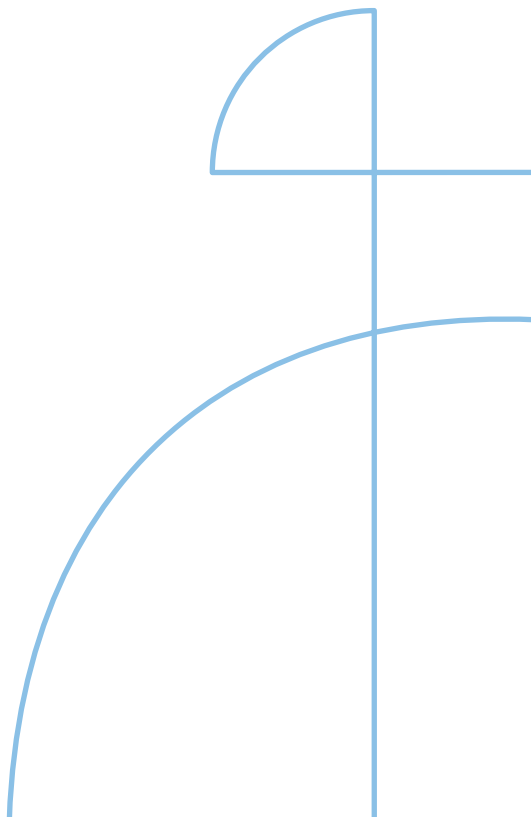
Doctoral Thesis in Electrical Engineering

Secure and resilient localisation in cyber-physical systems

WENJIE LIU

KTH ROYAL INSTITUTE OF TECHNOLOGY



Secure and resilient localisation in cyber-physical systems

WENJIE LIU

Academic Dissertation which, with due permission of the KTH Royal Institute of Technology, is submitted for public defence for the Degree of Doctor of Philosophy on Tuesday, the 13th January 2026 at 09:00 in F3, Lindstedtvägen 26, Stockholm.

Doctoral Thesis in Electrical Engineering
KTH Royal Institute of Technology
Stockholm, Sweden 2025

TRITA-EECS-AVL-2026:5
ISBN 978-91-8106-496-4

Printed by: Universitetsservice US-AB, Sweden 2025

Abstract

Global navigation satellite system (GNSS) and other assisted positioning infrastructures provide ubiquitous, precise locations for cyber-physical system (CPS), from autonomous vehicles to location-based service (LBS) applications on mobile phones in daily lives. Combining multiple satellite constellations, network infrastructures, and onboard sensors typically makes the position solutions more accurate and robust than any single source alone.

However, civilian GNSS signals, Wi-Fi beacons, and cellular pilot signals lack cryptographic protection and are therefore vulnerable to signal spoofing attacks. Even if they can be upgraded to support authentication, meaconing or wormhole attacks can relay and falsify the wireless signals and then manipulate the localisation. More seriously, an attacker can selectively jam the wireless signals from specific infrastructures to force CPS to downgrade to less secure signals, which are later spoofed; coordinated adversaries can also target multiple infrastructures simultaneously to manipulate the positioning result.

This thesis is in the broad area of data trustworthiness for CPS, focusing on the security and resilience of localisation. Emphasis is given on securing the localisation based on GNSS, as they are relevant to a multiplicity of modern systems (e.g., connected vehicles, smartphones, and other Internet-of-Things (IoT) platforms). Significant efforts are dedicated to detecting attacks on position and providing secure and reliable location information, even in the presence of adversaries and benign faults (e.g., challenging propagation environments). Where perfect recovery is unlikely, the proposed methods aim for a best-effort position estimation by opportunistically fusing the remaining available benign signals.

These efforts are concerned with designing, analysing, implementing, and evaluating diverse protocols that address GNSS-specific attacks, other positioning signal attacks, and simultaneous GNSS with other signal attacks. The approaches are theoretically rigorous, are evaluated through detailed simulations, real-world experiments, and system implementation, proposing concrete defense mechanisms.

Keywords
Secure localisation, global navigation satellite system, spoofing detection, cyber physical system, location-based services, opportunistic position information, federated learning, self-supervised learning, multimodal sensing

Sammanfattning

Global navigation satellite system (GNSS) och andra infrastrukturer för assisterad positionering tillhandahåller överallt närvarande, precisa positioner för cyber-physical system (CPS) — från autonoma fordon till location-based service (LBS)-applikationer i mobiltelefoner i vardagen. Fusionen av flera satellitkonstellationer, nätverksinfrastrukturer och ombordliggande sensorer gör positionslösningarna mer precisa och robusta än vad varje enskild lokaliseringsmetod kan erbjuda.

Avsaknaden av kryptografiskt skydd för GNSS-signaler, Wi-Fi-beacons och cellulära pilotsignaler gör dem dock sårbara för signalförfalskningsattacker. Även om systemen kan uppgraderas för att stödja autentisering, kan meaconing- och maskhålsattacker vidarebefordra och förfalska trådlösa signaler och därigenom manipulera positionsbestämningen. Ännu värre är att en angripare kan selektivt störa trådlösa signaler från specifika infrastrukturer för att tvinga CPS att falla tillbaka på mindre säkra signaler, vilka därefter kan förfalskas. På liknande sätt kan angriparen samordna attacker för att förfalska samtliga infrastrukturer.

Denna avhandling rör det breda området datatillförlitlighet för CPS, med fokus på säkerhet och motståndskraft vid lokalisering (positionering). Särskild tonvikt läggs på att säkra lokalisering baserad på GNSS, eftersom dessa är relevanta för en mängd moderna system — från smarta/uppkopplade fordon till smartphones och Internet-of-Things (IoT)-plattformar. Betydande insatser ägnas åt att upptäcka attacker mot positionsinformation och att tillhandahålla säker och tillförlitlig platsinformation även i närvaro av angripare och godartade fel (t.ex. i svåra utbredningsmiljöer). I vissa fall sker detta som en best-effort-lösning genom att utnyttja alternativa lokaliseringstekniker.

Dessa insatser omfattar design, analys, implementering och utvärdering av olika protokoll som hanterar GNSS-specifika attacker, andra attacker mot positioneringssignaler samt samtidiga attacker riktade mot GNSS och andra signaler. Metoderna är teoretiskt rigorösa och utvärderas genom detaljerade simuleringar, verkliga experiment och systemimplementation, och föreslår konkreta försvarsmekanismer.

Nyckelord
Säker lokalisering, globalt satellitnavigationssystem, förfalskningsdetektering, cyber-fysiska system, platsbaserade tjänster, opportunistisk positionsinformation, federerat lärande, självövervakat lärande, multimodal avkänning

Acknowledgment

So many people have helped me along the way. I can only list a few here because of space limitations, but I am deeply thankful to everyone.

First and foremost, I would like to express my sincere gratitude to my advisor, Prof. Panos Papadimitratos, and co-advisor, Prof. Ragnar Thobaben, for invaluable guidance and support throughout this research. Thanks to Prof. Milan Horemuz, Prof. Gustaf Hendeby, Prof. David Broman, Prof. Thomas Sjöland, Prof. Mats Bengtsson, Ms. Hui Qu, and Prof. Junting Chen. Thanks also to my colleagues, Marco, Kewei, Cihan, Zahra, Kostas, Ahmed, Zhichao, Sheng, Hongyu, Iraklis, Di, Sourav, Andrew, Borna, Gianluca, and Johan, whose engaging discussions and insightful comments have greatly improved my work.

Special appreciation goes to Bradford Parkinson, whose pioneering contributions to GPS and meticulous attention to detail continue to inspire me and countless researchers. I also acknowledge the Jammertest organizer and the National Academic Infrastructure for Supercomputing in Sweden.

Finally, I would like to thank my family and friends for their unwavering support and encouragement throughout this journey. I am also grateful to my peers Yanjun, Feifan, Li, Jingyang, Zhenghong, Nan, Zhikai, Zheng, Shuai, Chuan, Zhenyu, Qichen, Shiqian, Yizhi, Wenyao, Yingying, Haoxing, Yuhang, Yumeng, Ziyun, and Rongkuan.

This research work was partially supported by the Knut and Alice Wallenberg (KAW) Academy Fellow program and the China Scholarship Council.

Sincerely,

Wenjie Liu
Stockholm, December 8, 2025

List of included papers

Paper A **Probabilistic Detection of GNSS Spoofing Using Opportunistic Information**

W. Liu and P. Papadimitratos

Published in the *Proceedings of the IEEE/ION Position, Location and Navigation Symposium (IEEE/ION PLANS)*, Monterey, CA, April 2023 [Peer Reviewed, [1]]

Abstract—Global navigation satellite system (GNSS) are integrated into many devices. However, civilian GNSS signals are usually not cryptographically protected. This makes attacks that forge signals relatively easy. Considering modern devices often have network connections and on-board sensors, the proposed here Probabilistic Detection of GNSS Spoofing (PDS) scheme is based on such opportunistic information. PDS has at its core two parts. First, a regression problem with motion model constraints, which equalizes the noise of all locations considering the motion model of the device. Second, a Gaussian process, that analyzes statistical properties of location data to construct uncertainty. Then, a likelihood function, that fuses the two parts, as a basis for a Neyman-Pearson lemma (NPL)-based detection strategy. Our experimental evaluation shows a performance gain over the state-of-the-art, in terms of attack detection effectiveness.

Contributions—The author of this thesis contributed to the design of the detector, the simulator setup, and numerical analysis. The manuscript was written jointly by the authors.

Paper B **Extending RAIM with a Gaussian Mixture of Opportunistic Information**

W. Liu and P. Papadimitratos

Published in the *Proceedings of the International Technical Meeting of The Institute of Navigation (ION ITM)*, Long Beach, CA, USA, January 2024 [Peer Reviewed, [2]]

Abstract—Global navigation satellite system (GNSS) are indispensable for various applications, but they are vulnerable to spoofing attacks. The original receiver autonomous integrity monitoring (RAIM) was not designed for securing GNSS. In this context, RAIM was extended with wireless signals, termed signals of opportunitys (SOPs), or onboard sensors, typically assumed benign. However, attackers might also manipulate wireless networks, raising the need for a solution that considers untrustworthy SOPs. To address this, we extend RAIM by incorporating all *opportunistic information*, i.e., measurements from terrestrial infrastructures and onboard sensors, culminating in one function for robust GNSS spoofing detection. Theoretical assessments of GNSS-only and multi-infrastructure scenarios under uncoordinated and coordinated attacks are conducted. The detection of these attacks is feasible when the number of benign subsets exceeds a specific threshold. A real-world dataset from the Kista Science City area is used for experimental validation. Comparative analysis against baseline methods shows a significant improvement in detection accuracy achieved by our Gaussian Mixture RAIM approach.

Contributions—This work is inspired by advanced RAIM by the second author. The author of this thesis contributed to the design of the detector, the mitigation, and the experimental setup. The manuscript was written jointly by the authors.

Paper C **Position-Based Rogue Access Point Detection**

W. Liu and P. Papadimitratos

Published in the *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Vienna, Austria, July 2024 [Peer Reviewed, [3]]

Abstract—Rogue Wi-Fi access point (AP) attacks can lead to data breaches and unauthorized access. Existing rogue AP detection methods and tools often rely on channel state information (CSI) or received signal strength indicator (RSSI), but they require specific hardware or achieve low detection accuracy. On the other hand, AP positions are typically fixed, and Wi-Fi can support indoor positioning of user devices. Based on this position information, the mobile platform can check if one (or more) AP in range is rogue. The inclusion of a rogue AP would in principle result in a wrong estimated position. Thus, the idea to use different subsets of APs: the positions computed based on subsets that include a rogue AP will be significantly different from those that do not. Our scheme contains two components: subset generation and position validation. First, we generate subsets of RSSIs from APs, which are then utilized for positioning, similar to receiver autonomous integrity monitoring (RAIM). Second, the position estimates, along with uncertainties, are combined into a Gaussian mixture, to check for

inconsistencies by evaluating the overlap of the Gaussian components. Our comparative analysis, conducted on a real-world dataset with three types of attacks and synthetic RSSIs integrated, demonstrates a substantial improvement in rogue AP detection accuracy.

Contributions—The author of this thesis contributed to the design and use case of RAIM algorithm for rogue Wi-Fi AP detection, the numerical evaluation on a publicly available dataset, and the result analysis. The manuscript was written jointly by the authors.

Paper D **Self-Supervised Federated GNSS Spoofing Detection with Opportunistic Data**

W. Liu and P. Papadimitratos

Published in the *Proceedings of the IEEE/ION Position, Location and Navigation Symposium (IEEE/ION PLANS)*, Salt Lake City, UT, USA, April 2025 [Peer Reviewed, [4]]

Abstract—Global navigation satellite system (GNSS) are vulnerable to spoofing attacks, with adversarial signals manipulating the location or time information of receivers, potentially causing severe disruptions. The task of discerning the spoofing signals from benign ones is naturally relevant for machine learning, thus recent interest in applying it for detection. While deep learning-based methods are promising, they require extensive labeled datasets, consume significant computational resources, and raise privacy concerns due to the sensitive nature of position data. This is why this paper proposes a self-supervised federated learning framework for GNSS spoofing detection. It consists of a cloud server and local mobile platforms. Each mobile platform employs a self-supervised anomaly detector using long short-term memory (LSTM) networks. Labels for training are generated locally through a spoofing-deviation prediction algorithm, ensuring privacy. Local models are trained independently, and only their parameters are uploaded to the cloud server, which aggregates them into a global model using FedAvg. The updated global model is then distributed back to the mobile platforms and trained iteratively. The evaluation shows that our self-supervised federated learning framework outperforms position-based and deep learning-based methods in detecting spoofing attacks while preserving data privacy.

Contributions—Based on Paper A, the author of this thesis contributed to the design of the learning and detection framework, the experimental platform, the data collection and evaluation. The manuscript was written jointly by the authors.

Paper E **Guardian Positioning System (GPS) for Location Based Services**

W. Liu and P. Papadimitratos

Published in the *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec)*, Arlington, VA, USA, June 2025 [Peer Reviewed, [5]]

Abstract—Location-based service (LBS) applications proliferate and support transportation, entertainment, and more. Modern mobile platforms, with smartphones being a prominent example, rely on terrestrial and satellite infrastructures (e.g., global navigation satellite system (GNSS) and crowdsourced Wi-Fi, Bluetooth, cellular, and IP databases) for correct positioning. However, they are vulnerable to attacks that manipulate positions to control and undermine LBS functionality—thus enabling the scamming of users or services. Our work reveals that GNSS spoofing attacks succeed even though smartphones have multiple sources of positioning information. Moreover, that Wi-Fi spoofing attacks with GNSS jamming are surprisingly effective. More concerning is the evidence that sophisticated, coordinated spoofing attacks are highly effective. Attacks can target GNSS in combination with other positioning methods, thus defenses that assume that only GNSS is under attack cannot be effective. More so, resilient GNSS receivers and special-purpose antennas are not feasible on smartphones. To address this gap, we propose an extended receiver autonomous integrity monitoring (RAIM) framework that leverages the readily available, redundant, often so-called opportunistic positioning information on off-the-shelf platforms. We jointly use onboard sensors, terrestrial infrastructures, and GNSS. We show that our extended RAIM framework improves resilience against location spoofing, e.g., achieving a detection accuracy improvement of up to 24–58% compared to the state-of-the-art algorithms and location providers; detecting attacks within 5 seconds, with a low false positive rate.

Contributions—The author of this thesis contributed to the real-world attack demonstrations, the design of the countermeasure, the experimental setup, and the result analysis. The manuscript was written jointly by the authors.

