integrity without shared secrets. Additionally, digital signatures provide non-repudiation, which prevents a sender from later challenging sending the message. This can be an important feature also in the context of location information because it ensures that a device that has claimed to be at a specific location cannot later refuse this claim.

The above schemes provide only authenticity and integrity of location but the location information itself is, by default, transferred as plaint text and is available to anyone observing traffic in the network. The simplest form of privacy of location information (i.e., privacy in respect to third parties) can be achieved by ensuring confidentiality of location information transferred in the network. Confidentiality can be achieved by encrypting the location information, again, with standard cryptographic techniques. Encryption can be performed either with secret-key cryptosystems, which require that the communicating parties have securely shared a secret key, or with public-key cryptosystems, where the key used for encrypting is public (anyone can encrypt) but decryption is possible only with the secret key of the receiver. Typically, a combination of these is used so that the parties exchange a secret key using public-key cryptography (e.g., with Diffie-Hellman key exchange protocol [129]) and the actual encryption is performed with significantly more efficient secret-key cryptography (e.g., with AES [130]) by using this key. Public-key cryptography provides a solution for key distribution but often requires a Public-Key Infrastructure (PKI) to ensure that public keys belong to certain entities. Combination of confidentiality, authenticity and integrity can be achieved with authenticated encryption which can be achieved by authenticating (with the above schemes) the encrypted location information or directly by

using a cryptographic mode for authenticated encryption (e.g., AES-GCM [131]). However, even plain encryption may give some guarantees of authenticity and integrity because it can be difficult to forge a ciphertext that decrypts into a meaningful location. Table VII gives a summary of cryptographic schemes and their properties. Support for cryptographic techniques is included in popular protocol suites such as IPSec, TLS/SSL (e.g,. OpenSSL), and SSH.

TABLE VII
SUMMARY OF STANDARD CRYPTOGRAPHY FOR LOCATION INFORMATION

Scheme	Conf.	Auth.	Integr.	Shared secret[1]
Check sum			x	
Secret-key encryption	x	(x)	(x)	x
Public-key encryption[2]	x		(x)	
Message authentication		x	x	x
Digital signature[2]		x	x	
Authenticated encryption	x	x	x	x
Encryption[2] + signature[2]	x	x	x	

[1] Requires a shared secret key between the parties implying (a) a pre-shared secret (e.g., hardwired into the devices before deployment) or (b) the use of a key exchange protocol[2]
[2] Public-key cryptography (more expensive to implement)

B. Distance-bounding and secure localization

The situation gets more difficult when a device does not know its location or the location that it provides cannot be trusted by the network (i.e., the device itself may try to cheat its location, e.g., because it may be compromised or is not to be trusted in the first place). This kind of challenges can be expected to be common in the future IoT where devices that do not trust and have no previous knowledge of each others should convince each others about their locations. The cryptographic solutions discussed in Section IV-A do not provide a solution in this case, although they are still required to secure communication between the devices. Some solutions to this problem have been discussed already in Section III, but here we discuss a specific solution called cryptographic distance-bounding and its implications.

Cryptographic distance-bounding [132] was originally introduced by Brands and Chaum in 1994. The protocol gives an upper bound for the distance between devices based on signal travel time that is bounded by c, the speed of light, and cryptographic techniques that prevent specific types of cheating. The protocol involves two nodes, a verifier V and a prover P, and it consists of the following steps:

1) V selects k uniformly random bits: $a \in_R \{0,1\}^k$.
2) P selects k uniformly random bits: $m \in_R \{0,1\}^k$.
3) P commits to m by using a cryptographic commitment scheme $d = \text{commit}(m)$ and sends d to V.
4) V and P repeat the following steps for $i = 1, \ldots, k$:
   a) V sends a_i to P and starts a timer.
   b) P receives a_i, computes $b_i = a_i \oplus m_i$, and sends b_i immediately to V.
   c) V receives b_i and gets the time t_i from the timer.
5) P sends the digital signature $s = \text{sign}(a, b)$ and means to open the commitment d to V.

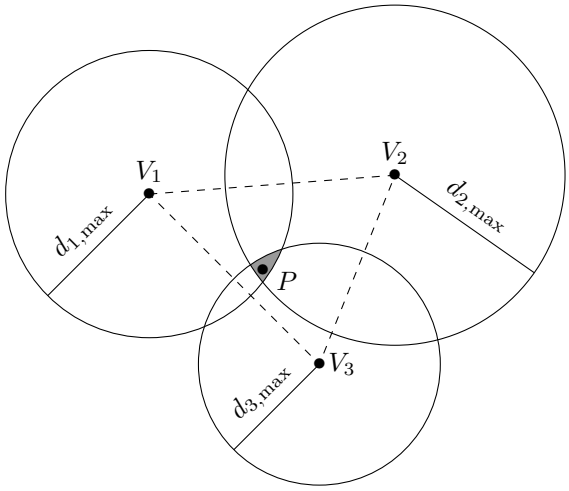


Fig. 3. Verifiable multilateration [141] where verifiers V_1, V_2 and V_3 each run the distance-bounding protocol with a prover P and can securely position P into the gray area when P is in the triangle formed by V_i.

6) V computes $m'_i = a_i \oplus b_i$ for $i = 1, \ldots, k$ and verifies that it matches with the commitment d (by opening d).
7) V verifies the signature s.
8) V accepts $d_{\max} = \max(t_i)\, c/2$ as the distance between V and P iff Steps 6 and 7 are successful.

Because b_i depends on a_i, P cannot transmit it before receiving a_i and the commitment of Steps 3 and 6 prevents P from fabricating the value of m during or after the rapid bit exchange (Step 4). Hence, the protocol prevents distance frauds [132] where P, who is at distance d from V, claims to be at distance d' such that $d' < d$ (claiming $d' > d$ is possible by delaying responses in Step 4). The signature prevents a malicious node M from impersonating P. Consequently, the protocol prevents mafia frauds [133] (a type of relay attacks), where M between P and V aims to convince V that P is closer than it is in reality.

The above protocol does not offer protection against all types of attacks. For instance, it permits a terrorist fraud, where a malicious P colludes with M to make V believe it is closer without giving its secret key to M. The protocol is also vulnerable to distance hijacking [134], where a malicious prover P takes advantage of an honest prover P' who is closer to V. However, distance-bounding protocols that are protected from (at least some of) these attacks are available (see, e.g., [134], [135], [136], [137], [138], [139]) and also reuse the basic idea of rapid bit exchange combined with cryptographic techniques such as commitments and signatures. Cryptographic distance-bounding protocols are very sensitive to processing delays because signals travel about 30 cm in one nanosecond. Accurate bounds are obtained only if transceivers and computation of the exclusive-or are very fast. Special hardware solutions are needed in practice in order to obtain the required nanosecond scale in processing delays. Surveys of distance-bounding protocols are available in [136], [140].

Secure localization gives means to a node to compute its location in a robust way in presence of malicious nodes and secure location verification allows verifying location claims

from other nodes [142]. Many schemes are available in the literature (e.g., [137], [139], [141], [142], [143], [144]) that are based on verifiable multilateration. Distance-bounding can be extended to verifiable multilateration in two (three) dimensions with cooperation of three (four) verifier nodes that know their mutual locations [141]. The principle of verifiable multilateration is shown in Fig. 3. Each verifier V_i obtains its maximum distance $d_{i,\max}$ to P by running a distance-bounding protocol placing P into the circle surrounding it. Together V_i can locate P into the intersection of the circles (the gray area in Fig. 3). The distance-bounding protocol allows P to increase any $d_{i,\max}$ by simply delaying responses in rapid bit exchange (Step 4). However, doing that makes the gray area larger and, consequently, V_i will notice the cheating attempt. In order to keep the gray area small and to successfully cheat its position, P would need to decrease $d_{i,\max}$ to at least one V_i, but this is prevented by the distance-bounding protocol. This requirement holds only in the triangle (pyramid) formed by V_i and, hence, secure localization and location verification are not possible outside the triangle (pyramid).

The simplest attacks on the above scheme are generalizations of the attacks (the frauds) on distance-bounding discussed above. We already showed above that it is not possible for a node to perform a generalization of the distance fraud and report a false location. The scheme is also protected from attacks where M impersonates either P or V_i because the two-party distance-bounding protocols will fail and from wormhole attacks where malicious nodes replicate signals from V_i to other parts of the network. The above scheme is vulnerable to more elaborated attacks where an attacker controls several malicious P [141], a malicious P takes advantage of an honest P' (location hijacking) [134], or a malicious P colludes with one or several compromised V_i. Protections against these attacks include using unclonable tamper-proof devices [141] and using different distance-bounding protocols [134]. Secure localization and location verification can be used also for improving data security of IoT more generally by introducing a location-aware security framework [145]. Surveys of secure localization can be found, e.g., from [146].

C. Secure lightweight cryptography for IoT

Although standard cryptography can be used for protecting location information in IoT as discussed in Section IV-A, implementation resources are commonly very limited for IoT devices making cryptography difficult to implement efficiently and securely. Lightweight cryptography refers to cryptographic algorithms and implementations that are designed to offer security with small implementation requirements (small circuit footprint, low power consumption, low memory requirements, etc.) [147]. These include both software running on small microcontrollers as well as dedicated integrated circuits. During the last decade or so, a lot of research has been done in lightweight cryptography. In secret-key cryptography, this includes introduction of several lightweight stream ciphers (e.g., Trivium [148], Grain [149], etc.) and block ciphers (e.g., PRESENT [150], KTAN/KTANTAN [151], SIMON/SPECK [152], etc.) together with lightweight implementations of various secret-key primitives (e.g., [153], [154], [155], [156]). In public-key cryptography, the work has focused predominately on elliptic curve cryptography [157], [158] and its lightweight implementations (e.g., [159], [160], [161], [162], [163]) because of its small key sizes and relatively low computational complexity. The results of research on lightweight cryptography can be used also for improving secure (and privacy-preserving) localization in IoT (and also for improving security of IoT more generally).