Paper F **GNSS Spoofing Detection Based on Opportunistic Position Information**

W. Liu and P. Papadimitratos

Published in the *IEEE Internet of Things (IoT) Journal*, vol. 12, no. 17, pp. 36168-36182, 2025 [Peer Reviewed, [6]]

Abstract—The limited or no protection for civilian global navigation satellite system (GNSS) signals makes spoofing attacks relatively easy. With modern mobile devices often featuring network interfaces, state-of-the-art signals of opportunity (SOP) schemes can provide accurate network positions in replacement of GNSS. The use of onboard inertial sensors can also assist in the absence of GNSS, possibly in the presence of jammers. The combination of SOP and inertial sensors has received limited attention, yet it shows strong results on fully custom-built platforms. We do not seek to improve such special-purpose schemes. Rather, we focus on countering GNSS attacks, notably detecting them, with emphasis on deployment with consumer-grade platforms, notably

smartphones, that provide *off-the-shelf opportunistic information* (i.e., network position and inertial sensor data). Our Position-based Attack Detection Scheme (PADS) is a probabilistic framework that uses regression and uncertainty analysis for positions. The regression optimization problem is a weighted mean square error of polynomial fitting, with constraints that the fitted positions satisfy the device velocity and acceleration. Then, uncertainty is modeled by a Gaussian process, which provides more flexibility to analyze how sure or unsure we are about position estimations. In the detection process, we combine all uncertainty information with the position estimations into a fused test statistic, which is the input utilized by an anomaly detector based on outlier ensembles. The evaluation shows that the PADS outperforms a set of baseline methods that rely on SOP or inertial sensor-based or statistical tests, achieving up to 3 times the true positive rate at a low false positive rate.

Contributions—Building upon Paper A, the author of this thesis contributed to the design of the learning-based detector, the enhanced network simulations, the collected dataset, and the experimental evaluation. The manuscript was written jointly by the authors.

Paper G **Interference-Resilient Optical Wireless Positioning via Machine Learning-Enhanced Subset Filtering**

Y. Huang, Y. Liu, W. Liu, P. Papadimitratos, H. Haas, and I. Tavakkolnia

Published in the *Proceedings of the European Conference on Optical Communication*, Copenhagen, Denmark, September 2025 [Peer Reviewed, [7]]

Abstract—Optical wireless positioning has emerged as a promising alternative due to its superior accuracy, achieving centimeter-level positioning errors (e.g., below 10 cm) and offering greater energy efficiency and electromagnetic immunity compared to Wi-Fi, Bluetooth, and ultra-wideband systems. However, existing solutions typically assume interference-free conditions, often ignoring the impact of external interference sources. In practice, spectral overlaps between positioning subcarriers and interference signals can severely degrade system performance. To address these challenges, we propose a machine learning-based optical wireless positioning framework that mitigates interference, recovers degraded position estimates, and detects the interference sources. Our design introduces the concept of subset-based received signal strength indicator inputs. We further develop and experimentally validate a reliability-aware subset fusion mechanism that detects anomalies, excludes corrupted signals, and aggregates reliable estimations to restore positioning accuracy. Through this approach, the proposed system remains robust and accurate even in the presence of spectral interference.

Contributions—The author of this thesis contributed to the design and the use case of receiver autonomous integrity monitoring (RAIM) algorithm for optical wireless positioning, the detection formulation, and

some analysis. The manuscript was written jointly by the authors.

Paper H **Coordinated Position Falsification Attacks and Countermeasures for Location-Based Services**

W. Liu and P. Papadimitratos

Published in the *IEEE Open Journal of the Communications Society (OJ-COMS)*, vol. 6, pp. 9229–9246, 2025 [Peer Reviewed, [8]]

Abstract—With the rise of location-based service (LBS) applications that rely on terrestrial and satellite infrastructures (e.g., global navigation satellite system (GNSS) and crowd-sourced Wi-Fi, Bluetooth, cellular, and IP databases) for positioning, ensuring their integrity and security is paramount. However, we demonstrate that these applications are susceptible to low-cost attacks (less than $50), including Wi-Fi spoofing combined with GNSS jamming, as well as more sophisticated coordinated location spoofing. These attacks manipulate position data to control or undermine LBS functionality, leading to user scams or service manipulation. Therefore, we propose a countermeasure to detect and thwart such attacks by utilizing readily available, redundant positioning information from off-the-shelf platforms. Our method extends the receiver autonomous integrity monitoring (RAIM) framework by incorporating opportunistic information, including data from onboard sensors and terrestrial infrastructure signals, and, naturally, GNSS. We theoretically show that the fusion of heterogeneous signals improves resilience against sophisticated adversaries on multiple fronts. Experimental evaluations show the effectiveness of the proposed scheme in improving detection accuracy by 62% at most compared to baseline schemes and restoring accurate positioning.

Contributions—Extending Paper E, the author of this thesis contributed to the design of the secure and isolated over-the-air testbed, the experimental setup, and the comprehensive analysis of the detection theory and computational complexity. The manuscript was written jointly by the authors.

Paper I **Multimodal Location Spoofing: Federated Detection with RAIM-Based Self-Labeling**

W. Liu and P. Papadimitratos

Accepted with Mandatory Revisions to the *IEEE Open Journal of the Communications Society (OJ-COMS)*, 2025 [Peer Reviewed, [9]]

Abstract—Modern localization relies on satellite and terrestrial infrastructures (e.g., global navigation satellite system (GNSS) and crowd-sourced Wi-Fi), supporting critical applications ranging from autonomous navigation to life services. However, they are susceptible to *multimodal* location spoofing attacks, where various types of wireless signals are crafted in a coordinated manner to deceive the receiver position. Such attacks can cause severe disruptions, such as misguiding vehicles and enabling fraud. Although recent deep

learning methods help detect GNSS spoofing and jamming, they require extensive labeled datasets, they are not designed for multimodal location spoofing, training is computationally intensive and centralized, thus raising privacy concerns due to the sensitive nature of location data. We propose `FedRAIM`, a novel federated learning framework designed for robust, efficient, and privacy-preserving multimodal location spoofing detection. The key `FedRAIM` elements are: Training labels are autonomously generated through an extended receiver autonomous integrity monitoring (RAIM) algorithm, incorporating diverse opportunistic information, i.e., terrestrial infrastructure signals, onboard sensor data, and naturally GNSS signals. During federated training, local long short-term memory (LSTM) models are trained independently on client devices. Server then aggregates, using the FedAvg algorithm, these local model parameters, not data, into a global model, which is subsequently distributed back to the clients for iterative training. Experimental results on real-world multimodal spoofing datasets demonstrate that `FedRAIM` achieves an area under the curve (AUC) of up to 98.3%.

Contributions—Building upon Paper D, the author of this thesis contributed to the design of the detection framework, and the experimental validation and analysis. The manuscript was written jointly by the authors.

Other contributions not included in this thesis

Paper J **[Poster] Probabilistic Detection of GNSS Spoofing Using Opportunistic Information**

W. Liu and P. Papadimitratos

Presented at the *Cybersecurity and Privacy (CySeP) Summer School*, June 2023 [Peer Reviewed]

Paper K **[Poster] GNSS Spoofing Detection Using Untrusted Opportunistic Information**

W. Liu and P. Papadimitratos

Presented at the *Cybersecurity and Privacy (CySeP) Summer School*, June 2024 [Peer Reviewed]

Paper L **[Poster] Self-Supervised Federated Learning for GNSS Attack Detection**

W. Liu and P. Papadimitratos

Presented at the *Cybersecurity and Privacy (CySeP) Summer School*, June 2025 [Peer Reviewed]

Paper M **G^{2}FL: Robust Federated Learning for GNSS Spoofing Detection**

S. Liu, W. Liu, A. Hussain, and P. Papadimitratos

Submitted to the *IEEE International Conference on Communications (ICC)*, November 2025

Contents

List of Figures

List of Tables

Acronyms

AGC automatic gain control 16, 17, 27
AoA angle of arrival 2, 3
AP access point viii, ix, xvii, 2–5, 9–11, 18–20, 23, 26, 29, 30
AUC area under the curve xiii, 18
BS base station 2, 3, 9
BSSID basic service set identifier 8
C/No carrier to noise density ratio 16, 17, 27, 28
CPS cyber-physical system i, iii, 1, 4, 7, 9–12, 29
CSI channel state information viii, 3
GLRT generalized likelihood ratio test 16
GNSS global navigation satellite system i, iii, vii–x, xii, xiii, xvii, xix, 1–5, 7–14, 16–20, 22, 23, 25–27, 29, 30
GPS global positioning system 25
i.i.d. independent and identically distributed 17, 18
ICMP Internet Control Message Protocol 11
IMU inertial measurement unit 3–5, 11, 12, 16, 17, 19, 22, 27, 30
IoT Internet-of-Things i, iii, 1
LBS location-based service i, iii, x, xii, xvii, 1, 5, 22, 23, 26, 30
LED light-emitting diode 21
LLM large language model 24
LSTM long short-term memory ix, xiii, xvii, 16–18, 27, 28
MAC medium access control 3
NPL Neyman-Pearson lemma vii
OSNMA Open Service Navigation Message Authentication 8, 10
PNT Positioning, Navigation and Timing 1–3, 7, 8, 30
PPD Privacy Protection Device 7
PVT position, velocity and time 2
RAIM receiver autonomous integrity monitoring viii–xiii, xvii, 4, 5, 11, 12, 20, 22, 23, 26–29
ROC receiver-operating characteristic xvii, 15, 17, 18
RSSI received signal strength indicator viii, ix, xvii, 3–5, 7, 11, 12, 18–21
RTK real-time kinematic 1, 25
RTT round-trip time 11
SDR software-defined radio 2, 7, 10, 23
SNR signal-to-noise ratio 3
SOP signals of opportunity viii, x, xi, 3, 4, 15, 23
SSID service set identifier 3, 8, 24
TOA time-of-arrival 3
UAV unmanned aerial vehicle 3
WPA3 Wi-Fi Protected Access 3 3

1 Introduction

Location information, as the fundamental link between the physical world and cyberspace, is the core element of cyber-physical system (CPS). With the globalization of Galileo satellites, the deployment of 5G/6G networks, and the popularization of Internet-of-Things (IoT) devices, precise and reliable localization is fundamental for numerous CPS applications essential to our modern society. From conventional and autonomous transportation [10] to critical infrastructure synchronization [11] and ubiquitous location-based service (LBS) [12], accurate Positioning, Navigation and Timing (PNT) information is indispensable. For example, in LBS, localization is not only a convenience but also a foundation for turn-by-turn navigation, ride-hailing, and even digital content region locking. Meanwhile, global navigation satellite system (GNSS), consisting of satellites from many different countries, has revolutionized PNT, offering widespread availability and remarkable accuracy. The proliferation of multi-frequency and multi-constellation GNSS receivers with real-time kinematic (RTK) station supports, even in mass-market devices like smartphones [13], has further expanded the reach of centimeter-level accuracy to everyday users.

However, this increasing reliance on GNSS and relevant terrestrial positioning infrastructures has enlarged the attack surface, making them highly vulnerable to malicious users, external attackers, or service providers [14]. The manipulation of location information can lead to a lot of real-world incidents, exemplified by “ghost driver” in ride-sharing services who is automatically assigned to passengers [15, 16]. This position manipulation allows the adversary to take subtle detours or simulate a pickup and trip completion, thereby carrying out a taxi fare scam. Game players of Pokémon GO or users of Google Maps, Waze, Foursquare, etc., can fake the current position of the smartphone to gain game points or non-compliant rewards [17, 18]. Scooter sharing services [19], a popular urban transportation method, are often managed using geofencing, an LBS feature that virtually restricts the riding area or dictates billing zones. However, position manipulation can break the geofencing, causing scooters to seemingly appear within the designated area while they are actually far outside. Public transport systems might use e-ticketing [20] and charge passengers based on travel dis-

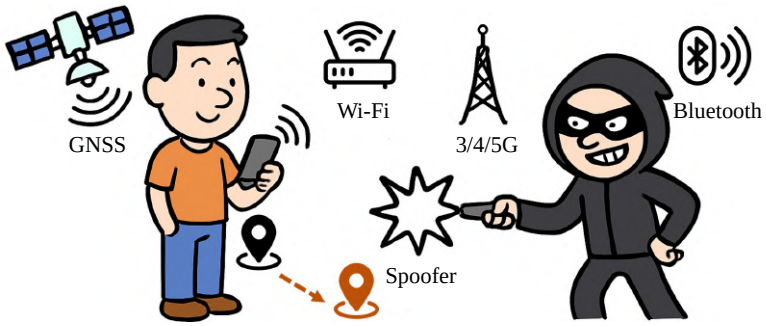


Figure 1.1: Modern positioning systems rely on diverse signals but face growing threats from sophisticated adversaries. Adversaries can spoof wireless signals, as well as jam, relay, etc., in either a coordinated or uncoordinated way.

tance; however, attackers can travel for free by crafting fake positions. These threats are from fundamental weaknesses in civilian positioning signals. GNSS signals, in particular, operate at very low power below the noise floor at the receiver, and their civilian protocol defines open, unencrypted signal structures, making them highly susceptible to interference and spoofing. Furthermore, modern localization relies on wireless signals everywhere, which are more exposed than wired connections and broaden the attack surface. Simple, affordable jamming devices [21] can easily deny service, while sophisticated spoofing attacks can subtly manipulate receiver PNT solutions [22]. The increasing popularization of software-defined radio (SDR) and open-source implementations of satellite transmitters, rogue Wi-Fi access points (APs), and base stations (BSs) have lowered the barrier for launching such attacks [23, 24, 25], necessitating a robust and secure approach to PNT.

Specifically, GNSS spoofing attacks have roughly three categories: simple attacks, advanced attacks, and multiple sophisticated spoofers. Simple spoofing attacks use false signals that are generated with a single GNSS signal simulator [23], and these signals are usually not synchronized, making them easy to detect [26, 27, 28]. More advanced attacks, e.g., the experimental setup in [29], use a professional GNSS simulator with an SDR and high-precise time source to mimic signal characteristics such as Doppler shift. They can also use the gradual deviation strategy [10], path drift [30], and more. Multi-spoofing attacks [31] can transmit false GNSS signals using multiple simulators to angle of arrival (AoA) and other characteristics of individual satellite signals. Meaconing or replay attacks also range from classical to advanced ones, and they actually can be seen as a strongly constrained type of spoofing. An adversary can record an entire block of GNSS signals and replay it somewhere else without modification [32]. Then, the victim receiver will estimate its position, velocity and time (PVT) solutions the same as the adversary. A more advanced replay attacker can estimate the signal security code on-the-fly and manipulate each signal received from the individual satellite [33]. Another more sophisticated modification, known as selective delay [34], rebroadcasts separate satellite signals, allowing for modification of the position solution according to the attack scenario. Distance-decreasing attacks [35, 36] provide additional options for adversaries, employing Early Detection and Late Commit to relay

the GNSS signal, thereby making the relayed one appear to arrive earlier than it would have.

Existing countermeasures for GNSS spoofing broadly fall into three categories: signal processing-based techniques [34, 37, 38, 39, 40, 41], navigation message authentication [42, 43], and data-level validation of the PNT solution [44, 45, 46]. Signal processing methods, often deployed as standalone detectors [34, 47, 48, 49, 50], focus on analyzing the physical characteristics of GNSS signals, e.g., Doppler effect, AoA, signal-to-noise ratio (SNR), and received signal strength indicator (RSSI). Recent advances include leveraging signal quality monitoring [51] or machine learning on signal features [52]. Other data-level approaches, such as [53] for unmanned aerial vehicles (UAVs), focus on fusing GNSS with inertial measurement unit (IMU) data, and use relative distance information obtained from RSSI data to detect spoofing, with alternative positions based on multi-agent systems enhancing navigation robustness under spoofing conditions. In [54, 55], signals of opportunity (SOP) from terrestrial network infrastructures can assess GNSS-provided positions. This involves assuming adequate network scanning and the availability of BS or AP positions, using RSSI or time-of-arrival (TOA) as the distance measure between the mobile platform and the station to estimate position for checking GNSS. Combined metric-based approach [56] integrates multiple detection features such as autocorrelation distortion, RSSI, pseudorange, carrier phase difference, and AoA to enhance detection. Time information from multiple reference time sources, such as local clocks and time servers, can effectively validate GNSS solutions through a time-based detector [57]. While these methods offer varying degrees of protection, they often come with significant hardware requirements (e.g., multi-antenna arrays for AoA [14, 31, 58]), or face limitations in terms of backward compatibility and susceptibility to advanced stealthy attacks [10, 59]. Furthermore, many of them rely on assumptions of benign alternative position information or specific, often unavailable, low-level signal data (e.g., carrier phase) on mass-market devices like smartphones [13]. A promising approach to improve detection is to collect data from mobile platforms with GNSS and leverage machine learning to train detection models. Deep learning-based methods [60, 61, 62] can use signal properties and opportunistic data as input features. These methods need a large amount of labeled dataset, which maybe not practical in real-world environments.

Defenses against malicious Wi-Fi hotspots have also received increasing interest. Industry standard solutions [63, 64, 65] often employ whitelist-based filtering using known AP medium access control (MAC) addresses and service set identifiers (SSIDs) to identify unauthorized APs. However, such records can be easily spoofed using consumer-grade hardware. For example, most of the Wi-Fi routers can set any SSID, and some others or open-source routers (e.g., OpenWrt) can even modify their MAC addresses [66]. Wi-Fi Protected Access 3 (WPA3) can provide limited beacon protection, but is not compatible with many former devices that are still in use. Hence, there is a need for detection beyond these Wi-Fi beacons. [67] uses RSSI measurements to perceive malicious Wi-Fi signals, but its clustering and two-step algorithm is affected by signal fluctuations as a result of environmental factors (interference and multipath). Another line of defense involves wireless fingerprinting, which operates independently of client devices [68]. Still, they also have limitations about hardware requirements, because Wi-Fi channel state information (CSI) fingerprints require certain network interfaces to measure [68, 69]. Thus, they are not applicable for the mass-market

CPS.

The widespread integration of GNSS, multiple network connectivity, and rich computational capabilities into modern CPS presents a unique opportunity to leverage multiple data sources for secure and resilient localization [70, 71, 72]. Previous works have explored using SOP, such as Wi-Fi or cellular signals [54, 73], to localize devices or detect deviations from GNSS-provided positions. [74, 75] incorporate IMU data for trajectory analysis to identify inconsistencies indicative of spoofing. Some sophisticated custom hardware platforms with SOP and IMU are also proposed to provide alternative positioning in GNSS-denied or multipath environments [76, 77, 78, 79, 80]. While these methods have shown promise for secure and resilient localization, they are not readily applicable on most consumer-grade platforms, such as smartphones, or, critically, they rely on the strong assumption that other network positioning infrastructures are beyond the adversary's reach. For example, [54] presumes that no Wi-Fi signal is adversarial. Hence, these defenses or localizations would fail against adversaries capable of cellular jamming or deploying rogue Wi-Fi APs [81, 82, 83, 24, 84, 85, 86]. This thesis considers precisely both the aforementioned evolving threats and the untapped potential of opportunistic information. It includes practical applicability on mass-market devices with limited low-level signal access and adds privacy constraints for learning-based detectors across devices. It focuses on developing advanced and universal defense mechanisms against a series of attacks that range from GNSS-specific manipulations to coordinated location attacks across multiple positioning infrastructures, then provides alternative positioning results during attacks. The overarching goal is to enhance the resilience and trustworthiness of positioning systems for CPS applications.

This thesis addresses these challenges by developing detection and mitigation strategies that combine probabilistic modeling, opportunistic position information, and federated learning. The proposed methods are designed to operate on real-world CPS (including smartphones) and with adversaries compromising GNSS and/or terrestrial positioning signals. Validation comprises theoretical analysis, simulations, and real-world experiments.

Thesis Contributions and Structure. This compilation thesis is conceptually viewed based on three types of attacks and their countermeasures using tools from either traditional signal processing or deep learning for location security. The common theme across these three parts is the exploitation of heterogeneous and opportunistic position information (GNSS, terrestrial network ranging, Li-Fi RSSI, and onboard sensors), and it combines classical model-based methods (e.g., receiver autonomous integrity monitoring (RAIM)-based outlier detection and motion-constrained regression) with data-driven techniques (self-supervised and privacy-preserving federated learning) to detect different kinds of location attacks. Together, these contributions form a coherent and flexible framework for securing single-signal and multi-signal positioning systems in CPS:

- **Defending Against GNSS Attacks.** The author and the research group members focused first on detecting and mitigating spoofing attacks solely targeting GNSS signals. The contributions include probabilistic frameworks for detection using opportunistic data [1, 6], and advanced self-supervised federated learning approaches for robust and privacy-preserving detection [4,

9]. Network-based positions and onboard sensors are fused within a probabilistic framework for GNSS position attack detection, which fuses position, velocity, acceleration, and orientation data from various sources with different accuracies and update rates. It provides a robust and interpretable detection outcome, as well as a recovered position using benign GNSS, networks, and onboard sensors. In the proposed so-called PADS, the formulation of a motion-constrained regression problem for position smoothing that combines short-term trajectory smoothing via IMU with long-term stabilization from network-based positions. Comprehensive experiments were done with the help of a simulated autonomous driving platform and various real Android smartphones, including different brands, prices, and chips (from Exynos, MTK, Qualcomm, and Google Tensor). Based on PADS, a self-supervised federated learning framework is built with opportunistic data for GNSS spoofing detection. It eliminates the requirement for labeled or annotated datasets in deep learning-based GNSS spoofing detection, while keeping comparable performance.

- **Defending Against Attacks on Other Positioning Signals.** This work addresses attacks on non-GNSS positioning infrastructures. Position-based rogue AP detection schemes are developed for Wi-Fi [3], and explore interference-resilient positioning for emerging optical wireless technologies [7]. The key contribution is a scheme that can work either as a tool used by wireless network operators for actively monitoring APs or by mobile users that can independently detect rogue APs. It just needs RSSIs to make the scheme compatible with other rogue AP detection schemes. I adopt and adapt the RAIM used in GNSS to achieve rogue AP detection, and term this Gaussian mixture RAIM. Position fusion from Wi-Fi/Li-Fi positioning algorithms and rogue AP exclusion strategies are exploited. The numerical experiments and a comparative analysis on a partially real-world Wi-Fi/Li-Fi RSSI dataset show significant improvement over baseline rogue AP detection schemes. Moreover, this scheme is the first to detect and exclude interferences in optical wireless communication and positioning.
- **Defending Against Simultaneous GNSS and Other Signal Attacks.** This part tackles the challenging scenario where adversaries simultaneously compromise multiple positioning signal types. Coordinated location falsification attacks are analyzed, and robust RAIM-based methodologies utilizing Gaussian mixture and opportunistic information fusion are proposed to secure fused positioning solutions [2, 5, 8]. Real-world proof of concept demonstrates geolocation API attacks and illustrates how they can disrupt LBS applications in the real world. Conversely, the RAIM-based framework can detect and mitigate threats in LBS position manipulation. Unlike RAIM on GNSS, it utilizes distance estimates from terrestrial networking infrastructures and GNSS with onboard sensors. By integrating this opportunistic ranging information from multiple sources, it gives an enhanced security likelihood against GNSS spoofing, rogue Wi-Fi APs, and other position manipulations. The evaluation confirms the effectiveness of this scheme, with an improved true positive rate and a reduced delay in detecting attacks in various real-world scenarios.

In the remainder of this thesis, Chapter 2 provides essential background on attacker

models and compares different types of attackers. Chapter 3 presents the main methodologies and contributions across these three main parts, with references to the appended papers for more details. Finally, Chapter 4 concludes the thesis and outlines future research directions.

2 Modeling attacks on positioning

This chapter provides essential background for understanding secure localization in cyber-physical system (CPS) through the vulnerabilities of positioning systems and the detailed characteristics of adversaries targeting them.

Global navigation satellite system (GNSS) localization is susceptible to various forms of intentional interference: Jamming aims to deny service by overpowering legitimate signals with noise [21]. Spoofing, on the other hand, involves crafting apparently valid signals to manipulate a victim receiver's Positioning, Navigation and Timing (PNT) solution [22]. Location fusion, which is widely used in most CPS instead of standalone localization, is based on GNSS combined with cellular networks (3G, 4G, 5G), Wi-Fi, Bluetooth, and other technologies. It typically employs advanced statistical estimation and combines multiple sources of locations, which was initially believed to be more accurate and robust against attacks or interferences. However, this assumption has been challenged. For example, [10] successfully exploits the system by proposing a two-stage attack, which first performs vulnerability profiling to identify a window of takeover effect and then initiates aggressive spoofing to cause the vehicle to deviate off-road or on the wrong route. Additionally, this thesis proposes and analyzes coordinated position falsification attacks that can very efficiently spoof the fused positions without being detected, which manipulates both GNSS and Wi-Fi (and/or other infrastructures) in a coordinated manner.

2.1 Generic attacker characteristics

A common characteristic of GNSS attacks is the low power of legitimate satellite signals, making GNSS easier to attack by even modest adversarial transmissions. Affordable Privacy Protection Devices (PPDs) and software-defined radios (SDRs) have democratized the ability to launch attacks, enabling sophisticated manipulations with relatively low budgets [23]. Similarly, Wi-Fi as well as Bluetooth beacons fundamentally lack cryptographic protection, while most network-based positioning systems depend on the received signal strength indicator (RSSI) of these beacons. Any consumer-grade

Wi-Fi router or Bluetooth device can mimic service set identifier (SSID), basic service set identifier (BSSID), and channel number in the beacons of another device. Malicious signals (GNSS pseudorandom noise, Wi-Fi beacons, cellular pilot messages, IP geolocation responses) can force a target to compute an incorrect position. Adversaries can vary in sophistication, ranging from simple jammers and basic position-jumping spoofers to highly coordinated spoofers that employ intricately designed strategies tailored to environmental conditions.

2.2 Attack models

2.2.1 Meaconing and signal relay

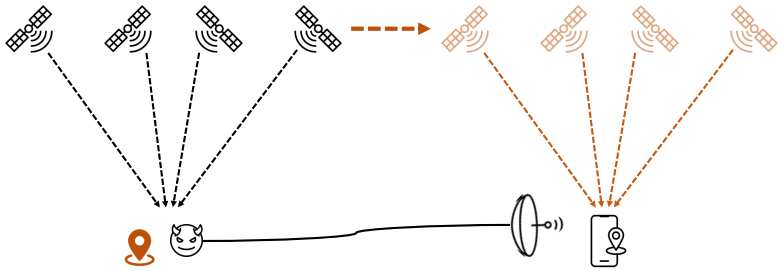


Figure 2.1: Meaconing: signals are relayed from an adversarial receiver to a transmitter.

Meaconing involves the replay of legitimate satellite signals, either in real time or from recordings, to deceive a receiver, as illustrated in Figure 2.1. This can be "block meaconing" where an entire frequency band is replayed [34], "message-level relay meaconing" where only navigation message information is relayed and the signal is regenerated [32], or even "distance-decreasing attacks" that can short the perceived distance between the transmitter and receiver [87, 35, 36]. While meaconing is powerful against cryptographically protected signals (e.g., Galileo Open Service Navigation Message Authentication (OSNMA)), it offers limited flexibility in controlling the victim's position compared to fully synthetic spoofing.

2.2.2 Synchronous GNSS simulation

Synchronous spoofing involves crafting and precisely synchronizing adversarial signals with legitimate ones to smoothly "drag" the victim's PNT solution, as depicted in Figure 2.2. This requires accurate knowledge of the victim's location, and even precise alignment of the Doppler shift and code phase [22]. Despite its complexity, this attack is highly stealthy. Existing open-source spoofers and commercial simulators, e.g., bladeGPS [23] and Skydel, can achieve this at an affordable cost. The GNSS spoofing detection mechanisms in this thesis can counteract such sophisticated simulated attacks.

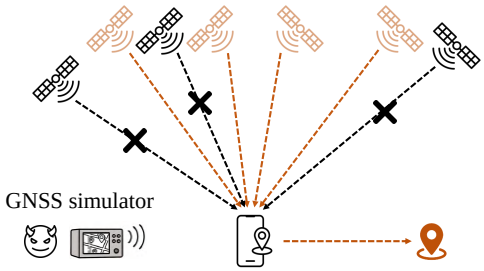


Figure 2.2: GNSS signal simulation: signals are generated and transmitted towards users for precise position manipulation.

2.2.3 Network signal spoofing

Wireless networks provide alternative positioning, but rogue Wi-Fi access points (APs) and cellular base stations (BSs) pose multiple security threats that intercept and spoof wireless communications [82, 66, 85, 86]. They can mimic legitimate ones to fool receivers into connecting to these fraudulent networks. Even more simply, adversaries can broadcast fake Wi-Fi beacons to spoof positions due to the lack of encryption and authentication in Wi-Fi beacons. This can be done with consumer-grade Wi-Fi routers or low-cost Wi-Fi chips (e.g., ESP8266 boards [24]).

2.2.4 Coordinated location falsification

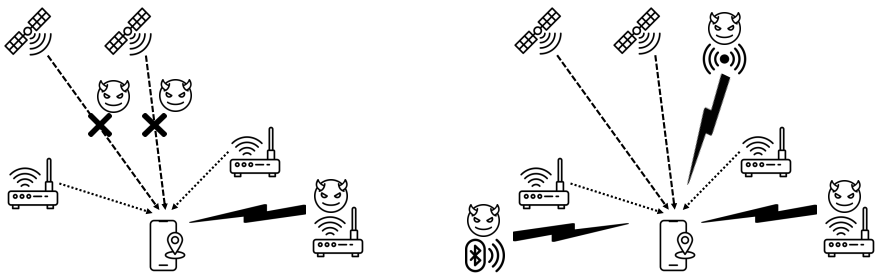


Figure 2.3: Left: Wi-Fi spoofing with GNSS jamming; right: coordinated multi-source spoofing, as it appears in Paper E.

Beyond GNSS-only attacks, this thesis examines sophisticated adversaries capable of simultaneously compromising multiple positioning infrastructure systems. As illustrated in Figure 2.3, these attacks can involve:

- **Wi-Fi Spoofing with GNSS Jamming:** Adversaries jam GNSS signals while replaying or forging Wi-Fi beacons to control positioning, forcing the location fusion algorithm to rely on manipulated network data. This is a low-cost, effective attack against general CPS. This is discussed and demonstrated in [5, 8].

- **Coordinated Multi-Source Spoofing:** The most advanced form, where GNSS, Wi-Fi, cellular, and even IP geolocation are simultaneously and coherently manipulated to deceive secure CPS applications that cross-validate multiple sources. This requires careful crafting of all relevant wireless signals and redirecting network traffic. The work in [5, 8, 9] demonstrates and analyzes such multimodal attacks.

To achieve the interference or modification of signals, attackers can employ tools such as jammers, spoofers, GNSS simulators, privacy protection devices [88], SDRs [32], or rogue APs [82]. While adversaries can take over unsuspecting devices nearby, this thesis assumes that they cannot alter the victim device's internal algorithms used to derive position. The adversaries may only suppress or corrupt some benign ranging sources for the location fusion. Furthermore, they are assumed to have no access to cryptographic keys and authentication files in the legitimate positioning infrastructures, and they only know publicly available protocols and parameters of GNSS, OSNMA, Wi-Fi, etc. Hence, they cannot simultaneously and completely eliminate *all* benign ranging information available to the device (i.e., at least some independent measurements remain available).