The main threats against well-designed cryptographic algorithms (including the above ones) are related to weak implementations and utilize information leakage through unintentional channels called side-channels, which are formed by different measurable characteristics of cryptographic devices [164]. To prevent these leakages, cryptographic algorithms must be implemented with special care so that they include protections against implementation attacks. Because devices in IoT are connected to the Internet, remote attacks over the network are a threat and all cryptographic implementations should have protections against them. In particular, all cryptographic software and hardware must be constant-time in order to protect against timing attacks [165], which reveal secret keys from execution time if it depends on the values of the secrets. Also attacks which require physical access to a device performing cryptographic computations (e.g., power analysis [166], electromagnetic emanation analysis [167], fault attacks [168], etc.) can be a threat. Obtaining secret keys from a device with a physical attack allows acting as the device later on (i.e. performing spoofing attacks). However, physical attacks are typically not a threat to the confidentiality of the location simply because having physical access already implies knowledge of the location of a device. However, attacks during a temporary access to a device may allow recovering its past or future locations.

D. Privacy-preserving location services

As discussed in Section IV-A, privacy against third parties (i.e., confidentiality in respect to outsiders) is relatively easy to achieve by encrypting the location information sent over the network. Techniques such as virtual private networks or Tor[1] provide location privacy in respect to the network and service provider by hiding the true origin of communication. However, they cannot provide full privacy in respect to the first node(s) that are accessed in the network because the first access node knows, e.g., that a user attaching to it via radio link is within the range of the radio. In such cases, privacy can be preserved by hiding all information that allows to identify a user, e.g., by using pseudonyms. Such solutions are used, e.g., in mobile communication systems, but their secure implementation is difficult and tracking users may still be possible in practice [169].

Privacy of the location information spans even further because often privacy in respect to LBS (a legitimate party of the communication) may be on the user's wish list. These services rely on the users' location in a fundamental way which prevents the user from obscuring his/her location and continue using the service. Good examples are real-time online

[1]The Onion Router, see www.torproject.org

map and route search services, location tracking of vehicles for taxing, road tolling, or insurance purposes, etc. This kind of LBSs have many advantages but have also raised serious concerns because they enable very accurate profiling for marketing purposes and, at least potentially, dystopian surveillance states where citizens' movements are tracked. Often the user's options are very limited: either share the location or stop using the service. IoT is expected to collect masses of data including data about our everyday movements so the problems will only grow in the future. Hence, solving the privacy issues regarding user location has significant importance and there is a clear need for privacy-preserving LBSs for IoT.

The topic of privacy-preserving LBSs spans far and has connections to general privacy-preserving (cloud) computation. Traditional anonymization techniques have largely failed to offer adequate levels of privacy (see, e.g., [170]). Hence, more elaborated techniques are required to truly protect users' privacy in the future IoT and cryptography plays a significant role in ensuring sufficient protection. Homomorphic encryption that allows computations on encrypted data offers a promise of privacy-preserving cloud computation [171]: A user can encrypt his/her data (e.g., location) and the cloud service can perform computations on it in the encrypted domain without learning the contents of the data. Unfortunately, fully homomorphic encryption [172] that allows arbitrary computations requires extensive computation making it impractical. Partially homomorphic encryption (e.g., Paillier cryptosystem [173]), which allows computations with only some operations (e.g., additions), or leveled homomorphic encryption [174], which allows arbitrary computations up to a predetermined complexity, may provide feasible solutions to some well-defined small problems.

Because there are no feasible general solutions for solving the privacy problem of LBSs, the solutions available in the literature are carefully designed for specific use cases; the following gives a few examples of solutions that rely on the use of cryptography. A method for privacy-preserving secure localization (see Section IV-B) was introduced in [175]. Solutions to privacy-preserving location tracking of vehicles were given in [176], which introduced a privacy-preserving car toll system, and [177] which presented a privacy-preserving driver's insurance. Private proximity testing for social networks, which allows persons to check if their contacts are in proximity without learning or revealing the exact locations, was presented in [178]. Because of the relatively low number of existing solutions and the urgency of the problem, designing techniques for privacy-preserving LBSs can be expected to be an active research area in the near future.

V. Legal Dimensions of Location Data Privacy

LBSs involve complex legal and policy issues. For instance, spectrum requirements and standardization, as well as privacy and data protection, must be addressed in the context of technologies and applications for location estimation, navigation and positioning. Currently existing infrastructures for the provision of geolocation services are manifold, while IoT, especially with 5G on the way, promises yet another layer thereto. Indeed, the practical room for privacy is becoming increasingly questionable as new areas of society become digitized and connected. Location privacy is one of the biggest concerns in relation to the use of mobile devices, and it involves two distinct dimensions:

- Personal data protection relating to the use of location-aware mobile devices, such as smartphones, and
- Vulnerabilities in localization related to GNSS technology and radio communications systems involving the use of jamming and spoofing devices.

These two issues require different legal treatment and instruments, although in most cases the first is given greater emphasis in considerations of location privacy in mobile devices. Indeed, compared to the approaches to location data privacy carried out under EU data protection laws, legal initiatives concerning the prevention of GNSS jamming and spoofing threats remain underdeveloped.

A. Personal data protection relating to the use of location-aware mobile devices

There is a robust legal framework and an evolving body of case law covering the area of privacy and personal data protection in Europe. First and foremost, the European Convention of Human Rights (ECHR, Art. 8) and the EU Charter of Fundamental Rights (CFR, Arts. 7, 8) safeguard privacy and data protection, while EU secondary law, alongside national laws, provides for more detailed regulation. For its part, the newly adopted General Data Protection Regulation (EU) 2016/679 (GDPR) [179] is applicable from May 2018 while the Data Protection Directive (95/46/EC) [180] applies in the meantime. The e-Privacy Directive [181] (as amended by 2009/136 EC) exists as a specific instrument regulating data protection and privacy in the electronic communications sector and is currently under reconstruction [182] alongside a wider reform of the core legal frameworks of the Digital Single Market. Cases are brought before national courts [183] as well as the European Court of Human Rights (ECtHR) [184] and the Court of Justice of the EU (CJEU) [183] .

There are various types of location data associated with geographic position, either implicitly or explicitly [185]. For instance, the location of a smart device can be identified by using different types of radio signals, such as, GNSS, GSM and WLAN [186].

Article 4 (1) of the GDPR recognizes location data as one of the 'identifiers' of personal data. This implies that such data will always be considered personal, which was previously somewhat unclear. Moreover, location data may potentially be a special category of personal data, as it can be associated with sensitive information (e.g. health-related data), thereby requiring special protection under Article 9 GDPR [186]. Location data can be collected and processed lawfully under EU data protection law (Art. 6 GDPR), for instance by securing the data subject's consent (Art. 7 GDPR) and by fulfilling privacy and human rights requirements [186]. Specific requirements, including for consenting, concern sensitive data (Art. 9 GDPR).

Article 32 of the GDPR requires data controllers or processors to employ appropriate technical and organisational measures to secure personal data (including location data) while Article 25 mandates data protection by design and by default. The principle of data protection by design and by default should be ensured from the very beginning of the development of LBS and navigation and position related services. The recommendations of the Article 29 Working Party are for LBS to be switched off by default and consent being granular and limited in time [187], [188], [189].

B. Privacy risks in an IoT environment

IoT presents a growing number of legal challenges, including privacy and trust issues. In an IoT and 'Big Data' environment, it is common that different geolocation infrastructures are combined. It is also common that data subjects disclose personal location data about themselves, but disclosure can also take place without the data subject's knowledge [189]. Furthermore, the collection of location data from multiple (sensor) devices creates unique identifiers which help IoT stakeholders identify specific individuals [190]. In such an environment, providers of LBS can gain a very comprehensive overview of users' habits and lifestyle ('profiling')[2]. Profiles, in turn, are apt to be used for decision-making that significantly affects individuals, even in a discriminatory manner. Risks imposed by the collection of location data include data theft, burglary, and even physical aggression or stalking while unauthorised access to profiling data may imply many types of conclusions to be drawn about a person [191].

In general, the lawfulness of the processing of personal (location) data on IoT is adherent to the general rules and principles of EU data protection law. The importance of certain provisions is however highlighted in IoT context. The IoT infrastructure needs to be properly secured in order to provide legal certainty for data subjects. With regard to the obligation to implement "appropriate technical and organisational measures to ensure a level of security appropriate to the risk", such measures include pseudonymisation, encryption and a process for regular testing (Art. 32 GDPR). However, devices operating on IoT are often difficult to secure. Therefore, it is important to comply with the data minimisation principle[3]. For its part, Article 82(1) of the GDPR prescribes the right to compensation for "any person who has suffered material or non-material damage as a result of an infringement of this Regulation". If security issues occur, product liability issues can also be brought against IoT stakeholders, such as app developers. The level of responsibility to the harm or damage determines liability [192].

Furthermore, the Commission has adopted a recommendation for RFID applications [COM (2009) 3200 final] [193]. According to the recommendations put forward in the document, Member States are to ensure that RFID applications apply with data protection law and the e-Privacy Directive where personal data is concerned. The industry and other stakeholders are to develop impact assessments for RFID application implementation as well as certification or self-assessment schemes for the existence of an appropriate level of information security and privacy. Furthermore, RFID applications should be transparent in their use of data and accompanied by information, including whether personal data is processed or location tracked [194].

The GDPR also explicitly includes provisions on profiling whereas its predecessor regulated automated decision-making. Not all 'profiling' falls under the scope of dedicated regulation even if it would be processing of personal data within the scope of the GDPR. According to Article 22, data subjects have "the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." Derogations include situations where such decisions are based on authorizing law or the data subject's explicit consent or where they are necessary for a contractual relation between the data subject and the controller.

Data subjects must be provided with information about personal data processed about them and the logic and means and consequences of the profiling while the controller should also ensure access to the personal data[4]. This is also indirectly required in the data quality principles in Article 5 of the GDPR. Where personal data are processed for "taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling" a data protection impact assessment is required (Art. 35 GDPR).

In an IoT and Big Data environment consenting, purpose limitation and data protection by design (esp. data minimization) are however challenged. Indeed, massive amounts of data is collected via (sensor) devices while (beneficial) future uses might still be unknown. The legal requirements must nonetheless be met. Thereby, purpose specification, identity verification and authenticating access requests become core issues to be tackled [195], [196].

C. Vulnerabilities exposed via jamming and spoofing devices

GNSS technology can be affected by intentional and illegal interference in GNSS signals through the use of GNSS jammers and spoofers. The illegal use of jamming and spoofing devices has exposed a serious threat to GPS/GNSS systems, and criminal activities may also be occurring [197].

Protection of privacy is the foremost reason for using certain civilian GPS/GNSS tracking jammers. For instance, some GPS/GNSS tracking jammers are misleadingly advertised as protecting the privacy of their users without affecting navigation devices. Nevertheless, there is a threat of illegal application when Personal or Privacy Protection Devices (PPDs) are used [197]. In fact, it is illegal to market, sell and use GNSS jammers in the EU, although it is not illegal to own them [198].

The legal issues related to GNSS jammers and spoofers are quite recent topics of discussion at the EU level, and the

[2]For a definition of profiling see art. 4 (4) of the GDPR

[3]See art. 5(1)(c) of the GDPR: Personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')".

[4]Art. 13(2)(f), 14(2)(g) and 15(1)(h), Recitals 60 and 63 of the GDPR

related legal provisions are scattered among various pieces of legislation. Jammers are mentioned in a document on the interpretation of the Radio and Telecoms Terminal Equipment Directive (R&TTE) (1999/5/EC) [199] so that the Member States are clearly against jammers being allowed among the public. This is apparent from the discussions around the R & TTE Directive as well as the Directive on Electromagnetic Compatibility (EMC) (2004/108/EC) [200] and implies the illegality of placing jammers on the market under either one of the directives. The Member States' authorities must therefore withdraw jammers from the market and notify the EU Commission [201]. Alongside, two very precise recommendations concerning the prohibition on the sale and use of jammers in CEPT member states are ECC Recommendation (04) 01 [202] and ECC Recommendation (03) 04 [203].

The legal instruments relevant in addressing the legal status of jamming and spoofing devises include 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) [204], 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) [205], the Radio Equipment Directive (RED) 2014/53/EU [206] (revising the R & TTE Directive 1999/5/EC), and 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) [207] (replacing EMC Directives 2004/108/EC).

VI. Technical and Legal Requirements and Recommendations for Trusted localization Solutions in IoT

This section summarizes the main design issues towards achieving robust privacy-preserving and/or trusted localization solutions in both GNSS and non-GNSS systems. First, in order to mitigate the threats to GNSS signals and improve the secure positioning in current IoT systems, the most suitable techniques include:

1) Using the correction parameters broadcast through the GNSS navigation message and through satellite-based or ground-based augmentation systems such as EGNOS to mitigate the system level or atmosphere interferences.
2) Applying low complexity signal processing methods to mitigate RFI and, especially, time-domain mitigation methods, e.g. the pulse blanking, etc.
3) Implementing more robust code-phase based and frequency-locked tracking loops to assist carrier-phase based and phase-locked loops, providing aiding with low-cost inertial sensors, and receiver integrity assessment and fault-detection using RAIM algorithms.

For future IoT, assuming an improvement in device battery capability, cloud-based data processing and the evolution of integrated circuit systems, implementation of vector tracking loops, tracking of modernized GNSS signals with dataless components, and processing dual-frequency signals and multiple GNSS signals may be viable options to eliminate system and ionospheric errors. In addition, more complicated and effective signal processing methods, such as techniques in transformed domains, adaptive methods, etc., will be implemented in the side of sensor node of IoT to mitigate RFI. Meanwhile, with the further development of wireless communication and cloud computing, cooperative localization and sensor integration in cloud servers will be more promising to mitigate different levels of GNSS threats to achieve security and robustness in IoT GNSS positioning.

In non-GNSS technologies based on RSS, database quality is crucial for the reliability of positioning. Statistical methods for outlier detection should be used in order to detect errors in the generated database. The threats related to malicious nodes and spoofing can be mitigated by using statistical methods, e.g., linear regression and variance analysis to identify and exclude these nodes. For privacy-preserving solutions, downlink positioning beacons could be sent for all mobile nodes in range, and trilateration methods could be employed at the mobile node based on the beacons received from several access nodes in range. Also, a random MAC address, known only by the authorized network, can increase the privacy of the positioning . In network-centric positioning methods, the client devices need to make sure that the network components are trustworthy, which requires support for authentication methods. Privacy threats related to the device location can also be mitigated using data perturbation or obfuscation methods.

The robustness and security aspects in the positioning can also be treated at the upper layer, independently of the type of positioning algorithm: GNSS or non-GNSS. For example, standard cryptographic techniques could be used for improving the security and privacy of location information in IoT. However, implementing cryptography for IoT devices is challenging because the overhead on performance and resource requirements must be kept to minimum as IoT devices are often minuscule devices. Besides, the distributed nature of IoT exposes the devices also to various types of implementation attacks which further complicates implementing secure cryptography for IoT. Fortunately, IoT can benefit from the results of secure and efficient lightweight cryptography. Techniques for robust and secure localization and location verification are also available based on existing work on WSN and RFID. The difficulty in adapting them to IoT is the requirement for special hardware solutions which are needed because cryptographic distance-bounding is very sensitive to processing delays. IoT also sets other challenges because devices are heterogeneous and do not have existing trust relationships with each others. Hence, adaptation of these techniques for IoT requires further research. Privacy of users' location information in LBS is an issue of increasing importance as more and more of peoples' sensitive location information gets recorded and stored into LBS. This issue still largely lacks sufficient solutions and can be expected to be an active topic of research in the near future.

Last but not least, there are the legal aspects to be considered towards secure and privacy-preserving localization solutions. In the issue related to privacy-preserving LBS in IoT, some stakeholders believe that the recent EU data protection legal framework is efficient enough to tackle (location) privacy

concerns in relation to the application of IoT, while others demand an advanced framework with more emphasis on privacy and data protection [208]. However, perhaps both sides are waiting for the application of the GDPR with high expectations for location privacy in the IoT environment. Despite legislative endeavours, technological development brings about many risks to location estimation. IoT environments will need to safeguard location privacy and security in order to be successful. The fundamental rights to privacy and data protection bind the modern IoT to comply with human right law requirements [209].

With regard to devices such as jammers and spoofers, intentional interference with GNSS signals has added to the legal challenges posed in the field of location and positioning security. In order to safeguard effective and secure use of GNSS services and to restrict the use and expansion of illegal devices, coordination of laws should take place in the EU. Laws need to be updated, harmonised and made clear for the general public.

By analysing the relevant provisions of existing laws, their suitability and limitations in the current situation should be analyzed in a deeper manner and new developments should be proposed to improve current policies and laws on the protection of privacy in localization and the prohibition of devices that interfere with radio communications.

VII. Conclusion

IoT has gained significant attention over the last decade. Thanks to the performance advances in small low-cost hardware technology, smart sensors are becoming pervasive. In IoT, various devices are exchanging information with each other without human interaction and computing the information intelligently. Context-awareness is a significant property of IoT and location information and LBS play important roles in such systems. Unfortunately, security and privacy aspects have often not received the attention that they deserve in designing IoT devices and systems, which has led to broad security problems, which also affect secure localization, location information, and LBS of IoT.

In this survey paper, we reviewed solutions to these problems. We first analyzed the threats and solutions to the GNSS and non-GNSS based solutions for localization. We then described certain cryptographic solutions for security and privacy of location information, localization and LBSs in IoT. Furthermore, we discussed the state-of-the-art of policy regulations regarding security of positioning solutions and legal instruments to location data privacy. We also reviewed our concerns and gave recommendations for developing more secure and privacy-preserving localization and LBSs for the future IoT. Our survey shows that many solutions are available for improving robustness, security and privacy of LBSs in IoT. Often they come with significant overheads and require specialized expertise to be implemented correctly which, arguably, are reasons why they are not included at the moment. Nevertheless, certain open problems also exist, in particular, in topics such as adapting existing solutions to the IoT framework of interconnected heterogeneous devices, secure localization in presence of powerful malicious adversaries, and privacy-preserving LBSs. We hope that this survey paper will help in focusing future research for more robust, secure, and privacy-preserving LBSs for IoT.