3 Protecting CPS positions

This chapter details the core defence contributions of the thesis, presenting novel defense mechanisms against the sophisticated location attacks discussed in Chapter 2, which can also be applied to many other location-based attacks. The central theme is leveraging diverse "opportunistic information"—data readily available from heterogeneous sensors and communication modules on modern cyber-physical system (CPS) platforms—to enhance the robustness and resilience of positioning systems.

3.1 Methodology overview

Modern global navigation satellite system (GNSS)-enabled devices are often embedded in complex systems offering a wide array of connectivity and computational capabilities [70]. Their "opportunistic information" includes: terrestrial wireless signals, e.g., Wi-Fi, cellular, and Bluetooth signals, which can be used for positioning (e.g., via received signal strength indicator (RSSI)-based methods; onboard sensors, e.g., wheel speed sensors and inertial measurement units (IMUs), providing velocity, acceleration, angular velocity, and orientation data; other position information like Internet Control Message Protocol (ICMP) messages providing round-trip time (RTT) values and IP addresses.

The fundamental principle is to cross-validate positioning solutions from these independent sources. In the first part of this chapter, GNSS spoofing attacks are considered while network signals are benign and can provide position information. A position-based attack detection method is proposed, building upon traditional machine learning approaches, and subsequently advances to an advanced deep learning-based method that enhances both the performance and privacy preservation of the position-based method.

In the second part of this chapter, the scenario primarily involves an indoor environment, so only network signal attacks are investigated, and GNSS is not available. The proposed rogue Wi-Fi/Li-Fi access point (AP) detection extends the receiver

autonomous integrity monitoring (RAIM) paradigm, traditionally focused on GNSS internal consistency, to encompass RSSI values as ranging information and positioning solutions based on their subsets.

In the third part, the adversary is more general and significantly stronger, capable of attacking both GNSS and other network signals. An extended RAIM of different types of ranging information can detect both GNSS spoofing and network-based location spoofing. Then, RAIM-supervised federated detection based on this scheme further improves the detection accuracy of position attacks on multiple infrastructures.

3.2 Countermeasures for GNSS-specific attacks

The contributions in this area focus on enhancing GNSS spoofing detection by exploiting opportunistic information, assuming other signal sources are inherently benign. Given that GNSS, Wi-Fi, and cellular signals mostly operate in different frequency bands, it is common and straightforward for an attacker to spoof GNSS only. Modern CPS are typically equipped with substantial computational ability, heterogeneous network infrastructures, and a variety of onboard sensors. This work leverages position solutions from network-based positioning and onboard sensors to validate GNSS positions.

3.2.1 Probabilistic detection using opportunistic data

Paper A proposes a novel Probabilistic Detection of GNSS Spoofing (PDS) that integrates network-based positioning results and velocity, acceleration, and orientation from onboard sensors within a probabilistic framework. This method constructs confidence intervals for positions by combining motion-constrained regression with Gaussian processes, leading to a fused test statistic for anomaly detection. This approach outperforms traditional sensor fusion methods by effectively handling noisy and non-Gaussian error characteristics. [1] details the foundational framework, demonstrating its effectiveness against gradual deviation spoofing attacks. The work is further expanded in Paper F to the Position-based Attack Detection Scheme (PADS), with a comprehensive theoretical and experimental analysis, demonstrating significant improvements in detection accuracy and reduced detection time delay.

The objective is to assess the consistency between the GNSS-derived position and opportunistic position information (network-based position and IMU) to determine whether the current GNSS position is indicative of an attack. By evaluating the probability of a GNSS position attack, the scheme aims to maximize the true positive rate of detection. Additionally, it aims for a detection scheme that remains reliable even if certain types of opportunistic information are unavailable.

As Figure 3.1 shows, the position-based attack detection scheme detects GNSS spoofing using information about network positions and movements (i.e., velocity, acceleration, and orientation). Input data is collected from GNSS, Wi-Fi, cellular, and onboard sensors. A rolling window collects a fixed-length series of positions, which are then interpolated to generate a smoothed trajectory. Subsequently, confidence intervals for these $M + 1$ position series are calculated. These confidence intervals are used to con-

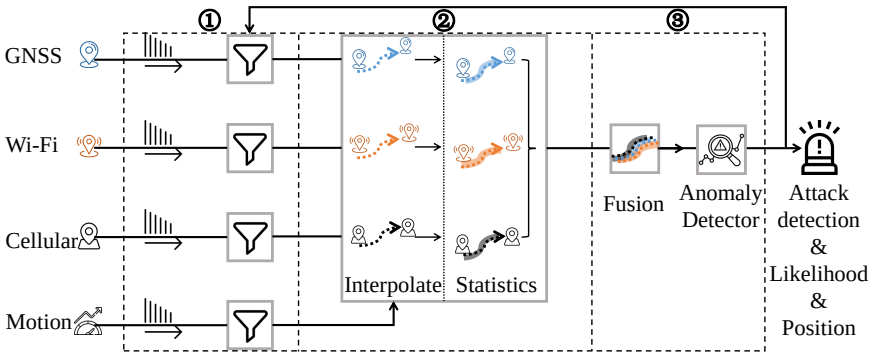


Figure 3.1: Overview of position-based attack detection scheme for GNSS-specific attacks, as it appears in Paper F.

struct a fused test statistic that determines whether the current GNSS position reflects an attack, and if so, trigger an alarm.

The first component of the scheme is the rolling window, which continuously collects real-time positions from GNSS, Wi-Fi, and cellular sources, in addition to velocity, acceleration, and orientation data from onboard sensors. These positions are organized in time order. The filters implement rolling window techniques, processing fixed-length data segments at each detection epoch rather than using the entire historical series.

The second component, confidence interval, is constructed by combining both motion and statistical models. The motion part uses a local polynomial regression algorithm with movement constraints to fit the position data. It exploits both the short- and long-term characteristics of data: while onboard sensors provide high short-term accuracy, they are unable to maintain stable positional accuracy over time; to overcome this limitation, it integrates their data with less frequent but periodic positioning updates from terrestrial networks. Regression is utilized to fit the positions, minimizing the fitting error while adhering to movement constraints to ensure the resulting trajectory conforms to velocity and acceleration. The statistical part is a Gaussian process, focusing on confidence intervals represented as a probability distribution, indicating the uncertainty of positions. It is assumed that the benign position series follows a Gaussian process, with a mean already determined through the motion part. To compute the variance, Gaussian process regression utilizes a predefined covariance function and differences between the fitted results. This provides a robust measure of the variability in position data.

In the last decision-making component, it builds a test statistic by using the mean and variance of confidence intervals. Then, anomaly detection relies on this test statistic across multiple sources and over the time domain. To integrate the confidence intervals in the time domain, it calculates a weighted sum over time, with the weights normalized to ensure their summation to one. The weighted sum is still Gaussian, with its mean and variance determined as a linear combination of the means and variances of the individual confidence intervals. To fuse the GNSS-derived position with multi-

Table 3.1: Datasets for experiments of position-based attack detection, as it appears in Paper F. Dataset A: Simulated 6 driving traces in outdoor urban environments. Dataset B: Measurements collected by the NSS field campaign at Jammertest 2024 (we call the part used here the Jammertest 2024 dataset/Dataset B).

	Ground Truth	GNSS	Network	Onboard Sensor
Dataset A	1 Hz	1 Hz	1 Hz & 1 Hz	200 Hz
Dataset B	1 Hz	1 Hz	0.1 – 0.3 Hz	100 Hz

ple opportunistic position sources, it multiplies the distributions at each time. Then, it creates a fused test statistic based on them and applies an anomaly detector (Loda [89]).

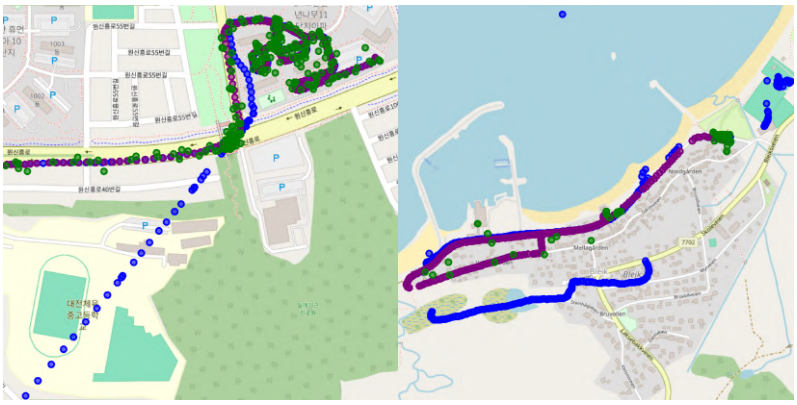


Figure 3.2: Ground truth (purple), network (green), and GNSS (blue) positions of two traces from Dataset A (left) and B (right), as it appears in Paper F. Note that "network position" refers to both Wi-Fi and cellular positions in Dataset A, and positions from Android Network Location Provider in Dataset B.

The effectiveness of PADS was evaluated using two datasets (Table 3.1 and illustrated in Figure 3.2): (i) Dataset A [10], comprising 6 GNSS traces from outdoor urban environments and simulated attacks, and (ii) Dataset B was collected in a real GNSS-attack environment, Jammertest 2024, in Bleik village, Norway [90]. GNSS receivers are mounted on vehicles with speeds ranging from 0 to 90 km/h. The error for benign GNSS positions is mostly within 3–10 meters for autonomous vehicles and smartphones in the test.

Four state-of-the-art methods as baselines can be implemented with the collected opportunistic information: Signals of Opportunity (SOP, Baseline 1) [54], Kalman Filter (KF, Baseline 2) [91], Particle Filter (PF, Baseline 3) [92], and Combined Metrics (GLRT, Baseline 4) [56]. To perform a fair comparison with the baseline methods, three cases (variants) are included: (i) exclusive utilization of network-based positioning results, termed PADS-N, (ii) sole reliance on onboard sensors, termed PADS-O,

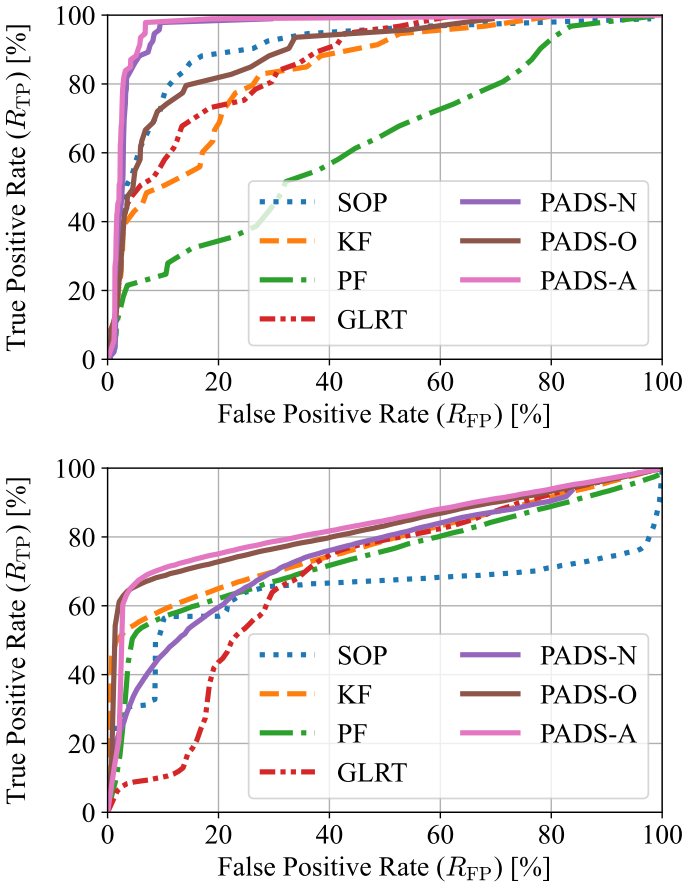


Figure 3.3: Receiver-operating characteristic (ROC) curves for Dataset A (upper) and B (lower), i.e., R_{TP} versus R_{FP}, as it appears in Paper F.

and (iii) combined usage of network positions and onboard sensors, termed PADS-A.

PADS-N shares the same network conditions as Baseline 1. As shown in Figure 3.3, PADS-N exhibits a modest improvement, at most 33%, when $R_{\text{FP}} < 15\%$. In Dataset A, it achieves R_{TP} of 81–96% when R_{FP} is 5–15%, compared to 63–87% for Baseline 1. In Dataset B, it achieves R_{TP} of 36–54% when R_{FP} is 5–15%, similar to 33–57% for Baseline 1. When $R_{\text{FP}} > 10\%$, PADS-N has at most 20% performance gain. Furthermore, the performance with Dataset A is better than that with B because network positions are much sparser and noisier in Dataset B. In general, as R_{FP} increases, R_{TP} tends to increase and converge for both PADS-N and signals of opportunity (SOP), both methods detecting the attacks well and thus resisting gradual deviation or position jumping spoofing.

PADS-O, KF (Baseline 2), and PF (Baseline 3) use GNSS position, incorporating motion data from onboard sensors. Figure 3.3 illustrates R_{TP} as a function of R_{FP}. PADS-O and Baseline 2 maintain relatively consistent and similar trends of R_{TP}. However, in both Dataset A and B, Baseline 2 and Baseline 3 indicate relatively low R_{TP}, even at higher R_{FP}. PADS-O outperforms them with at most a 44% R_{TP} gain in Dataset A and 23% in B, when R_{FP} is 5–15%. This is because the spoofed positions will influence the filters, while the proposed scheme detects and screens the spoofed position simultaneously. Furthermore, the regression in PADS-O can not only deal with Gaussian noise but also general zero-mean noise, according to the least squares assumptions. Whenever the noise is not zero-mean, PADS-O detects it as an anomaly caused by spoofing.

Compared to PADS-A, generalized likelihood ratio test (GLRT) (Baseline 4) struggles due to the absence of rolling window and motion-constrained regression for position data, hindering the effective fusion of heterogeneous data (i.e., positions, velocity, and acceleration). When utilizing all available opportunistic information sources, PADS-A consistently surpasses Baseline 4 across R_{FP}.

Given that the proposed position-based attack detection scheme can operate in a software-only way without any hardware modifications and does not rely on low-level hardware, its compatibility with other signal-level or cryptographic countermeasures is seamless. Incorporating this algorithm into existing consumer-grade devices is easy, making it convenient for deployment alongside other security measures to provide a multi-layer defense. With positions and motion information as its only inputs, both commonly available in consumer-grade mobile platforms, the algorithm can opportunistically validate GNSS positions whenever network-based positions are accessible, providing a versatile and easily implementable solution for GNSS attack detection.

3.2.2 Self-supervised federated learning for detection

To overcome the limitations of labeled datasets and privacy concerns in deep learning-based detection, a novel self-supervised federated learning framework is proposed for GNSS spoofing detection, and this framework is supervised by labels generated from the scheme in Section 3.2.1. It allows multiple mobile platforms to collaboratively train a robust detection model using long short-term memory (LSTM) networks, without sharing sensitive raw location data.

Paper D considers multiple mobile GNSS platforms (e.g., smartphone, car, and drone) equipped with common modules (e.g., Wi-Fi, Bluetooth, cellular, IMU, and speed sensors), and streaming signal-level properties from satellites (automatic gain control (AGC), antenna carrier to noise density ratio (C/No), baseband C/No, and Doppler shift). The platforms are connected to a cloud server, which is curious but honest, so sharing datasets that contain location, motion, and network information with the cloud server or other mobile platforms is not acceptable. In the event of a GNSS position attack, when a mobile platform moves and navigates within the attacked area (which is unknown to both the platform and the server), the GNSS-provided location will deviate from the actual location. As a result, network-provided positions, motion information, and signal-level properties will be inconsistent with GNSS position information and its benign behavior. Acknowledging that mobile platforms may differ

in their navigation areas and hardware, there are so-called non-independent and identically distributed (i.i.d.) data situations. Similarly, if the hardware were the same and the navigation traces were similar, the data could be considered i.i.d..

The proposed framework consists of two main parts: a server part and an edge client part. The server part is a cloud server responsible for tasks such as housing the global detector model and model aggregation. The edge clients' part involves numerous local mobile platforms, each equipped with a self-supervised anomaly detector model. These models utilize LSTM networks, which are also well-suited for capturing temporal dependencies in sequential data. Each platform processes a local dataset, which includes time-series information collected from GNSS receiver (GNSS position, AGC, C/No, Doppler shift, etc.), network infrastructures (network position), and onboard sensors (acceleration, attitude, etc.). The self-supervised model is trained using the spoofing-deviation labels generated from the method in [1]. The local mobile platforms do not upload their local datasets to the cloud server. Instead, they transmit only the parameters of their respective local models. Upon receiving these parameters, the cloud server performs model aggregation by combining them into a single global model using the FedAvg algorithm. The aggregated global model is distributed back to the mobile platforms and then trained again.

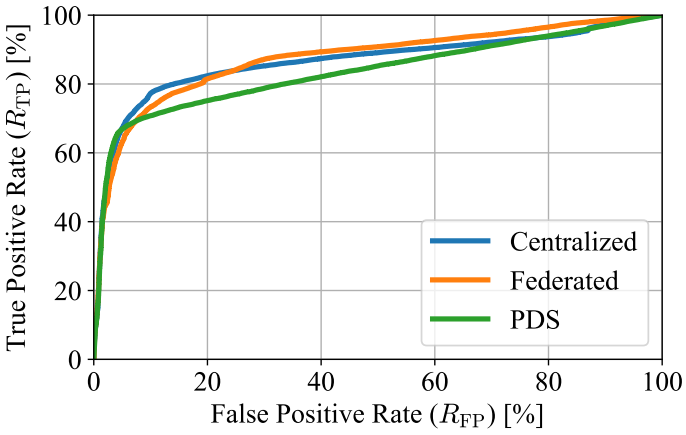


Figure 3.4: ROC curves of the centralized and federated self-supervised detection, and the position-based detection, as it appears in Paper D.

In the experimental evaluation, GNSS spoofing data is collected by the NSS field campaign at Jammertest 2024 [90] using six vehicle-mounted smartphones. Phone 1 and Phone 4 are Google Pixel 8. Phones 2 and 6 are Google Pixel 4 XLs. Phone 3 is a Xiaomi Redmi 9, and Phone 5 is a Samsung Galaxy S9. All smartphones support multiple constellations, while only the Google Pixel 4 XL and Pixel 8 support double frequencies. The dataset consists of 85 drive-testing traces in total, recorded throughout the day, from morning to evening, around the Bleik town area. The smartphones record timestamps, GNSS positions, network positions, IMU data, and GNSS signal properties (AGC, antenna C/No, baseband C/No, and Doppler shift) via Android APIs.

Ground truth positions are obtained from two u-blox ZED-F9P receivers using benign constellations with the help of a nearby reference station. Labels for self-supervised learning are generated locally through the opportunistic data fusion algorithm [1]. The deep learning framework is Keras with a TensorFlow backend, and it chooses the LSTM module to process time series data, allowing it to capture temporal dependencies in the features. Regarding the federated learning part, the FedAvg algorithm is implemented on the cloud server to average all local model parameters. It is important to note that processing overhead, transmission delays, or packet loss in wireless communications between the server and clients were not simulated in this evaluation.

ROC curves for the methods of position fusion, centralized training, and the proposed federated learning are shown in Figure 3.4. The centralized training curve has an area under the curve (AUC) value of 86.6%. The federated learning curve's AUC is 87.4%, while the curve of position-based detection is 83.5%. This comparison shows that the self-supervised learning-based approach outperforms the baseline method, and validates that federated learning can achieve competitive performance compared to centralized training. Furthermore, the proposed scheme has at most 10% true positive rate gain over PDS [1] in Figure 3.4, and preserves location data privacy. Centralized training achieves a higher accuracy than federated one, when $R_{\text{FP}} < 10\%$. This phenomenon is common in federated learning because data samples are sequential and shuffled across batches during centralized training. In contrast, federated learning involves parallel training across clients, where each client trains on relatively unrefined models and locally available data. As a result, the model struggles to generalize effectively, as it fails to capture shared patterns across the entire dataset.

This detection method is self-supervised and federatively trained by multiple devices that provide heterogeneous traces and opportunistic data. Unlike existing deep learning-based detections, the proposed method does not require manual annotation for training data, meaning that its training process is self-supervised by the labels generated from a traditional detection, PDS [1]. Notably, while PDS provides training labels for the proposed federated detection, the proposed method outperforms PDS in accuracy. Additionally, without compromising privacy, each device transmits only model parameters, rather than position-related data. The proposed federated detection can also be generalized to different situations, devices, smartphone models, and driving traces, and performs robustly on i.i.d. and non-i.i.d. data.

3.3 Countermeasures for other positioning signal attacks

Beyond GNSS, other positioning infrastructures are also vulnerable. The work in this section addresses these specific attack vectors in Wi-Fi and Li-Fi.

3.3.1 Position-based rogue Wi-Fi detection

Wi-Fi positioning, widely used in indoor and urban environments, is susceptible to rogue AP attacks where unauthorized APs mimic legitimate ones. This work proposes a position-based rogue AP detection scheme. This method generates multiple position estimates from different subsets of observed Wi-Fi RSSI values. By combining these estimates into Gaussian mixtures and cross-validating their consistency, inconsistencies indicative of a rogue AP can be identified. This approach enhances detection accu-

racy significantly compared to traditional RSSI-based clustering or anomaly detection methods and enables the exclusion of rogue APs for more robust positioning.

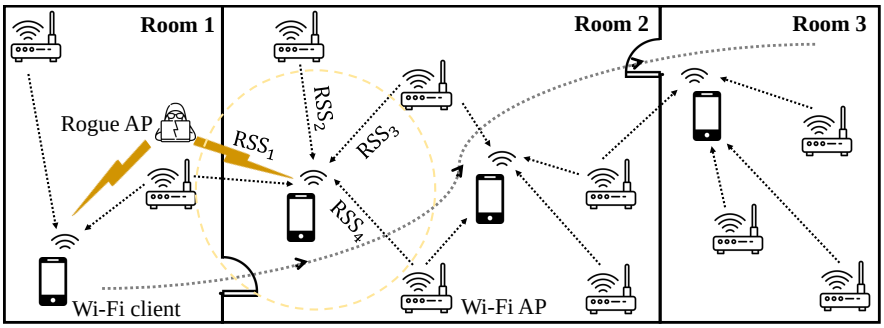


Figure 3.5: The mobile Wi-Fi client in the dashed yellow circle can locate itself using four RSSIs from AP in range, as it appears in Paper C.

Paper C considers a mobile Wi-Fi device illustrated in Figure 3.5, with unknown position—the device can be held by a security patrol person from the network provider or be a user device (e.g., a smartphone). The client actively explores Wi-Fi APs and gathers beacon information from them. Although the client is indoors, walking and without GNSS reception, it is assumed that pre-surveyed data is available, depending on the requirements of the Wi-Fi positioning algorithm. The data can be: (i) a fingerprint database of RSSIs, or (ii) a list of AP positions.

In the first component of the scheme, Wi-Fi RSSI subsets are generated without presuming a known number of rogue APs, considering all possible combinations of APs, varying in size—from the minimum to the maximum allowable for the given positioning algorithm. Given that the number of subsets can be large, a straightforward sampling strategy is employed: a random selection of subsets is made, with each subset chosen based on a predetermined probability distribution. Then, the positioning algorithm compares each RSSI subset with the fingerprint database or uses geolocation localization [93] to return the estimated latitude, longitude coordinates, and height of the receiver. In the second component, the scheme combines all position estimations of the Wi-Fi RSSI subsets to fuse a temporary position. Based on this temporary position, rogue AP detection and exclusion are carried out by analyzing the deviation between each positioning estimation and the fused one. Finally, an ultimate position is estimated based on the APs after exclusion.

The dataset for the experiments was collected on the fourth floor of a shopping mall, covering an area of 170 by 90 m [94]. 8 APs are visible at each position, while the landmarks and AP positions were used to generate trajectories. The device WHUWearTrack was employed for trajectory acquisition as ground truth, incorporating a low-cost IMU, a Bluetooth module, and a multiprotocol system-on-chip. The reference trajectories have decimeter-level positioning accuracy. The Wi-Fi positioning algorithm from [94] exhibits meter-level accuracy. To simulate attacks, rogue AP signals were generated by modifying RSSI data. Specifically, 16 traces containing rogue AP signals were generated for each attack, resulting in a total of 48. In the attack detection results, the

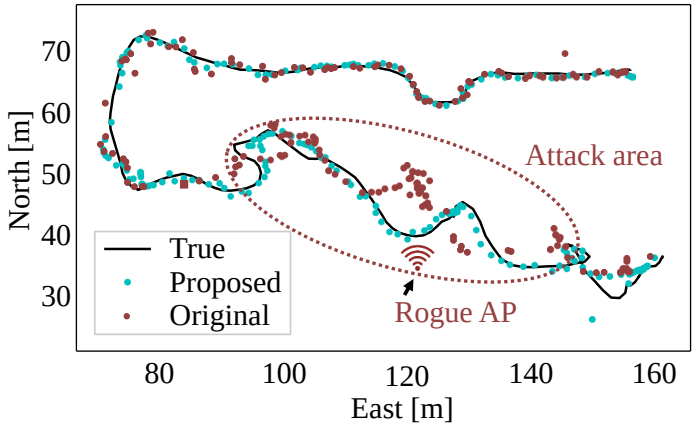


Figure 3.6: An illustration of the positioning results before (i.e., original) and after (i.e., proposed) exclusion, as it appears in Paper C.

proposed detection consistently achieves a higher true positive rate (67% to 97%) compared to the clustering-based and ECOD-based detection methods [95, 96]. Clustering-based detection exhibits low rates (below 21%) across all cases. While ECOD-based detection shows some improvement over clustering-based detection, it still falls short of our proposed approach variants. Then, in the position recovery, the indoor Wi-Fi positioning algorithm, which relies solely on benign RSSI measurements, estimates the client's position accurately. The effectiveness of position recovery can be evaluated by comparing the reference positions (ground truth) with the positioning results obtained before and after the exclusion of the rogue APs. This comparison enabled an assessment of the accuracy of the client's position estimation and, naturally, how rogue AP detection and exclusion enhance the accuracy of the Wi-Fi positioning system. The positioning results before and after rogue APs exclusion are visually represented in Figure 3.6. The red solid dots represent the original Wi-Fi positioning results, illustrating the deviation of the attack area from the actual path, which is drawn as a black line. In contrast, the cyan-blue solid dots represent the results of the proposed method, which exhibit much lower deviation.

This scheme can work either as a tool used by wireless network operators for actively monitoring APs or by mobile users that can independently detect rogue APs. The only need is RSSI to make the scheme compatible with other rogue AP detection schemes. The novelty lies in adopting and adapting the RAIM used in GNSS to achieve rogue Wi-Fi AP detection, and thus this approach is termed Gaussian mixture RAIM. It exploits position fusion from Wi-Fi positioning algorithms and rogue AP exclusion strategies. Paper C demonstrated significant improvements based on numerical experiments and comparative analysis using a partially real-world Wi-Fi RSSI dataset over baseline rogue AP detection schemes.

3.3.2 Interference-resilient optical wireless positioning

Emerging positioning technologies, such as optical wireless positioning, offer high accuracy and electromagnetic immunity but face their own interference challenges. A need exists for an interference-resilient positioning framework enhanced with machine learning. This framework leverages subset filtering and reliability-aware fusion of RSSI inputs. It detects anomalies, excludes corrupted signals, and aggregates reliable estimations to restore positioning accuracy even in the presence of spectral interference. This framework is detailed in Paper G, demonstrating the potential for robust positioning in environments beyond traditional radio frequencies.

To support simultaneous optical wireless communication and positioning, Paper G considers employing the downlink channel for data transmission, while utilizing the uplink channel for positioning and communication. Specifically, the indoor positioning environment is equipped with multiple ceiling-mounted angle diversity receivers facing downward, whose novel design ensures that, regardless of the user equipment position, at least one photodetector surface is oriented toward it. The user carries an infrared-light-emitting diode (LED) that transmits a multi-carrier on-off keying-frequency division multiplexing signal. Each receiver is assigned to a distinct subcarrier and independently records and stores the RSSI corresponding to that subcarrier. The total channel gain between the infrared-LED and each angle diversity receiver is calculated, based on which, the signal-to-noise ratio at each receiver is derived.

In conventional machine learning-based optical wireless positioning systems, the RSSI at each receiver is directly used to train neural networks for position estimation. In the proposed interference-aware scheme, the concept of RSSI subsets is introduced. The scheme does not require prior knowledge of the number or locations of interferences but instead generates all possible combinations of RSSI indices, with subset sizes varying from a minimum threshold—ensuring sufficient positioning information—to the full set. Each subset provides a position estimation and is treated as a Gaussian-distributed localization hypothesis. A temporary position estimate is computed via uncertainty-aware fusion of all subsets. Then, subsets exhibiting excessive deviation are considered unreliable and are excluded from the final fusion. To validate the performance of the proposed method under practical conditions, a MATLAB-based simulated positioning system is first constructed to generate training data. In this setting, 1000 test samples were generated in MATLAB to evaluate the system, resulting in an average Euclidean positioning error of only 0.947 centimeters. The proposed interference identification mechanism successfully detected overlapping spectral channels between the interference sources and the target user, achieving a success rate of 99.3% across 1000 test samples. Meanwhile, real-world experiments were conducted, and the system consistently identifies the overlapping channels in every test.

This design introduces the first concept of subset-based RSSI interference mitigation in machine learning-based optical wireless positioning. It further develops and experimentally validates a reliability-aware subset fusion mechanism that detects anomalies, excludes corrupted signals, and aggregates reliable estimations to restore positioning accuracy.

3.4 Countermeasures for simultaneous GNSS and other signal attacks

The most challenging scenario involves coordinated attacks that simultaneously compromise GNSS and other positioning infrastructures. This work addresses this by designing and detecting such multimodal attacks, then mitigating them.

3.4.1 Securing fused positioning against coordinated attacks

This work analyzes the vulnerabilities inherent in location-based service (LBS) applications that rely on location fusion from multiple sources, and implements "Coordinated Location Falsification Attacks" where GNSS, Wi-Fi, cellular, and IP geolocation are simultaneously manipulated to be mutually consistent, thereby deceiving advanced security mechanisms. To counter these, an extended RAIM framework is proposed leveraging all available opportunistic information. This scheme generates diverse subsets of ranging information, computes temporary position estimates, and refines them using onboard sensor data. These refined estimates, along with their associated uncertainties, are fused into a composite likelihood function to identify inconsistencies indicative of coordinated attacks. This approach proves effective even when multiple information sources are untrusted. The design of these attacks and their robust countermeasures are comprehensively discussed in [2, 5] and further elaborated in [8], emphasizing the robust fusion of heterogeneous signals.