Acknowledgments

This work is partially supported by the "Information Security of Location Estimation and Navigation Applications (INSURE)" project funded by the Academy of Finland under the grant no. 303576.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.
[3] E. Borgia, "The internet of things vision: Key features, applications and open issues," *Computer Communications*, vol. 54, pp. 1–31, 2014.
[4] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.
[5] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414–454, 2014.
[6] Telit, "Fast-track your smart IoT device development," http://www.telit.com/sofia-3gr, accessed 4 Feb. 2017.
[7] Sirrra Wireless, https://www.sierrawireless.com/, accessed 4 Feb. 2017.
[8] Sofia, "The first middleware for smart applications," http://sofia2.com/home_en.html, accessed 4 Feb. 2017.
[9] Crystal, "Crystal - critical system engineering acceleration," http://www.crystal-artemis.eu/, accessed 4 Feb. 2017.
[10] Carriots, https://www.carriots.com/, accessed 4 Feb. 2017.
[11] Thingworx, https://www.thingworx.com/, accessed 4 Feb. 2017.
[12] V. Diggelen and F. S. Tromp, *A-GPS: Assisted GPS, GNSS, and SBAS*. Artech House, 2009.
[13] V. Lucas-Sabola, G. Seco-Granados, J. A. López-Salcedo, J. A. García-Molina, and M. Crisci, "Cloud gnss receivers: New advanced applications made possible," in *Localization and GNSS (ICL-GNSS), 2016 International Conference on*, 2016, pp. 1–6.
[14] Rohde & Schwarz, "eMTC and NB-IoT pave the way to 5G/IoT," https://www.rohde-schwarz.com/us/solutions/wireless-communications/lte/in-focus/emtc-and-nb-iot-pave-the-way-to-5g-iot_230416.html.
[15] 3GPP, "Progress on 3GPP IoT," http://www.3gpp.org/news-events/3gpp-news/1766-iot_progress, Feb. 2016.
[16] ——, "Standardization of nb-iot completed," http://www.3gpp.org/news-events/3gpp-news/1785-nb_iot_complete, June 2016.
[17] Huawei, "Huawei and partners leading nb-iot standardization," http://www.prnewswire.co.uk/news-releases/huawei-and-partners-leading-nb-iot-standardization-528516901.html, Sept 2015, retrieved 2016-02-01.
[18] LoRa Alliance, "LoRaWAN R1.0 Open Standard Released for the IoT," http://www.businesswire.com/news/home/20150616006550/en/LoRaWAN-R1.0-Open-Standard-Released-IoT, retrieved 2016-02-01.
[19] A.-L. Vogel, C. Macabiau, and N. Suard, "Effect of a GPS anomaly on different GNSS receivers," in *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005)*, Long Beach, CA, 2005, pp. pp–1645.
[20] K. V. Dyke, K. Kovach, J. Kraemer, J. Lavrakas, J. Fernow, J. Reese, N. Attallah, and B. Baevitz, "GPS Integrity Failure Modes and Effects Analysis,," in *Proceedings of the 2003 National Technical Meeting of The Institute of Navigation*, Anaheim, CA, Jan. 2003, pp. 689–703.
[21] C. Edgar, "A Cooperative Anomaly Resolution on PRN-19," in *Proceedings of the 12th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS 1999)*, Nashville, TN, Sep. 1999, pp. 2269–2268.
[22] G. Beutler, R. Dach, U. Hugentobler, O. Montenbruck, G. Weber, and E. Brockmann, "The System: GLONASS in April, What Went Wrong," *GPS World*, Jun. 2014. [Online]. Available: http://gpsworld.com/the-system-glonass-in-april-what-went-wrong/

[23] F. Blume, H. T. Berglund, I. Romero, and E. D'Anastasio, "Effects of the April 1st, 2014 GLONASS Outage on GNSS Receivers," *American Geophysical Union Fall Meeting*, Dec. 2014. [Online]. Available: http://adsabs.harvard.edu/abs/2014AGUFM.G13A0508B

[24] A. Mujunen, J. Aatrokoski, M. Tornikoski, and J. Tammi, "GPS Time Disruptions on 26-Jan-2016," Aalto University, Tech. Rep., 2016. [Online]. Available: https://aaltodoc.aalto.fi:443/handle/123456789/19833

[25] *Minimum Operational Performance Standards for Global Positioning System/Aircraft Base Augmentation System (DO-316)*, RTCA Std., Apr. 2009.

[26] European GNSS Agency, *EGNOS Safety of Life Service (SoL) Service Definition Document, issue 3.0*. European Union, 2015.

[27] *Minimum Operational Performance Standards for Global Positioning System/Wide Area Augmentation System Airborne Equipment (DO-229D)*, RTCA Std., Dec. 2006.

[28] Working Group C - ARAIM Technical Subgroup, "Milestone 3 Report," EU-U.S. Cooperation on Satellite Navigation, Tech. Rep., Feb. 2016.

[29] T. Walter, J. Blanch, M. Joerger, and B. Pervan, "Determination of fault probabilities for ARAIM," in *2016 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, Savannah, GA, Apr. 2016, pp. 451–461.

[30] C. S. Dixon, C. J. Hill, M. Dumville, and D. Lowe, "Gnss vulnerabilities: Testing the truth," *Coordinates*, March 2012.

[31] S. Bhattacharyya, *Performance and Integrity Analysis of the Vector Tracking Architecture of GNSS Receivers*. The University of Minnesota, April 2012.

[32] P. Kintner, T. Humphreys, and J. Hinks, "Gnss and ionospheric scintillation: How to survive the next solar maximum," *Inside GNSS*, vol. 4, no. 4, pp. 22–30, 2009.

[33] E. F. Danson, "Managing solar effects in gnss operations," Tech. Rep., July 2011. [Online]. Available: http://www.ee.co.za/article/danson-100-africageo-001.html

[34] M. Thomas, J. Norton, A. Jones, A. Hopper, N. Ward, P. Cannon, N. Ackroyd, P. Cruddace, and M. Unwin, "Global navigation space systems: reliance and vulnerabilities," The Royal Academy of Engineering, Tech. Rep., March 2011. [Online]. Available: http://www.raeng.org.uk/publications/reports/global-navigation-space-systems

[35] "Introduction to gps: Sources of error in gps-collected data - atmospheric interference," Warnell School of Forestry and Natural Resources, Tech. Rep. [Online]. Available: http://gps.sref.info/course/5a.html

[36] O. Isoz, *Interference in Global Positioning System Signals and its Effect on Positioning and Remote Sensing*. Kiruna, Sweden: Luleå University of Technology, May 2015.

[37] J. S. Subirana, J. J. Zornoza, and M. Hernández-Pajares, "Atmospheric effects modelling," Navipedia, Tech. Rep. [Online]. Available: http://www.navipedia.net/index.php/Atmospheric_Effects_Modelling

[38] "Global positioning system standard positioning service performance standard," US Department of Defense, Tech. Rep., September 2008, http://www.navipedia.net/index.php/Atmospheric_Effects_Modelling.

[39] R. Padullés, E. Cardellach, M. de la Torre Juárez, S. Tomás, F. J. Turk, S. Oliveras, C. O. Ao, and A. Rius, "Atmospheric polarimetric effects on gnss radio occultations: The rohp-paz field campaign," *Atmos. Chem. Phys.*, pp. 635—-649, 2016.

[40] G. MacGougan, G. Lachapelle, R. Nayak, and A. Wang, "Overview of gnss signal degradation phenomena," in *Proceedings of the International Symposium on Kinematic Systems in Geodesy, Geomatics And Navigation*, Banff, Canada, June 2001, pp. 87–100.

[41] V. Sreeja, M. Aquino, and Z. G. Elmas, "Impact of ionospheric scintillation on gnss receiver tracking performance over latin america: Introducing the concept of tracking jitter variance maps," *Space Weather*, vol. 9, no. 10, October 2011.

[42] K. S. Jacobsen and M. Dähnn, "Statistics of ionospheric disturbances and their correlation with gnss positioning errors at high latitudes," *Space Weather Space Climate*, vol. 4, no. A27, October 2014.

[43] N. Jakowski, "On developing space weather services for the end users of gnss," in *Third European Space Weather Week*, Brussels, November 2006.

[44] Y. C. Lee, "New advanced raim with improved availability for detecting constellation-wide faults, using two independent constellations," *NAVIGATION, Journal of The Institute of Navigation*, vol. 60, no. 1, pp. 71—-83, Spring 2013.

[45] E. Kaplan and C. Hegarty, *Understanding GPS: principles and applications*. Artech house, 2005.

[46] F. Dovis, *GNSS Interference Threats and Countermeasures*. Artech House, 2015.

[47] R. Landry Jr and A. Renard, "Analysis of potential interference sources and assessment of present solutions for gps/gnss receivers," 1997.

[48] C. Fernández-Prades, J. Arribas, and P. Closas, "Robust gnss receivers by array signal processing: theory and implementation," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1207–1220, 2016.

[49] D. Borio, F. Dovis, H. Kuusniemi, and L. L. Presti, "Impact and detection of gnss jammers on consumer grade satellite navigation receivers," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1233–1245, 2016.

[50] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "Gps vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, 2012.

[51] H. Kuusniemi, M. Bhuiyan, , and T. Kröger, "Signal Quality Indicators and Reliability Testing for Spoof-Resistant GNSS Receivers," *European Journal of Navigation*, vol. 11, no. 2, 2013.

[52] M. Z. H. Bhuiyan, E. Airos, H. Kuusniemi, and S. Soderholm, "The impact of interference on gnss receiver observables–a running digital sum based simple jammer detector," *Radioengineering*, 2014.

[53] L. Musumeci and F. Dovis, "Use of the Wavelet Transform for Interference Detection and Mitigation in Global Navigation Satellite Systems," *International Journal of Navigation and Observation*, vol. 2014, 2014.

[54] N. Fadaei, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "Detection, Characterization and Mitigation of GNSS Jammers Using Windowed-HHT," in *Proceedings of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2015)*, 2015, pp. 1625–1633.

[55] F. Dovis and L. Musumeci, "Use of the Karhunen-Loève Transform for interference detection and mitigation in GNSS," *ICT Express*, vol. 2, no. 1, pp. 33–36, 2016.

[56] D. Borio, C. O'Driscoll, and J. Fortuny, "GNSS jammers: Effects and countermeasures," in *2012 6th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing, (NAVITEC)*, 2012, pp. 1–7.

[57] D. Borio, "A multi-state notch filter for GNSS jamming mitigation," in *International Conference on Localization and GNSS 2014 (ICL-GNSS 2014)*, 2014, pp. 1–6.

[58] ——, "Swept GNSS jamming mitigation through pulse blanking," in *European Navigation Conference (ENC), 2016*, 2016, pp. 1–8.

[59] A. Jafarnia-Jahromi, T. Lin, A. Broumandan, and J. N. G. Lachapelle, "Detection and Mitigation of Spoofing Attacks on a Vector Based Tracking GPS Receiver," in *Proceedings of the 2012 International Technical Meeting of The Institute of Navigation*, 2012, pp. 790–800.

[60] K. Ali, E. G. Manfredini, and F. Dovis, "Vestigial signal defense through signal quality monitoring techniques based on joint use of two metrics," in *2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014*. IEEE, 2014, pp. 1240–1247.

[61] C. E. McDowell, "GPS Spoofer and Repeater Mitigation System using Digital Spatial Nulling," 2007, uS Patent 7,250,903.

[62] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A GNSS Structural Interference Mitigation Technique using Antenna Array Processing," in *2014 IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM)*. IEEE, 2014, pp. 109–112.

[63] M. Kirkko-Jaakkola, L. Ruotsalainen, M. Z. H. Bhuiyan, S. Söderholm, S. Thombre, and H. Kuusniemi, "Performance of a MEMS IMU Deeply Coupled with a GNSS Receiver under Jamming," in *Ubiquitous Positioning Indoor Navigation and Location Based Service (UPINLBS), 2014*. IEEE, 2014, pp. 64–70.

[64] L. Ruotsalainen, "Visual Gyroscope and Odometer for Pedestrian Indoor Navigation with a Smartphone," Ph.D. Thesis, Tampere University of Technology, 2013.

[65] L. Ruotsalainen, M. Kirkko-Jaakkola, M. Bhuiyan, S. Söderholm, S. Thombre, and H. Kuusniemi, "Deeply-coupled GNSS, INS and visual sensor integration for interference mitigation," in *Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2014)*, 2014, pp. 2243–2249.

[66] R. Bauernfeind, T. Kraus, A. S. Ayaz, D. Dotterbock, and B. Eissfeller, *Analysis, Detection and Mitigation of incar GNSS Jammer Interference in Intelligent Transport Systems*. Deutsche Gesellschaft für Luft-und Raumfahrt-Lilienthal-Oberth eV, 2013.

[67] E. Domínguez, A. Pousinho, P. Boto, D. Gómez-Casco, S. Locubiche-Serra, G. Seco-Granados, J. A. López-Salcedo, F. Z. H. Fragner, O. Peña, and D. Jiménez-Baños, "Performance evaluation of high

sensitivity gnss techniques in indoor, urban and space environments," in *Proc. of ION GNSS+*, Portland, OR, U.S.A., September 2016.

[68] J. Dampf and T. Pany, "Measuring high bandwidth gnss signals for indoor positioning," *Inside GNSS*, pp. 76–80, September 2013.

[69] N. Samama, "Indoor positioning with gnss-like local signal transmitters," *Global Navigation Satellite Systems—Signal, Theory and Applications*, pp. 299–338, 2012.

[70] A. Puengnim, L. Patino-Studencka, J. Thielecke, and G. Rohmer, "Precise positioning for virtually synchronized pseudolite system," in *Indoor Positioning and Indoor Navigation (IPIN), 2013 International Conference on*, 2013, pp. 1–8.

[71] H. Kuusniemi, M. Z. H. Bhuiyan, M. Ström, S. Söderholm, T. Jokitalo, L. Chen, and R. Chen, "Utilizing pulsed pseudolites and high-sensitivity gnss for ubiquitous outdoor/indoor satellite navigation," in *Indoor Positioning and Indoor Navigation (IPIN), 2012 International Conference on*, 2012, pp. 1–7.

[72] G. Falco, G.and Einicke, J. Malos, and F. Dovis, "Performance analysis of constrained loosely coupled GPS/INS integration solutions," *Sensors*, vol. 12, pp. 15 983–16 007, 2012.

[73] J. Collin, *Investigations of self-contained sensors for personal navigation*. Tampere University of Technology, 2006.

[74] S. E. Langel, M. Samer, F.-C. Chan, and B. S. Pervan, "Tightly coupled gps/ins integration for differential carrier phase navigation systems using decentralized estimation," in *Position Location and Navigation Symposium (PLANS), 2010 IEEE/ION*, 2010, pp. 397–409.

[75] M. Petovello and G. Lachapelle, "Comparison of vector-based software receiver implementations with application to ultra-tight gps/ins integration," in *Proceedings of ION GNSS*, vol. 6, 2006.

[76] L. Chen, Y. Li, and C. Rizos, "Stability analysis of tracking weak GPS signals through non-coherent ultra-tight GPS/INS integration," in *Proc. of Indoor Positioning and Indoor Navigation (IPIN)*, Sydney, Australia, September 2012.

[77] J. W. Kim, D.-H. Hwang, and S. J. Lee, "A deeply coupled gps/ins integrated kalman filter design using a linearized correlator output," in *Position, Location, And Navigation Symposium, 2006 IEEE/ION*, 2006, pp. 300–305.

[78] D. Serant, D. Kubrak, M. Monnerat, G. Artaud, and L. Ries, "Field test performance assessment of gnss/ins ultra-tight coupling scheme targeted to mass-market applications," in *Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing,(NAVITEC), 2012 6th ESA Workshop on*, 2012, pp. 1–8.

[79] M. Langer and G. F. Trommer, "Multi gnss constellation deeply coupled gnss/ins integration for automotive application using a software defined gnss receiver," in *Position, Location and Navigation Symposium-PLANS 2014, 2014 IEEE/ION*, 2014, pp. 1105–1112.

[80] S. Kennedy and J. Rossi, "Performance of a deeply coupled commercial grade gps/ins sytem from KVH and NovAtel Inc," in *Proc. of ION GNSS+*, Portland, OR, U.S.A., September 2016.

[81] P. D. Groves, "Shadow matching: A new GNSS positioning technique for urban canyons," *Journal of Navigation*, vol. 64, pp. 417–430, 2011.

[82] P. D. Groves and M. Adjrad, "Intelligent urban positioning using shadow matching and gnss ranging aided by 3d mapping," in *Proc. of ION GNSS+*, Portland, OR, U.S.A., September 2016.

[83] Q. Li, W. Li, W. Sun, J. Li, and Z. Liu, "Fingerprint and assistant nodes based Wi-Fi localization in complex indoor environment," *IEEE Access*, vol. 4, pp. 2993–3004, 2016.

[84] B. Wang, Q. Chen, L. T. Yang, and H. C. Chao, "Indoor smartphone localization via fingerprint crowdsourcing: challenges and approaches," *IEEE Wireless Communications*, vol. 23, no. 3, pp. 82–89, June 2016.

[85] A. Zanella, "Best practice in rss measurements and ranging," *IEEE Communications Surveys Tutorials*, vol. 18, no. 4, pp. 2662–2686, Fourthquarter 2016.

[86] K. Lin, M. Chen, J. Deng, M. M. Hassan, and G. Fortino, "Enhanced fingerprinting and trajectory prediction for IoT localization in smart buildings," *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1294–1307, July 2016.

[87] I. Sharp and K. Yu, "Improved indoor range measurements at various signal bandwidths," *IEEE Transactions on Instrumentation and Measurement*, vol. 65, no. 6, pp. 1364–1373, June 2016.

[88] A. A. Adebomehin and S. D. Walker, "Enhanced ultrawideband methods for 5G LOS sufficient positioning and mitigation," in *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, June 2016, pp. 1–4.

[89] A. Shahmansoori, G. E. Garcia, G. Destino, G. Seco-Granados, and H. Wymeersch, "5G position and orientation estimation through millimeter wave MIMO," in *2015 IEEE Globecom Workshops (GC Wkshps)*, Dec 2015, pp. 1–6.

[90] K. Radnosrati, F. Gunnarsson, and F. Gustafsson, "New trends in radio network positioning," in *2015 18th International Conference on Information Fusion (Fusion)*, July 2015, pp. 492–498.

[91] X. Du and K. Yang, "A map-assisted wifi ap placement algorithm enabling mobile device's indoor positioning," *IEEE Systems Journal*, vol. PP, no. 99, pp. 1–9, 2016.