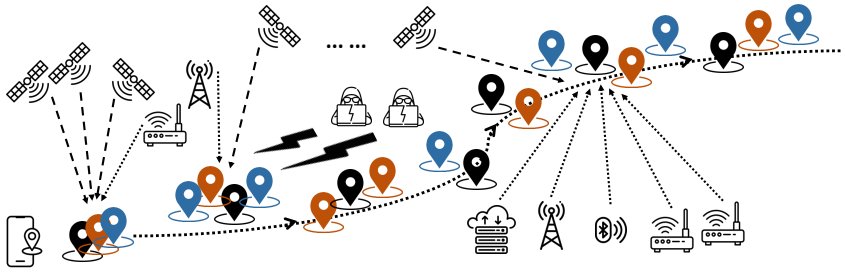


Figure 3.7: LBS applications have ranging information with anchor positions from GNSS and network infrastructures, as it appears in Paper E.

As shown in Figure 3.7, Paper B, Paper E, and Paper H consider LBS deployed on mobile platforms (e.g., smartphone, tablet, or intelligent vehicle) that can process both GNSS and other opportunistic signals to position themselves. At time t, the true position of the platform is estimated by using GNSS and opportunistic information to compute the fused position. Opportunistic information includes wireless signals received from network modules (e.g., Wi-Fi, cellular networks), Bluetooth, GeoIP, as well as motion data from onboard sensors (e.g., IMUs or wheel speed sensors). Position estimates from different sources have varying accuracy; however, in benign conditions without any attacks, these estimates are expected to be consistent. If position manipulation occurs, significant deviations between the fused position and the true position are expected.

Considering high-quality GNSS simulators cost thousands of dollars, the price of an software-defined radio (SDR) is at least hundreds of dollars, and these instruments are not portable to moving targets (e.g., Uber or DiDi on smartphones), Paper E proposes Wi-Fi spoofing mixed with GNSS jamming. Instead of jamming GNSS at the beginning, legitimate GNSS signals are continuously jammed throughout the entire duration of the attack. Concurrently, a commercial Wi-Fi router (Linksys WRT1200AC) is used to replay prerecorded Wi-Fi beacons from an intended spoofing trajectory. The Python script for this location spoofing is available below, designed for compatibility with Wi-Fi routers installed with the OpenWrt system and enabled virtual APs. Lastly, the fusion algorithms of LBS applications, upon losing GNSS signals, default to Wi-Fi-based positioning, thereby accepting the spoofed positions.

Listing 3.1: Wi-Fi location spoofing script tested on a consumer-grade router installed OpenWrt system and enabled virtual APs. It broadcasts Wi-Fi beacons of `ap_set`.

```
def uci_set_wifi (ap_set):
    # ap_set is either prerecorded or obtained from WiGLE.net for
        the targeted spoofing position
    ap_set = ap_set.replace(np.nan, '', regex=True)
    ssh.exec_command("sed␣-i␣'37, $d'␣/etc/config/wireless")
    for i in range(len(ap_set)):
        cmd_to_execute = "uci␣batch␣«␣EOF\n"
        cmd_to_execute += f"""
            set wireless.wifinet{i}=wifi-iface
            set wireless.wifinet{i}.device='radio1'
            set wireless.wifinet{i}.mode='ap'
            set wireless.wifinet{i}.ssid='{ap_set.loc[i,"SSID"]}'
            set wireless.wifinet{i}.encryption='psk2'
            set wireless.wifinet{i}.macaddr='{ap_set.loc[i,
                "BSSID"]}'
            set wireless.wifinet{i}.key='Password'
            """
        cmd_to_execute += "commit\nEOF"
        ssh.exec_command(cmd_to_execute)
    ssh.exec_command("wifi␣reload")
```

While GNSS spoofing, other positioning signal attacks, and Wi-Fi spoofing with GNSS jamming can manipulate the positions of most LBS applications, they can be detected using the aforementioned countermeasures. Hence, Paper E further proposes coordinated location spoofing. It uses a GNSS simulator alongside a Wi-Fi router (Linksys WRT1200AC) to generate and broadcast GNSS signals and Wi-Fi beacons (retrieved from public databases [97]) at a predetermined spoofed position. Additionally, a Wi-Fi router relays all TCP and UDP packets to a cloud server located near the spoofed position using the iptables tool. The iptables configurations are provided in Listing 3.2.

In turn, Paper B, Paper E, and Paper H also propose an extended RAIM method leveraging opportunistic information to detect LBS position manipulation scams. This approach integrates multiple information sources, including GNSS, SOP (Wi-Fi, cellular, Bluetooth, GeoIP, etc.), and motion (speed, acceleration, and orientation), to improve

Listing 3.2: An example of iptables rules for a proxy server running on the IP <TARGET_IP> and port 12345. The iptables tool on the router will relay all TCP and UDP packets to a cloud server near the spoofed position.

```
# Policy Routing Setup
ip rule add fwmark 1 table 100
ip route add local 0.0.0.0/0 dev lo table 100
# Proxy for LAN Devices
iptables -t mangle -N LAN
iptables -t mangle -A LAN -d 127.0.0.1/32 -j RETURN
iptables -t mangle -A LAN -d 224.0.0.0/4 -j RETURN
iptables -t mangle -A LAN -d 255.255.255.255/32 -j RETURN
iptables -t mangle -A LAN -d 192.168.0.0/16 -p tcp -j RETURN
iptables -t mangle -A LAN -d 192.168.0.0/16 -p udp ! -dport 53 -j
    RETURN
iptables -t mangle -A LAN -j RETURN -m mark -mark 0xff
iptables -t mangle -A LAN -p udp -j TPROXY -on-ip <TARGET_IP> -
    on-port 12345 -tproxy-mark 1
iptables -t mangle -A LAN -p tcp -j TPROXY -on-ip <TARGET_IP> -
    on-port 12345 -tproxy-mark 1
iptables -t mangle -A PREROUTING -j LAN
```

detection accuracy. By systematically integrating diverse ranging information into subsets corresponding to heterogeneous infrastructures, the fusion process captures the diverse statistical characteristics (e.g., range, uncertainty, accuracy) of different signal types. Temporary position estimation for each subset is computed using the corresponding positioning algorithm and then smoothed using movement information from onboard sensors. By comparing the fused position with uncertainty against the original temporary estimations from subsets, the scheme assesses the likelihood that ranging information has been manipulated. The proposed scheme includes two primary stages: subset generation and position fusion. In the first stage, real-time ranging information is collected from multiple infrastructures. Subsets are created by combining ranging information associated with known anchor positions, in which Wi-Fi service set identifiers (SSIDs) can be filtered using an large language model (LLM)-based semantics-matching technique. A sampling strategy is also employed to limit the total number of subsets, thereby reducing computational overhead. Finally, temporary position estimates are computed for each subset and infrastructure. In the second stage, onboard sensors collect speed, acceleration, and orientation data to refine temporary position estimates from the first stage. The polynomial regression filtering process smooths position estimations by incorporating physical constraints derived from the platform's kinematic behavior. The filtered positions are then fused with their positioning uncertainties, represented as probability density functions. A composite function is derived from these densities to enable probabilistic cross-validation and exclusion of manipulated signals.

In the evaluation, an over-the-air testbed for isolated wireless attacks on mobile devices is proposed and illustrated in Figure 3.8, and three datasets (from Jammertest 2024, controlled indoor spaces, and an outdoor testbed) are collected in the format as Table 3.2 and Table 3.3. Performance metrics include the accuracy of detecting at-

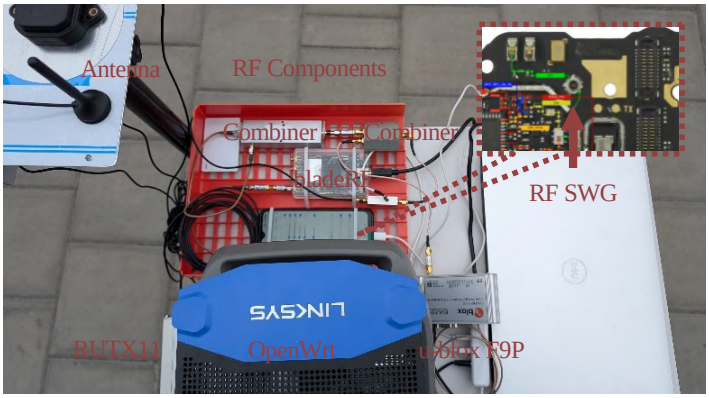


Figure 3.8: Implementation of the secure and isolated over-the-air testbed, as it appears in Paper H.

Table 3.2: Format of the derived major features from GNSS raw measurements, as it appears in Paper H.

Time Information	Unix Time [ms]
Distance/Speed	Pseudorange [m]
	Pseudorance Uncertainty [m]
Satellite Status	Satellite Identifier
	Signal Type
	Satellite Location [m,m,m]

tacks, the accuracy of excluding the ranging information under attack, the number of false alarms, and the accuracy of position recovery. The testbed is composed of a testing phone, a bladeRF 2.0 micro xA9, a Linksys WRT1200AC Wi-Fi router installed with OpenWrt, a u-blox EVK-F9P receiver, a u-blox ANN-MB1-00 antenna, a Teltonika RUTX11 4G router, an XPS laptop installed with Windows 11, and RF cables, attenuators, and connectors (LMR195, LMR400, RG316). The testing phone has an SWG-type RF switch connector, and it was modified to connect a cable with an SMA connector. First, the laptop generates global positioning system (GPS) spoofing signals using the bladeGPS tool for real-time signal generation [23]. Simultaneously, the Wi-Fi router is coordinated to generate beacons to spoof network positioning [5]. The ANN-MB1-00 antenna is powered by 5-volt direct current and transmits benign live sky L1+L5 GNSS signals. Second, benign and attack GNSS signals are combined with 30 dB attenuation and fed into the testing phone[1]. Meanwhile, benign GNSS signals without attenuation are fed into the u-blox receiver as a reference. The receiver is configured to perform precise positioning with the help of our real-time kinematic (RTK) station. In the Jammertest 2024 dataset, the proposed method improves the true positive rate by 9% to

[1]Given that Wi-Fi operates in an unlicensed spectrum, we broadcast them instead of using wired connections.

Table 3.3: Format of the major features from network raw measurements, as it appears in Paper H.

Time Information	Unix Time [s]
Ranging Information	Signal Strength [dB]
	Signal Frequency [Hz]
Cellular Status	Mobile Country Code
	Mobile Network Code
	Cell Identifier
	Cellular Base Station Location [m,m,m]
Wi-Fi Status	Medium Access Control
	Service Set Identifier
	Wi-Fi Access Point Location [m,m,m]
Bluetooth Status	Medium Access Control
	Service Set Identifier
	Bluetooth Device Location [m,m,m]

18% compared to Google Play location and network-based detection, when the false positive rate is between 5% and 10%. This confirms that as long as GNSS precision is favorable (GNSS positions are more precise than those based on network positioning), Google Play location prioritizes GNSS even when spoofed. However, datasets of coordinated attacks are more challenging than GNSS spoofing, and the accuracy in detecting coordinated attacks is lower than the detection for Jammertest.

Paper E implements coordinated attacks at low cost on the most popular location providers and illustrates real-world LBS position manipulations[2]. Subsequently, it develops a RAIM-based framework for detecting and mitigating threats from these coordinated position attacks. By integrating opportunistic information from multiple sources, this approach provides a likelihood function against GNSS spoofing, rogue Wi-Fi APs, etc. The numerical results demonstrate its effectiveness and practicality without relying on any trusted source. However, due to legal restrictions on outdoor GNSS spoofing, these results largely relied on simulations. Furthermore, few existing efforts have developed a testbed capable of supporting multimodal evaluation. Hence, Paper H addresses this gap by designing a secure and isolated over-the-air testbed that supports outdoor testing of multiple attacks on wireless signals. This work also includes a more comprehensive analysis of the detection theory, computational complexity, and experimental validation.

3.4.2 RAIM-supervised federated detection against multimodal attacks

Building upon the RAIM concept and deep learning, this work proposes extending the detection of multimodal location attacks to handle untrusted opportunistic informa-

[2] https://doi.org/10.5281/zenodo.15437800

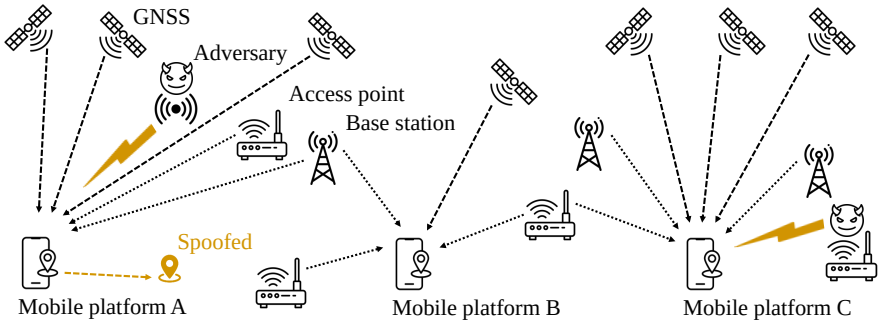


Figure 3.9: System model illustration: multiple mobile platforms and spoofers, as it appears in Paper I.

tion sources. Paper D assumes benign satellite signals, but Paper I embraces the possibility of adversarial manipulation across GNSS, Wi-Fi, and cellular signals. To overcome the limitations of labeled datasets and privacy concerns in deep learning, Paper I uses a self-supervised federated detection framework similar to Paper D.

This work considers multiple mobile platforms (e.g., smartphone, car, and drone) equipped with common modules (e.g., GNSS, Wi-Fi, Bluetooth, cellular, IMU, and speed sensors), and streaming signal-level properties from satellites (AGC, antenna C/No, baseband C/No, and Doppler shift). As shown in Figure 3.9, in the presence of a multimodal location attack (using GNSS/Wi-Fi jamming/spoofing), when the mobile platform moves and navigates within the attacked area, the fused location will deviate from the actual location. Additionally, the training data (encompassing the GNSS receiver, network infrastructures, and onboard sensors) is not manually labeled or annotated to indicate whether it is "benign" or "under attack".

Paper I uses a federated self-supervised learning-based detection framework, as depicted in Figure 3.10. This framework enables effective collaboration and online knowledge sharing among mobile platforms while safeguarding user data privacy. First, the mobile platforms collect (possibly attacked) ranging information from all available infrastructures and motion data from onboard sensors, including speed, acceleration, and orientation. Each platform constructs its own local dataset and trains an LSTM regression model using the generated labels from the extended RAIM [5, 98], and then uploads the model parameters to the cloud server. The cloud server employs the FedAvg algorithm to aggregate model parameters trained on distributed datasets, thereby improving both the accuracy of spoofing detection and data privacy.