[92] Y. Zhuang, Z. Syed, Y. Li, and N. El-Sheimy, "Evaluation of two wifi positioning systems based on autonomous crowdsourcing of handheld devices for indoor navigation," *IEEE Transactions on Mobile Computing*, vol. 15, no. 8, pp. 1982–1995, Aug 2016.

[93] P. Davidson and R. Piche, "A survey of selected indoor positioning methods for smartphones," *IEEE Communications Surveys Tutorials*, vol. PP, no. 99, pp. 1–1, 2016.

[94] R. Faragher and R. Harle, "Location fingerprinting with bluetooth low energy beacons," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 11, pp. 2418–2428, Nov 2015.

[95] L. Chen, L. Pei, H. Kuusniemi, Y. Chen, T. Kröger, and R. Chen, "Bayesian fusion for indoor positioning using bluetooth fingerprints," *Wireless personal communications*, vol. 70, no. 4, pp. 1735–1745, 2013.

[96] M. Cremer, U. Dettmar, C. Hudasch, R. Kronberger, R. Lerche, and A. Pervez, "Localization of passive UHF RFID tags using the AoAct transmitter beamforming technique," *IEEE Sensors Journal*, vol. 16, no. 6, pp. 1762–1771, March 2016.

[97] L. Chen, O. Julien, P. Thevenon, D. Serant, A. G. Peña, and H. Kuusniemi, "Toa estimation for positioning with dvb-t signals in outdoor static tests," *IEEE Transactions on Broadcasting*, vol. 61, no. 4, pp. 625–638, 2015.

[98] L. Chen, P. Thevenon, G. Seco-Granados, O. Julien, and H. Kuusniemi, "Analysis on the toa tracking with dvb-t signals for positioning," *IEEE Transactions on Broadcasting*, vol. 62, no. 4, pp. 957–961, 2016.

[99] P. Müller, H. Wymeersch, and R. Piché, "UWB positioning with generalized gaussian mixture filters," *IEEE Transactions on Mobile Computing*, vol. 13, no. 10, pp. 2406–2414, Oct 2014.

[100] S. Han, Z. Gong, W. Meng, C. Li, D. Zhang, and W. Tang, "Automatic precision control positioning for wireless sensor network," *IEEE Sensors Journal*, vol. 16, no. 7, pp. 2140–2150, April 2016.

[101] A. Kotanen, M. Hannikainen, H. Leppakoski, and T. D. Hamalainen, "Experiments on local positioning with bluetooth," in *Proceedings ITCC 2003. International Conference on Information Technology: Coding and Computing*, April 2003, pp. 297–303.

[102] C. di Flora and M. Hermersdorf, "A practical implementation of indoor location-based services using simple WiFi positioning," *Journal of Location Based Services*, vol. 2, no. 2, pp. 87–111, 2008. [Online]. Available: http://dx.doi.org/10.1080/17489720802415205

[103] L. Koski, R. Piché, V. Kaseva, S. Ali-Löytty, and M. Hännikäinen, "Positioning with coverage area estimates generated from location fingerprints," in *2010 7th Workshop on Positioning, Navigation and Communication*, March 2010, pp. 99–106.

[104] P. Bahl and V. N. Padmanabhan, "Radar: an in-building RF-based user location and tracking system," in *Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No.00CH37064)*, vol. 2, 2000, pp. 775–784 vol.2.

[105] T. Roos, P. Myllymäki, H. Tirri, P. Misikangas, and J. Sievänen, "A probabilistic approach to WLAN user location estimation," *International Journal of Wireless Information Networks*, vol. 9, no. 3, pp. 155–164, 2002. [Online]. Available: http://dx.doi.org/10.1023/A:1016003126882

[106] H. Wang, H. Lenz, A. Szabo, J. Bamberger, and U. D. Hanebeck, *Enhancing the Map Usage for Indoor Location-Aware Systems*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 151–160.

[107] S. Nambiar, A. Nikolaev, M. Greene, L. Cavuoto, and A. Bisantz, "Low-cost sensor system design for in-home physical activity tracking," *IEEE Journal of Translational Engineering in Health and Medicine*, vol. 4, pp. 1–6, 2016.

[108] J. Gozalvez, "New 3GPP standard for IoT [mobile radio]," *IEEE Vehicular Technology Magazine*, vol. 11, no. 1, pp. 14–20, March 2016.

[109] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Communications Surveys Tutorials*, vol. PP, no. 99, pp. 1–1, 2017.

[110] J. W. Qiu and Y. C. Tseng, "M2M encountering: Collaborative localization via instant inter-particle filter data fusion," *IEEE Sensors Journal*, vol. 16, no. 14, pp. 5715–5724, July 2016.

[111] M. Gupta, J. Gao, C. C. Aggarwal, and J. Han, "Outlier detection for temporal data: A survey," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 9, pp. 2250–2267, Sept 2014.

[112] W. Meng, W. Xiao, W. Ni, and L. Xie, "Secure and robust Wi-Fi fingerprinting indoor localization," in *2011 International Conference on Indoor Positioning and Indoor Navigation*, Sept 2011, pp. 1–7.

[113] Y. Kim, H. Shin, Y. Chon, and H. Cha, "Crowdsensing-based Wi-Fi radio map management using a lightweight site survey," *Computer Communications*, vol. 60, pp. 86 – 96, 2015. [Online]. Available: //www.sciencedirect.com/science/article/pii/S014036641400365X

[114] Y.-C. Chen and J.-C. Juang, "Outlier-detection-based indoor localization system for wireless sensor networks," *International Journal of Navigation and Observation*, pp. 1 – 9, 2012.

[115] A. Khalajmehrabadi, N. Gatsis, D. Pack, and D. Akopian, "A joint indoor WLAN localization and outlier detection scheme using LASSO and Elastic-Net optimization techniques," *IEEE Transactions on Mobile Computing*, vol. PP, no. 99, pp. 1–1, 2016.

[116] Y. Chen, W. Trappe, and R. P. Martin, "ADLS: Attack detection for wireless localization using least squares," in *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth Annual IEEE International Conference on*, March 2007, pp. 610–613.

[117] K. Penna, V. Yalavarthi, H. Fu, and Y. Zhu, "Evaluation of active position detection in vehicular Ad Hoc networks," in *2014 International Joint Conference on Neural Networks (IJCNN)*, July 2014, pp. 2234–2239.

[118] R. Varghese, T. Chithralekha, and C. Kharkongor, "Self-organized cluster based energy efficient meta trust model for internet of things," in *2016 IEEE International Conference on Engineering and Technology (ICETECH)*, March 2016, pp. 382–389.

[119] A. A. A. Silva, E. Pontes, A. E. Guelfi, I. Caproni, R. Aguiar, F. Zhou, and S. T. Kofuji, "Predicting model for identifying the malicious activity of nodes in manets," in *2015 IEEE Symposium on Computers and Communication (ISCC)*, July 2015, pp. 700–707.

[120] S. Taha and X. Shen, "A physical-layer location privacy-preserving scheme for mobile public hotspots in NEMO-based VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 4, pp. 1665–1680, Dec 2013.

[121] L. Ou, Z. Qin, Y. Liu, H. Yin, Y. Hu, and H. Chen, "Multi-user location correlation protection with differential privacy," in *2016 IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS)*, Dec 2016, pp. 422–429.

[122] P. I. Han and H. P. Tsai, "SST: privacy preserving for semantic trajectories," in *2015 16th IEEE International Conference on Mobile Data Management*, vol. 2, June 2015, pp. 80–85.

[123] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp. 1746–1759, Aug 2014.

[124] L. Lazos and M. Krunz, "Selective jamming/dropping insider attacks in wireless mesh networks," *IEEE Network*, vol. 25, no. 1, pp. 30–34, January 2011.

[125] A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Secure localization algorithms for wireless sensor networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 96–101, 2008.

[126] National Institute of Standards and Technology (NIST), "Secure hash standard (SHS)," FIPS PUB 180-4, 2015. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[127] ——, "The keyed-hash message authentication code (HMAC)," FIPS PUB 198-1, 2008. [Online]. Available: http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

[128] ——, "Digital signature standard (DSS)," FIPS PUB 186-4, 2013. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[129] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[130] National Institute of Standards and Technology (NIST), "Advanced encryption standard (AES)," FIPS PUB 197, 2001. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[131] ——, "Recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC," NIST Special Publication 800-38D, 2007. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

[132] S. Brands and D. Chaum, "Distance-bounding protocols," in *Advances in Cryptology — EUROCRYPT 1993*, ser. LNCS, vol. 765. Springer, 1994, pp. 344–359.

[133] Y. Desmedt, "Major security problems with the 'unforgeable'(feige)-fiat-shamir proofs of identity and how to overcome them," in *Proceedings of the 6th Worldwide Congress on Computer and Communications Security and Protection (SecuriCom)*, vol. 88, 1988, pp. 147–159.

[134] C. Cremers, K. B. Rasmussen, B. Schmidt, and S. Čapkun, "Distance hijacking attacks on distance bounding protocols," in *Proceedings of the 2012 IEEE Symposium on Security and Privacy (IEEE S&P 2012)*, 2012, pp. 113–127.

[135] G. Avoine, C. Lauradoux, and B. Martin, "How secret-sharing can defeat terrorist fraud," in *Proceedings of the 4th ACM Conference on Wireless Network Security (WiSec '11)*. ACM, 2011, pp. 145–156.

[136] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "Towards secure distance bounding," in *Fast Software Encryption — FSE 2013*, ser. LNCS, vol. 8424. Springer, 2014, pp. 55–67.

[137] S. Čapkun, L. Buttyán, and J.-P. Hubaux, "SECTOR: Secure tracking of node encounters in multi-hop wireless networks," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03)*. ACM, 2003, pp. 21–32.

[138] C. H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, and O. Pereira, "The swiss-knife RFID distance bounding protocol," in *Information Security and Cryptology — ICISC 2008*, ser. LNCS, vol. 5461. Springer, 2009, pp. 98–115.

[139] D. Singelee and B. Preneel, "Location verification using secure distance bounding protocols," in *Proceedings of the 2005 IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*. IEEE, 2005.

[140] A. Abu-Mahfouz and G. P. Hancke, "Distance bounding: A practical security solution for real-time location systems," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 16–27, 2013.

[141] S. Čapkun and J.-P. Hubaux, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, 2006.

[142] L. Lazos, R. Poovendran, and S. Čapkun, "ROPE: Robust position estimation in wireless sensor networks," in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05)*. IEEE, 2005, art. no. 43.

[143] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proceedings of the 2nd ACM workshop on Wireless security (WiSe '03)*. ACM, 2003.

[144] Y. Wei and Y. Guan, "Lightweight location verification algorithms for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 5, pp. 938–950, 2013.

[145] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing location-aware end-to-end data security in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 5, pp. 585–598, 2008.

[146] Y. Zeng, J. Cao, J. Hong, S. Zhang, and L. Xie, "Secure localization and location verification in wireless sensor networks: A survey," *Journal of Supercomputing*, vol. 64, no. 3, pp. 685–701, 2013.

[147] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," *IEEE Design & Test of Computers*, vol. 24, pp. 522–533, 2007.

[148] C. De Cannière, "Trivium: A stream cipher construction inspired by block cipher design principles," in *Proceedings of the 9th International Conference on Information Security (ISC 2006)*, ser. LNCS, vol. 4176. Springer, 2006, pp. 171–186.

[149] M. Hell, T. Johansson, and W. Meier, "Grain: a stream cipher for constrained environments," *International Journal of Wireless and Mobile Computing*, vol. 2, no. 1, pp. 86–93, 2007.

[150] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," in *Cryptographic Hardware and Embedded Systems — CHES 2007*, ser. LNCS, vol. 4727. Springer, 2007, pp. 450–466.

[151] C. De Cannière, O. Dunkelman, and M. Knežević, "KATAN and KTANTAN — a family of small and efficient hardware-oriented block ciphers," in *Cryptographic Hardware and Embedded Systems — CHES 2009*, ser. LNCS, vol. 5747. Springer, 2009, pp. 272–288.

[152] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK families of lightweight block ciphers," Cryptology ePrint Archive, Report 2013/404, 2013. [Online]. Available: http://eprint.iacr.org/2013/404

[153] P. Hämäläinen, T. Alho, M. Hännikäinen, and T. D. Hämäläinen, "Design and implementation of low-area and low-power AES encryption hardware core," in *Proceedings of the 9th EUROMICRO Conference on Digital System Design (DSD'06)*, 2006, pp. 577–583.

[154] C. Rolfes, A. Poschmann, G. Leander, and C. Paar, "Ultra-lightweight implementations for smart devices – security for 1000 gate equivalents," in *Proceedings of the 8th International Conference on Smart Card Research and Advanced Applications (CARDIS 2008)*, ser. LNCS, vol. 5189. Springer, 2008, pp. 89–103.

[155] A. Y. Poschmann, "Lightweight cryptography: Cryptographic engineering for a pervasive world," Ph.D. dissertation, Ruhr University Bochum, 2009.

[156] T. Eisenbarth, Z. Gong, T. Güneysu, S. Heyse, S. Indesteege, S. Kerckhof, F. Koeune, T. Nad, T. Plos, F. Regazzoni, F.-X. Standaert, and L. van Oldeneel tot Oldenzeel, "Compact implementation and performance evaluation of block ciphers in ATtiny devices," in *Progress in Cryptology — AFRICACRYPT 2012*, ser. LNCS, vol. 7374. Springer, 2012, pp. 172–187.

[157] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[158] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology — CRYPTO '85*, ser. LNCS, vol. 218. Springer, 1986, pp. 417–426.

[159] Y. K. Lee, K. Sakiyama, L. Batina, and I. Verbauwhede, "Elliptic-curve-based security processor for RFID," *IEEE Transactions on Computers*, vol. 57, no. 11, pp. 1514–1527, 2008.

[160] Z. Liu, E. Wenger, and J. Großschädl, "MoTE-ECC: Energy-scalable elliptic curve cryptography for wireless sensor networks," in *Proceedings of the 12th International Conference on Applied Cryptography and Network Security (ACNS 2014)*, ser. LNCS, vol. 8479. Springer, 2014, pp. 361–379.

[161] R. De Clercq, L. Uhsadel, A. Van Herrewege, and I. Verbauwhede, "Ultra low-power implementation of ECC on the ARM Cortex-M0+," in *Proceedings of the 51st Annual Design Automation Conference (DAC 2014)*. ACM, 2014, pp. 1–6.

[162] P. Pessl and M. Hutter, "Curved tags – a low-resource ECDSA implementation tailored for RFID," in *Revised Selected Papers of the 10th International Workshop on Radio Frequency Identification: Security and Privacy Issues (RFIDSec 2014)*, ser. LNCS, vol. 8651. Springer, 2014, pp. 156–172.

[163] S. Sinha Roy, K. Järvinen, and I. Verbauwhede, "Lightweight coprocessor for Koblitz curves: 283-bit ECC including scalar conversion with only 4300 gates," in *Cryptographic Hardware and Embedded Systems – CHES 2015*, ser. LNCS, vol. 9293. Springer, 2015, pp. 102–122.

[164] Y. B. Zhou and D. G. Feng, "Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing," IACR ePrint Archive, Report 2005/388, 2005.

[165] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Advanced in Cryptology — CRYPTO '96*, ser. LNCS, vol. 1109. Springer, 1996, pp. 104–113.

[166] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptography—CRYPTO'99*, ser. LNCS, vol. 1666. Springer, 1999, pp. 388–397.

[167] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side-channel(s)," in *Cryptographic Hardware and Embedded Systems—CHES'02*, ser. LNCS, vol. 2523. Springer, 2002, pp. 29–45.

[168] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, "The sorcerer's apprentice guide to fault attacks," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 370–382, 2006.

[169] A. Shaik, J.-P. Seifert, R. Borgaonkar, N. Asokan, and V. Niemi, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems," in *Proceedings of the 23nd Annual Network and Distributed System Security Symposium (NDSS 2016)*. The Internet Society, 2016.

[170] P. Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization," *UCLA Law Review*, vol. 57, pp. 1701–1777, 2010.

[171] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of Secure Computation*, vol. 4, no. 11, pp. 169–180, 1978.

[172] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the 41st ACM Symposium on Theory of Computing (STOC 2009)*. ACM, 2010, pp. 169–178.

[173] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology — EUROCRYPT 1999*, ser. LNCS, vol. 1592. Springer, 1999, pp. 223–238.

[174] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(leveled) fully homomorphic encryption without bootstrapping," *ACM Transactions on Computation Theory*, vol. 6, no. 3, pp. 13:1–13:36, Jul. 2014.

[175] T. Shu, Y. Chen, J. Yang, and A. Williams, "Multi-lateral privacy-preserving localization in pervasive environments," in *Proceedings of the 2014 IEEE Conference on Computer Communications (INFOCOM 2014)*. IEEE, 2014, pp. 2319–2327.

[176] J. Balasch, A. Rial, C. Troncoso, B. Preneel, I. Verbauwhede, and C. Geuens, "PrETP: Privacy-preserving electronic toll pricing," in *Proceedings of 2010 USENIX Security Symposium*, 2010, pp. 63–78.

[177] C. Troncoso, G. Danezis, E. Kosta, J. Balasch, and B. Preneel, "PriPAYD: Privacy-friendly pay-as-you-drive insurance," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 5, pp. 742–755, 2011.

[178] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location privacy via private proximity testing," in *Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS 2011)*. The Internet Society, 2011.

[179] European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation)," May 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

[180] ——, "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," October 1995, http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

[181] ——, "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 (Directive on privacy and electronic communications)," July 2002, http://eur-lex.europa.eu/eli/dir/2002/58/oj.

[182] European Commission, "Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing directive 2002/58/EC (Regulation on Privacy and Electronic Communications)," January 2017, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN.

[183] "Google Spain et al. v AEDP, Costeja Gonzales, C-131/12 (CJEU) ECLI:EU:C:2014:317," May 2014.

[184] "Uzun v Germany, App no 35623/05, IHRL 1838 (ECtHR)," September 2010.

[185] P. Barrett, A. Berrill, and et al., "Location Data Privacy Guidelines, Assessments and Recommendations ," May 2013, https://iapp.org/media/pdf/resource_center/LocationDataPrivacyGuidelines_v2.pdf.

[186] S. Bu-Pasha, A. Alén-Savikko, J. Mäkinen, R. Guinness, and P. Korpisaari, "EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency," *European Data Protection Law Review*, vol. 2, no. 3, pp. 312–323, 2016.

[187] European Commission, "Fifteenth annual report of the article 29 working party on data protection (adopted on 3.12.2013)," December 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/annual-report/files/2013/15th_annual_report_en.pdf.