In terms of privacy-preserving computing, compared to traditional centralized deep learning solutions, where uploading raw location data is required, the proposed method utilizes a self-supervised federated learning framework, where local devices only upload model parameters (i.e., LSTM weights), thus preventing the leakage of sensitive location and motion information. Labels are automatically generated using the local RAIM algorithm, eliminating the need for manual labeling. Global model parameters are aggregated using FedAvg, achieving a balance between privacy and collaboration. In terms of communication efficiency, compared to solutions that

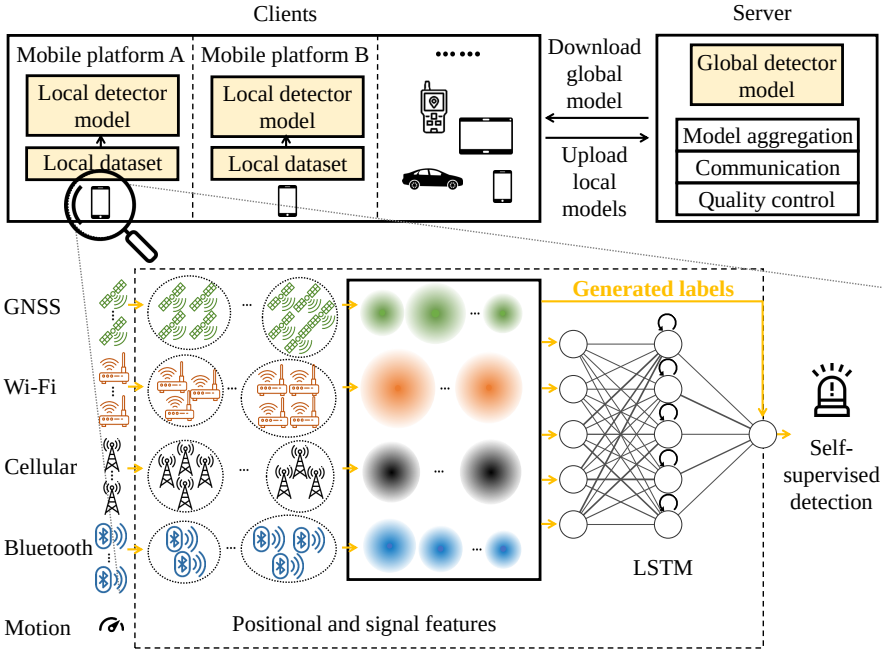


Figure 3.10: Overview of federated self-supervised multimodal location spoofing detection, as it appears in Paper I. Mobile platforms locally generate labels using an extended RAIM, train LSTM models on multimodal features, and upload model parameters to a cloud server for FedAvg aggregation, as it is included in Paper I.

homomorphically encrypt data, the proposed framework requires only one round of communication per aggregation, and the transmitted payload is lightweight model parameters (approximately 100-dimensional LSTM weights). For example, a single parameter update on a Google Pixel 8 device requires only approximately 600 KB of data, reducing the communication overhead by 90% compared to transmitting homomorphically encrypted raw data. In terms of protection against real-world attacks, based on a real-world spoofing attack experiment conducted at Jammertest 2024, the proposed method effectively defends against gradual drift, replay attacks, and other similar threats. By analyzing signal feature statistics (mean, median, and extreme values) and motion consistency, the model can identify deceptive signal power characteristics (such as abnormal increases in C/N0) and trajectory mutations.

4 Conclusions and future work

This thesis has investigated the critical problem of securing cyber-physical system (CPS) positioning algorithms against a spectrum of sophisticated attacks, ranging from global navigation satellite system (GNSS)-specific manipulations to coordinated assaults across heterogeneous infrastructures. By systematically leveraging both traditional machine learning and deep learning methods with diverse "opportunistic information" available on modern mobile platforms, this thesis has developed and validated novel defense mechanisms that significantly enhance the robustness and resilience of CPS.

4.1 Summary of contributions

The contributions can be summarized along the three main work areas: For GNSS-specific attacks, Paper A and Paper F introduce probabilistic detection frameworks that utilize opportunistic data from networks and inertial sensors. Further, Paper D pioneers a self-supervised federated learning approach for privacy-preserving and highly accurate GNSS spoofing detection, demonstrating its generalization capabilities across diverse devices and real-world traces. For attacks on other positioning signals, Paper C develops a position-based rogue access point (AP) detection scheme for Wi-Fi, effectively identifying and excluding malicious Wi-Fi signals using a Gaussian mixture receiver autonomous integrity monitoring (RAIM) approach. Paper G also explores advanced interference-resilient positioning in emerging optical wireless positioning systems, showcasing robust performance against spectral interference. For simultaneous GNSS and other signal attacks, Paper E and Paper H design and demonstrate sophisticated coordinated location falsification attacks that bypass conventional multi-source validation mechanisms. To counter these, Paper B, Paper E, Paper H, and Paper I propose and validate an extended RAIM framework based on Gaussian mixtures, capable of fusing heterogeneous and potentially untrusted opportunistic information to secure positioning against multimodal adversaries.

Collectively, these contributions provide practical and effective solutions for safeguard-

ing the integrity of position information, mitigating the impact of location attacks, and ensuring the continued reliability of location-based service (LBS) in increasingly challenging environments.

4.2 Future directions

While this thesis has made significant efforts in advancing location security, several exciting avenues for future research remain:

Given the heterogeneous capabilities of clients (e.g., low-end or high-end smartphones, dynamic network conditions, and various sensor quality), adaptive and real-time deployment are crucial factors to consider. For example, the proposed federated learning framework distributes computational tasks from the server to clients, thereby consuming a significant amount of computational power and battery life on the clients. Hence, further exploration is needed in model compression, quantization, adaptive client participation, training task scheduling, and communication efficiency optimization.

Stronger adversaries might also be a future challenge. Current work assumes the presence of benign onboard sensors, the availability of benign ranging information for some period, benign mobile platforms, and so on. However, more advanced and stealthier attack strategies would include inertial measurement unit (IMU) data injection, vulnerability exploitation in the underlying operating system, and wideband jamming that removes all benign signals. Future work should explore the combination with other detectors, such as signal-based, solution-based, and cryptography-based detectors.

As quantum computing advances, the security of current cryptographic primitives used in authenticated GNSS signals may be compromised. Future work could explore the integration of quantum-resistant cryptographic algorithms into Positioning, Navigation and Timing (PNT) authentication mechanisms.

Beyond detection, localization and characterization of attack sources (e.g., GNSS spoofers or rogue APs) using mobile platforms could contribute to rapid response and mitigation strategies. This could leverage distributed sensing and machine learning methods.

Bibliography

[1] Wenjie Liu and Panos Papadimitratos. “Probabilistic Detection of GNSS Spoofing Using Opportunistic Information”. In: *Proc. IEEE/ION PLANS*. Monterey, CA, USA, Apr. 2023.

[2] Wenjie Liu and Panos Papadimitratos. “Extending RAIM with a Gaussian Mixture of Opportunistic Information”. In: *Proc. ION ITM*. Long Beach, CA, USA, Jan. 2024.

[3] Wenjie Liu and Panos Papadimitratos. “Position-Based Rogue Access Point Detection”. In: *Proc. IEEE EuroS&PW*. Vienna, Austria, July 2024.

[4] Wenjie Liu and Panos Papadimitratos. “Self-Supervised Federated GNSS Spoofing Detection with Opportunistic Data”. In: *Proc. IEEE/ION PLANS*. Salt Lake City, UT, USA, Apr. 2025.

[5] Wenjie Liu and Panos Papadimitratos. “Guardian Positioning System (GPS) for Location Based Services”. In: *Proc. 18th ACM WiSec*. Arlington, VA, USA, June 2025.

[6] Wenjie Liu and Panos Papadimitratos. “GNSS Spoofing Detection Based on Opportunistic Position Information”. In: *IEEE Internet Things J.* 12.17 (2025), pp. 36168–36182.

[7] Yifan Huang, Yi Liu, Wenjie Liu, Panos Papadimitratos, Harald Haas, and Iman Tavakkolnia. “Interference-Resilient Optical Wireless Positioning via Machine Learning-Enhanced Subset Filtering”. In: *Proc. 51st ECOC*. Copenhagen, Denmark, Sept. 2025.

[8] Wenjie Liu and Panos Papadimitratos. “Coordinated Position Falsification Attacks and Countermeasures for Location-Based Services”. In: *IEEE Open J. Commun. Soc.* 6 (2025), pp. 9229–9246.

[9] Wenjie Liu and Panos Papadimitratos. “Multimodal Location Spoofing Detection Using Federated Self-Supervised Learning”. In: *IEEE Open J. Commun. Soc.* (2025).

[10] Junjie Shen, Jun Yeon Won, Zeyuan Chen, and Qi Alfred Chen. “Drift with Devil: Security of Multi-Sensor Fusion Based Localization in High-Level Au-

tonomous Driving under GPS Spoofing". In: *Proc. 29th USENIX Security*. virtual event, Aug. 2020.

[11] Qian Bin, Cai Ziwen, Xiao Yong, Hong Liang, and Su Sheng. "GPS Spoofing-Based Time Synchronisation Attack in Advanced Metering Infrastructure and Its Protection". In: *J. Eng.* 2020.9 (2020), pp. 809–815.

[12] Manuel Del Castillo. "Protecting LBS Applications against GNSS Spoofing". In: *Broadcom* (June 30, 2021). URL: https://web.archive.org/web/https://www.broadcom.com/blog/broadcom-bcm47765-gnss-antispoofing-receiver (visited on 06/20/2024).

[13] Sean Barbeau. "GPSTest Database". In: *Google Sheets* (Jan. 23, 2025). URL: https://docs.google.com/spreadsheets/d/1jXtRCoEnnFNWj6_oFlVWflsf-b0jkfZpyhN-BXsv7uo/ (visited on 01/23/2025).

[14] Desmond Schmidt, Kenneth Radke, Seyit Camtepe, Ernest Foo, and Michal Ren. "A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures". In: *ACM Comput. Surv.* 48.4 (2016), pp. 1–31.

[15] Yue Wang. "Ghost Drivers Are Just One of Uber China's Problems following DIDI Takeover". In: *Forbes* (Sept. 27, 2016). URL: https://www.forbes.com/sites/ywang/2016/09/27/ghost-drivers-are-just-one-of-uber-chinas-problems-following-didi-takeover/ (visited on 04/01/2024).

[16] Yiying Fan. "Fare Play: China Targets Ride-Hailing Drivers Using Fraud Software". In: *Sixth Tone* (Jan. 23, 2025). URL: https://www.sixthtone.com/news/1016572 (visited on 03/01/2025).

[17] Jeni Paay, Jesper Kjeldskov, Daniele Internicola, and Mikkel Thomasen. "Motivations and Practices for Cheating in Pokémon GO". In: *Proc. 20th MobileHCI*. Barcelona, Spain, Sept. 2018.

[18] Cihan Eryonucu and Panos Papadimitratos. "Sybil-Based Attacks on Google Maps or How to Forge the Image of City Life". In: *Proc. 15th ACM WiSec*. San Antonio, TX, USA, May 2022.

[19] Ahmet Saim Yilmaz, Haydar Cukurtepe, and KUGU Emin. "Geo-Location Spoofing on E-Scooters; Threat Analysis and Prevention Framework". In: *Balkan J. Electr. Comput. Eng.* 11.4 (2023), pp. 364–372.

[20] Marazzi Michele, Patrick Jattke, Jason Zibung, and Kaveh Razavi. "PayRide: Secure Transport e-Ticketing with Untrusted Smartphone Location". In: *Proc. DIMVA*. Lausanne, Switzerland, July 2024.

[21] Daniele Borio, Cillian O'driscoll, and Joaquim Fortuny. "GNSS Jammers: Effects and Countermeasures". In: *Proc. 6th Navitec*. Noordwijk, Netherlands, Dec. 2012.

[22] Todd E Humphreys, Brent M Ledvina, Mark L Psiaki, Brady W O'Hanlon, Paul M Kintner, et al. "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer". In: *Proc. 21st ION GNSS+*. Savannah, GA, USA, Sept. 2008.

[23] Takuji Ebinuma. *Bladegps*. https://github.com/osqzss/bladeGPS/. 2022.

[24] Adam Harvey. *Skylift: Wi-Fi Geolocation Spoofing with the ESP8266*. https://github.com/adamhrv/skylift. 2016.

[25] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. "On the Impact of Rogue Base Stations in 4G/LTE Self Organizing Networks". In: *Proc. 11th ACM WiSec*. Stockholm, Sweden, June 2018.

[26] Marco Spanghero, Kewei Zhang, and Panagiotis Papadimitratos. "Authenticated Time for Detecting GNSS Attacks". In: *Proc. 33rd ION GNSS+*. virtual event, Sept. 2020.

[27] Marco Spanghero and Panos Papadimitratos. "Detecting GNSS Misbehaviour with High-Precision Clocks". In: *Proc. 14th ACM WiSec*. virtual event, June 2021.

[28] Marco Spanghero and Panos Papadimitratos. "Detecting GNSS Misbehavior Leveraging Secure Heterogeneous Time Sources". In: *Proc. IEEE/ION PLANS*. Monterey, CA, USA, Apr. 2023.

[29] Marco Spanghero and Panos Papadimitratos. "UnReference: Spoofing GNSS Differential Reference Stations and Effects on Connected Rovers". In: *Proc. IEEE/ION PLANS*. Salt Lake City, UT, USA, Apr. 2025.

[30] Sashank Narain, Aanjhan Ranganathan, and Guevara Noubir. "Security of GPS/INS Based On-Road Location Tracking Systems". In: *Proc. IEEE S&P*. San Francisco, CA, USA, May 2019.

[31] Antonello Venturino, Enrica d'Afflisio, Nicola Forti, Paolo Braca, Peter Willett, and Moe Z Win. "Adaptive Resilience Navigation Filter for Detecting and Mitigating Multi-Spoofing Attacks in Range-Based Localization Systems using Antenna Arrays". In: *IEEE Trans. Aerosp. Electron. Syst.* 61.3 (2025), pp. 6856–6872.

[32] Malte Lenhart, Marco Spanghero, and Panos Papadimitratos. "Distributed and Mobile Message Level Relaying/replaying of GNSS Signals". In: *Proc. ION ITM*. Long Beach, CA, USA, Jan. 2022.

[33] Todd E Humphreys. "Detection Strategy for Cryptographic GNSS Anti-Spoofing". In: *IEEE Trans. Aerosp. Electron. Syst.* 49.2 (2013), pp. 1073–1090.

[34] Panagiotis Papadimitratos and Aleksandar Jovanovic. "GNSS-based Positioning: Attacks and Countermeasures". In: *Proc. IEEE Mil. Commun. Conf.* San Diego, CA, USA, Nov. 2008.

[35] Kewei Zhang and Panos Papadimitratos. "On the Effects of Distance-Decreasing Attacks on Cryptographically Protected GNSS Signals". In: *Proc. ION ITM*. Reston, VA, USA, Jan. 2019.

[36] Kewei Zhang, Erik G Larsson, and Panos Papadimitratos. "Protecting GNSS Open Service Navigation Message Authentication against Distance-Decreasing Attacks". In: *IEEE Trans. Aerosp. Electron. Syst.* 58.2 (2022), pp. 1224–1240.

[37] Dennis M Akos. "Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)". In: *J. Inst. Navigation* 59.4 (2012), pp. 281–290.

[38] Aleksandar Jovanovic, Cyril Botteron, and Pierre-Andre Fariné. "Multi-Test Detection and Protection Algorithm against Spoofing Attacks on GNSS Receivers". In: *Proc. IEEE/ION PLANS*. Monterey, CA, USA, May 2014.

[39] Jingxiaotao Fang, Jiang Yue, Bing Xu, and Li-Ta Hsu. "A Post-Correlation Graphical Way for Continuous GNSS Spoofing Detection". In: *Measurement* 216 (2023), p. 112974.

[40] Wenyi Wang and Yinglong Hou. “GNSS Induced Spoofing Detection Based on Dynamic 3-D Correlation Function”. In: *IEEE Trans. Instrum. Meas.* 73 (2024), pp. 1–18.

[41] Song Li, Xiaomei Tang, Honglei Lin, and Feixue Wang. “GNSS spoofing detection based on frequency domain processing”. In: *Measurement* 242 (2025), p. 115872.

[42] GMV. “GNSS Authentication and Encryption”. In: *Navipedia* (Feb. 17, 2021). URL: https://gssc.esa.int/navipedia/index.php/GNSS-Authentication-and-encryption (visited on 03/03/2023).