[188] ——, "Working party 29 opinion on the use of location data with a view to providing value-added services," November 2005, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf.

[189] European Commission, Article 29 Data Protection Working Party, "Opinion 13/2011 on Geolocation services on smart mobile devices ," May 2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf.

[190] ——, "Opinion 8/2014 on the on Recent Developments on the Internet of Things," September 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

[191] P. D. Hert and S. Gutwirth, "Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location-based services and virtual residence," pp. 111–162, July 2003, http://www.europarl.europa.eu/stoa/webdav/shared/3_activities/privacy/general/ipts_security_citizen_en.pdf.

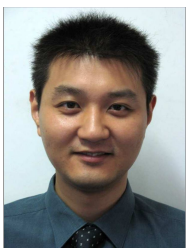
[192] M.-H. Maras, "Tomorrow's privacy internet of things: security and privacy implication," *International Data Privacy Law*, vol. 5, no. 2, pp. 99–104, May 2015.

[193] European Commission, "Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio frequency identification," May 2009, http://ec.europa.eu/smart-regulation/impact/ia_carried_out/docs/ia_2009/c_2009_3200_en.pdf.

[194] R. H. Weber, "Internet of things–new security and privacy challenges," *Computer law & security review*, vol. 26, no. 1, pp. 23–30, 2010.

[195] M. Paez and M. La Marca, "The internet of things: Emerging legal issues for businesses," *N. Ky. L. Rev.*, vol. 43, pp. 29–71, 2016.

[196] A. Cavoukian, "Evolving FIPPs: Proactive Approaches to Privacy, Not Privacy Paternalism," in *Reforming European Data Protection Law*. Springer, 2015, pp. 293–309.
[197] A. Ruegamer and D. Kowalewski, "Jamming and spoofing of GNSS signals–an underestimated risk?!" *the Wisdom of the Ages to the Challenges of the Modern World Sofia, Bulgaria*, pp. 17–21, 2015.
[198] European GNSS Agency, "GNSS User Technology Report," 2016, https://www.gsa.europa.eu/system/files/reports/gnss_user_technology_report_webb.pdf.
[199] European Union, "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," March 1999, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:1999:091:TOC.
[200] Council of European Union , "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 Text with EEA relevance," December 2004, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2004:390:TOC.
[201] European Commission, "Interpretation of the Directive 1999/5/EC," 1999, http://ec.europa.eu/DocsRoom/documents/9903/attachments/1/translations.
[202] Electronic Communications Committee , "ECC Recommendation (04)01: With regard to forbidding the placing on the market and use of jammers in the CEPT member countries," May 2016, http://www.erodocdb.dk/docs/doc98/official/pdf/Rec0401.pdf.
[203] ——, "ECC Recommendation (03)04: With regard to forbidding the placing on the market and use of jammers in the CEPT member countries," 2016, http://www.erodocdb.dk/docs/doc98/official/pdf/Rec0304.pdf.
[204] European Union, "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," November 2011, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011D1104.
[205] ——, "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)," April 2002, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002D0676.
[206] ——, "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," May 2014, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014L0053.
[207] ——, "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) Text with EEA relevance," March 2014, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0030.
[208] European Commission , "Report on the public consultation on IoT governance," January 2013, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1746.
[209] ——, "IoT privacy, data protection, information security," http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753.



Liang Chen is a Senior Research Scientist in the Department of Navigation and Positioning at the Finnish Geospatial Research Institute (FGI), Finland. Before he joined in FGI, he worked in the Department of Mathematics at Tampere University of Technology, Finland from 2009 to 2011. He received his PhD in Signal and Information Processing from Southeast University, China, in 2009. He has authored or co-authored over 60 publications related to statistical signal processing for positioning, wireless positioning using signals of opportunity and sensor fusion algorithm for indoor positioning.

Sarang Thombre is a Specialist Research Scientist at the Department of Navigation and Positioning (N&P) of FGI. He received his Ph.D. degree in 2014 from Tampere University of Technology (TUT), Finland. He is an External Project Reviewer for the European GNSS Agency within the Horizon2020 Galileo programme, and a member of the Board of the Nordic Institute of Navigation. He has authored or co-authored over 35 publications related to multi-GNSS, multi-frequency receiver implementation and performance validation, interference detection, and maritime situational awareness.

Kimmo Järvinen received the M.Sc. (Tech.) degree in 2003 and the D.Sc. (Tech.) degree in 2008, both from Helsinki University of Technology (TKK), Finland. He was with Signal Processing Laboratory at TKK from 2002 to 2008. In 2008-2013 and again in 2015-2016, he was a postdoctoral researcher in Department of (Information and) Computer Science, Aalto University, Finland. From 2014 to 2015, he was with the COSIC group of KU Leuven ESAT, Belgium. Since Nov. 2016, he is a senior researcher in Department of Computer Science, University of Helsinki, Finland. His research interests lie in the domains of security and cryptography and, especially, in developing efficient and secure implementations of cryptosystems. He has (co-)authored more than 40 peer-reviewed scientific publications.

Elena Simona Lohan received a M.Sc. degree from Polytechnics University of Bucharest (1997), a D.E.A. degree at Ecole Polytechnique, Paris (1998), and a Ph.D. degree in wireless communications from Tampere University of Technology (2003). She is now an Associate Professor at TUT and has been a Visiting Professor at Universitat Autonoma de Barcelona since 2012. She is the group leader for the signal processing for wireless positioning group at TUT. Her current research interests include wireless location techniques based on Signals of Oportunity, wireless navigation receiver architectures and multipath mitigation, and cognitive, privacy and security aspects related to user positioning.

Anette Alén-Savikko is a postdoctoral researcher at the Faculty of Law, University of Helsinki and University of Lapland, as well as a visiting researcher at Aalto University. Her research covers new media, digitization, intellectual property (IP) and data protection while she is particularly interested in EU law dimensions thereof. Anette has published and been involved in numerous projects in the fields of media law, IP and data protection law with her research interests currently including also human centered models of personal data management. In addition, Anette has provided national expertise with regard to her areas of interest.

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

M. Zahidul H. Bhuiyan received Ph.D. degree in 2011 from the Department of Electronics and Communications Engineering, Tampere University of Technology, Finland. Dr. Bhuiyan is now working as a Research Manager at the Department of Navigation and Positioning in the Finnish Geospatial Research Institute. Since 2014, he is also acting as the deputy head of the Satellite and Radio Navigation research group of the institute. His main research interests include various aspects of multi-GNSS receiver design, GNSS vulnerabilities identification and mitigation, sensor fusion algorithms for seamless outdoor/indoor positioning, Differential GNSS, SBAS performance monitoring, etc. He has also been actively involved in teaching GNSS related courses in Aalto University, Tampere University of Technology and in other GNSS training schools.

Shakila Bu-Pasha is a doctoral researcher at the Faculty of Law, University of Helsinki. She completed her second Master's degree from Faculty of Law, University of Turku on Law and Information Society. Her research covers communication law and data protection with keen focus on personal data protection under EU law.

Giorgia Nunzia Ferrara is a Research Scientist at the Department of Navigation and Positioning of the Finnish Geospatial Research Institute (FGI), Finland. She obtained her M.Sc. degree in telecommunications engineering from the University of Catania, Italy. Before joining FGI, from 2014 to 2016, she worked in the Department of Electronics and Communications Engineering at Tampere University of Technology, where she is currently enrolled as Ph.D student. Her research interests are mainly in the areas of multi-GNSS receiver implementation, and interference detection and mitigation.

Salomon Honkala is a Research Scientist at the Department of N&P at FGI. He received his M.Sc. (Tech.) degree in electrical engineering from Aalto University, Finland in 2016. His research interests include software GNSS receiver design, GNSS vulnerabilities, interference mitigation, and GNSS timing robustness.

Jenna Lindqvist is a doctoral candidate at Helsinki University conducting her doctoral research on privacy and European data protection legislation. She is specializing especially in the field of data protection within the Internet of Things and has published on topics such as data quality, sensitive data, joint controllership and location data. She is a member of three multi-disciplinary research projects: Information Security of Location Estimation and Navigation Applications (INSURE), MyGeoTrust and Henkilötietojen suoja digitalisoituvassa yhteiskunnassa.

Laura Ruotsalainen is a Research Manager and Deputy Director of the Department of N&P at FGI, Finland, where she leads the research group on Sensors and indoor navigation. Her current research interests cover vision-aided navigation, GNSS interference detection and mitigation and various aspects of GNSS and sensor fusion. She has authored or co-authored over 45 publications related to vision-aided navigation, GNSS and sensor integration, and GNSS interference mitigation.

Päivi Korpisaari is a professor in Communication Law at the Faculty of Law, University of Helsinki. She completed a Master of Laws in 1993, defended her Licentiate in 2000 and her law degree in 2007 from the University of Helsinki. She was appointed communications law professor at the University of Helsinki on 1.5.2014. Her research interests are in the intellectual property and data protection law, freedom of expression, privacy, media law and communications law.

Heidi Kuusniemi is the Director of the Department of Navigation and Positioning at FGI. Kuusniemi studied navigation technology at the University of Calgary in 2003-2004 and completed her doctoral dissertation on personal satellite navigation in 2005 at Tampere University of Technology. Her research interests cover various aspects of satellite navigation, GNSS receiver design, interference mitigation and sensor fusion for seamless outdoor/indoor positioning and usage of positioning in various mobile applications. She has authored or co-authored over 100 journal and conference papers related to positioning technology.