[43] GMV. “Galileo Open Service Navigation Message Authentication”. In: *Navipedia* (May 21, 2021). URL: https://gssc.esa.int/navipedia/index.php/Galileo-Open-Service-Navigation-Message-Authentication (visited on 03/03/2023).

[44] Mathieu Joerger, Fang-Cheng Chan, and Boris Pervan. “Solution Separation Versus Residual-Based RAIM”. In: *J. Inst. Navigation* 61.4 (2014), pp. 273–291.

[45] Juan Blanch, Todd Walker, Per Enge, Young Lee, Boris Pervan, Markus Rippl, Alex Spletter, and Victoria Kropp. “Baseline Advanced RAIM User Algorithm and Possible Improvements”. In: *IEEE Trans. Aerosp. Electron. Syst.* 51.1 (2015), pp. 713–732.

[46] Shuai Han, Desi Luo, Weixiao Meng, and Cheng Li. “Antispoofing RAIM for Dual-Recursion Particle Filter of GNSS Calculation”. In: *IEEE Trans. Aerosp. Electron. Syst.* 52.2 (2016), pp. 836–851.

[47] Ali Broumandan, Ali Jafarnia-Jahromi, Vahid Dehghanian, John Nielsen, and Gérard Lachapelle. “GNSS Spoofing Detection in Handheld Receivers Based on Signal Spatial Correlation”. In: *Proc. IEEE/ION PLANS*. Myrtle Beach, SC, USA, Apr. 2012.

[48] Shinan Liu, Xiang Cheng, Hanchao Yang, Yuanchao Shu, Xiaoran Weng, Ping Guo, Kexiong Curtis Zeng, Gang Wang, and Yaling Yang. “Stars Can Tell: A Robust Method to Defend against GPS Spoofing Attacks Using Off-the-Shelf Chipset”. In: *Proc. 30th USENIX Security*. virtual event, Aug. 2021.

[49] Wenlong Zhou, Zhiwei Lv, Xu Deng, and Ye Ke. “A New Induced GNSS Spoofing Detection Method Based on Weighted Second-Order Central Moment”. In: *IEEE Sens. J.* 22.12 (2022), pp. 12064–12078.

[50] Marco Spanghero, Filip Geib, Ronny Panier, and Panos Papadimitratos. “GNSS Jammer Localization and Identification With Airborne Commercial GNSS Receivers”. In: *IEEE Trans. Inf. Forensics Secur.* 20 (2025), pp. 3550–3565.

[51] Wenlong Zhou, Zhiwei Lv, Guangyun Li, Bo Jiao, and Wenbo Wu. “Detection of Spoofing Attacks on Global Navigation Satellite Systems Using Kolmogorov-Smirnov Test-Based Signal Quality Monitoring Method”. In: *IEEE Sens. J.* 24.7 (2024), pp. 10474–10490.

[52] Asif Iqbal, Muhammad Naveed Aman, and Biplab Sikdar. “A Deep Learning Based Induced GNSS Spoof Detection Framework”. In: *IEEE Trans. Mach. Learn. Commun. Netw.* 2 (2024), pp. 457–478.

[53] Giulia Michieletto, Francesco Formaggio, Angelo Cenedese, and Stefano Tomasin. “Robust Localization for Secure Navigation of UAV Formations Under GNSS Spoofing Attack”. In: *IEEE Trans. Autom. Sci. Eng.* (2022).

[54] Gabriele Oligeri, Savio Sciancalepore, Omar Adel Ibrahim, and Roberto Di Pietro. “GPS Spoofing Detection via Crowd-Sourced Information for Connected Vehicles”. In: *Comput. Netw.* 216 (2022), p. 109230.

[55] Lu Bai, Chao Sun, Andrew G. Dempster, Wenquan Feng, and Chen Zhuang. “Robust GNSS Spoofing Detection Against UE Maneuver in a GNSS-5G mmWave Hybrid Positioning System”. In: *IEEE Sens. J.* 24.13 (2024), pp. 21237–21253.

[56] Fabian Rothmaier, Yu-Hsuan Chen, Sherman Lo, and Todd Walter. “A Framework for GNSS Spoofing Detection through Combinations of Metrics”. In: *IEEE Trans. Aerosp. Electron. Syst.* 57.6 (2021), pp. 3633–3647.

[57] Marco Spanghero and Panos Papadimitratos. “Time-Based GNSS Attack Detection”. In: *IEEE Trans. Aerosp. Electron. Syst.* 61.3 (2025), pp. 5594–5610.

[58] Haijun Tan, Ning Xie, Lei Huang, and Hongbin Li. “Enhancing GNSS Signal Authentication through Multi-Antenna Systems”. In: *IEEE Trans. on Wireless Commun.* 24.5 (2025), pp. 4361–4376.

[59] Yangjun Gao and Guangyun Li. “A Slowly Varying Spoofing Algorithm Avoiding Tightly-Coupled GNSS/IMU With Multiple Anti-Spoofing Techniques”. In: *IEEE Trans. Veh. Technol.* 71.8 (2022), pp. 8864–8876.

[60] Ruben Morales Ferre, Alberto de la Fuente, and Elena Simona Lohan. “Jammer Classification in GNSS Bands via Machine Learning Algorithms”. In: *Sensors* 19.22 (2019), p. 4841.

[61] Parisa Borhani-Darian, Haoqing Li, Peng Wu, and Pau Closas. “Detecting GNSS Spoofing Using Deep Learning”. In: *EURASIP J. Adv. Signal Process.* 2024.1 (2024), p. 14.

[62] Yae Chai, Mingqian Liu, and Ming Li. “Navigation Spoofing and Jamming Signals Identification of UAV Based on Federated Learning”. In: *IEEE Internet Things J.* (2025).

[63] ArubaOS. “Detecting Rogue APs”. In: *Hewlett Packard Enterprise Development LP* (Mar. 1, 2024). URL: https://www.arubanetworks.com/techdocs/ArubaOS_64_Web_Help/Content/ArubaFrameStyles/New_WIP/Rogue_AP_Detection.htm (visited on 03/01/2024).

[64] IBM SevOne Network Performance Management. “Wifi Monitoring for Modern Networks”. In: *IBM* (Mar. 1, 2024). URL: https://www.ibm.com/products/sevone-network-performance-management/wifi-monitoring (visited on 03/01/2024).

[65] Douglas Gantenbein. “Finding and Remediating Rogue Access Points on the Microsoft Corporate Network”. In: *Microsoft* (Aug. 11, 2023). URL: https://www.microsoft.com/insidetrack/blog/finding-rogue-access-points-on-the-microsoft-corporate-network/ (visited on 03/01/2024).

[66] Bandar Alotaibi and Khaled Elleithy. “Rogue Access Point Detection: Taxonomy, Challenges, and Future Directions”. In: *Wirel. Pers. Commun.* 90 (2016), pp. 1261–1290.

[67] Nazrul M Ahmad, Anang Hudaya Muhamad Amin, Subarmaniam Kannan, Mohd Faizal Abdollah, and Robiah Yusof. “A RSSI-based Rogue Access Point Detection Framework for Wi-Fi Hotspots”. In: *Proc. 2nd IEEE ISTT*. Langkawi, Malaysia, Nov. 2014.

[68] Yuxiang Lin, Yi Gao, Bingji Li, and Wei Dong. “Accurate and Robust Rogue Access Point Detection with Client-Agnostic Wireless Fingerprinting”. In: *Proc. IEEE PerCom*. Austin, TX, USA, Mar. 2020.

[69] Dawei Yan, Yubo Yan, Panlong Yang, Wen-Zhan Song, Xiang-Yang Li, and Pengfei Liu. “Real-Time Identification of Rogue WiFi Connections in the Wild”. In: *IEEE Internet Things J.* 10.7 (2022), pp. 6042–6058.

[70] Cillian O’Driscoll and Gianluca Caparra. “Nautilus: An Embedded Navigation Authentication Testbed”. In: *Proc. 34th ION GNSS+*. St. Louis, MO, USA, Sept. 2021.

[71] Guowei Wan, Xiaolong Yang, Renlan Cai, Hao Li, Yao Zhou, Hao Wang, and Shiyu Song. “Robust and Precise Vehicle Localization Based on Multi-Sensor Fusion in Diverse City Scenes”. In: *Proc. IEEE ICRA*. Brisbane, QLD, Australia, May 2018.

[72] Silvia Ceccato, Francesco Formaggio, Gianluca Caparra, Nicola Laurenti, and Stefano Tomasin. “Exploiting Side-Information for Resilient GNSS Positioning in Mobile Phones”. In: *Proc. IEEE/ION PLANS*. Monterey, CA, USA, Apr. 2018.

[73] Lu Bai, Chao Sun, Andrew G. Dempster, Hongbo Zhao, and Wenquan Feng. “GNSS Spoofing Detection and Mitigation With a Single 5G Base Station Aiding”. In: *IEEE Trans. Aerosp. Electron. Syst.* 60.4 (2024), pp. 4601–4620.

[74] Samer Khanafseh, Naeem Roshan, Steven Langel, Fang-Cheng Chan, Mathieu Joerger, and Boris Pervan. “GPS Spoofing Detection Using RAIM with INS Coupling”. In: *Proc. IEEE/ION PLANS*. Monterey, CA, USA, May 2014.

[75] Marco Ceccato, Francesco Formaggio, Nicola Laurenti, and Stefano Tomasin. “Generalized Likelihood Ratio Test for GNSS Spoofing Detection in Devices with IMU”. In: *IEEE Trans. Inf. Forensics Secur.* 16 (2021), pp. 3496–3509.

[76] Joshua J Morales and Zaher M Kassas. “Tightly Coupled Inertial Navigation System with Signals of Opportunity Aiding”. In: *IEEE Trans. Aerosp. Electron. Syst.* 57.3 (2021), pp. 1930–1948.

[77] Mahdi Maaref and Zaher M Kassas. “Autonomous Integrity Monitoring for Vehicular Navigation with Cellular Signals of Opportunity and an IMU”. In: *IEEE Trans. Intell. Transp. Syst.* 23.6 (2022), pp. 5586–5601.

[78] Zaher M. Kassas, Joe Khalife, Ali A. Abdallah, and Chiawei Lee. “I Am Not Afraid of the GPS Jammer: Resilient Navigation Via Signals of Opportunity in GPS-Denied Environments”. In: *IEEE Aerosp. Electron. Syst. Mag.* 37.7 (2022), pp. 4–19.

[79] Wang Hu, Yingjie Hu, Mike Stas, and Jay A Farrell. “Optimization-Based Outlier Accommodation for Tightly Coupled RTK-Aided Inertial Navigation Systems in Urban Environments”. In: *Proc. 27th IEEE ITSC*. Edmonton, AB, Canada, Sept. 2024.

[80] Zaher M Kassas, Nadim Khairallah, Joe J Khalife, Chiawei Lee, Juan Jurado, Steven Wachtel, Jacob Duede, Zachary Hoeffner, Thomas Hulsey, Rachel Quirarte, et al. “Aircraft Navigation in GNSS-denied Environments via Radio SLAM with Terrestrial Signals of Opportunity”. In: *IEEE Trans. Intell. Transp. Syst.* 25.10 (2024), pp. 14164–14182.

[81] Nils Ole Tippenhauer, Kasper Bonne Rasmussen, Christina Pöpper, and Srdjan Čapkun. “Attacks on Public WLAN-based Positioning Systems”. In: *Proc. 7th MobiSys*. Kraków, Poland, June 2009.

[82] Mathy Vanhoef and Frank Piessens. “Advanced Wi-Fi Attacks Using Commodity Hardware”. In: *Proc. 30th ACSAC*. New Orleans, LA, USA, Dec. 2014.

[83] Altaf Shaik, Ravishankar Borgaonkar, N Asokan, Valtteri Niemi, and Jean-Pierre Seifert. “Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems”. In: *Proc. NDSS*. San Diego, CA, USA, Feb. 2016.

[84] Maximilian Von Tschirschnitz, Ludwig Peuckert, Fabian Franzen, and Jens Grossklags. “Method Confusion Attack on Bluetooth Pairing”. In: *Proc. IEEE S&P*. San Francisco, CA, USA, May 2021.

[85] Xiao Han, Junjie Xiong, Wenbo Shen, Zhuo Lu, and Yao Liu. “Location Heartbleeding: The Rise of Wi-Fi Spoofing Attack via Geolocation API”. In: *Proc. ACM CCS*. New York, NY, USA, Nov. 2022.

[86] Xiao Han, Junjie Xiong, Wenbo Shen, Mingkui Wei, Shangqing Zhao, Zhuo Lu, and Yao Liu. “The Perils of Wi-Fi Spoofing Attack Via Geolocation API and Its Defense”. In: *IEEE Trans. Dependable Secure Comput.* 21.5 (2024), pp. 4343–4359.

[87] Manuel Flury, Marcin Poturalski, Panos Papadimitratos, Jean-Pierre Hubaux, and Jean-Yves Le Boudec. “Effectiveness of Distance-Decreasing Attacks against Impulse Radio Ranging”. In: *Proc. 3rd ACM WiSec*. Hoboken, NJ, USA, Mar. 2010.

[88] *GALILEO OPEN SERVICE NAVIGATION MESSAGE AUTHENTICATION (OSNMA) Info Note*. Tech. rep. EUSPA, Nov. 2021. URL: https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OSNMA_Info_Note.pdf.

[89] Tomáš Pevnỳ. “Loda: Lightweight On-Line Detector of Anomalies”. In: *Machine Learning* 102 (2016), pp. 275–304.

[90] Jammertest. “The World’s Largest Open Jamming and Spoofing Test”. In: *Jammertest* (Jan. 31, 2024). URL: https://jammertest.no/about-2/ (visited on 09/16/2024).

[91] Manon Kok, Jeroen D Hol, and Thomas B Schön. “Using Inertial Sensors for Position and Orientation Estimation”. In: *arXiv preprint arXiv:1704.06053* (2018).

[92] Armando Domi. *Particle Filter*. https://github.com/ArmandoDomi/Particle_Filter/. 2020.

[93] Mozilla. *Ichnaea*. https://github.com/mozilla/ichnaea/blob/main/ichnaea/api/locate/mac.py. 2023.

[94] Zhenqi Zheng, You Li, Zongbo Liao, Yizhou Xue, Jian Kuang, Yuan Zhuang, and Peng Zhang. “The Necessity of Modeling Location Uncertainty of Fingerprints for Ubiquitous Positioning”. In: *IEEE Sens. J.* 23.16 (2023), pp. 18413–18422.

[95] Wenjia Wu, Xiaolin Gu, Kai Dong, Xiaomin Shi, and Ming Yang. “PRAPD: A Novel Received Signal Strength-Based Approach for Practical Rogue Access Point Detection”. In: *Int. J. Distrib. Sens. Netw.* 14.8 (2018), pp. 1–11.

[96] Zheng Li, Yue Zhao, Xiyang Hu, Nicola Botta, Cezar Ionescu, and George Chen. “ECOD: Unsupervised Outlier Detection Using Empirical Cumulative Distribution Functions”. In: *IEEE Trans. Knowl. Data Eng.* (2022).

[97] Bobzilla, Arkasha, and Uhtu. “Wigle.net. All the Networks. Found by Everyone.” In: *WiGLE* (Sept. 15, 2023). URL: `https://wigle.net/` (visited on 09/15/2023).

[98] Derek Knowles, Ashwin Vivek Kanhere, Sriramya Bhamidipati, and Grace Gao. “A Modular and Extendable GNSS Python Library”. In: *Proc. 35th ION GNSS+*. Denver, CO, USA, Sept. 2022.

Appended papers