IMT School for Advanced Studies, Lucca
Lucca, Italy

Resilience of 5G Positioning: Optimization Framework, Physical Layer Security, and Experimental Validation

PhD Program in Cybersicurezza

Track in Foundational Aspects in Cybersecurity

XXXVIII Cycle

By

Samuele Zanini

2025

The dissertation of Samuele Zanini is approved.

PhD Program Coordinator: Mirco Tribastone, IMT School for Advanced Studies Lucca

Advisor: Prof. Giuseppe Bianchi, University of Rome "Tor Vergata"

Co-Advisor: Prof. Stefania Bartoletti, University of Rome "Tor Vergata"

The dissertation of Samuele Zanini has been reviewed by:

Ilenia Tinnirello, University of Palermo

Andrea Zanella, University of Padua

IMT School for Advanced Studies Lucca
2025

Contents

List of Figures

List of Tables

List of Acronyms

3GPP	3rd Generation Partnership Project
5G	5th Generation
AF	Application Function
AI	Artificial Intelligence
AL	Alert Limit
AMF	Access And Mobility Function
AOA	Angle of Arrival
AOD	Angle of Departure
AWGN	Additive White Gaussian Noise
BF	Brute Force
BFGS	Broyden–Fletcher–Goldfarb–Shanno
CFAR	Constant False Alarm Rate
CFO	Carrier Frequency Offset
CG	Conjugate Gradient
CIR	Channel Impulse Response
CN	Core Network

COTS	Commercial Off The Shelf
DL-AOD	Downlink-Angle of Departure
DL-TDOA	Downlink-Time Difference of Arrival
DoS	Denial of Service
DS	Delay Spread
E2E	End-to-End
ECCDF	Empirical Complementary Cumulative Distribution Function
eCID	Enhanced CID
EM	Expectation-Maximization
FDD	Frequency Division Duplex
FIR	finite impulse response
FPGA	Field Programmable Gate Arrays
GMLC	Gateway Mobile Location Center
GMM	Gaussian Mixture Model
GLRT	Generalized Likelihood Ratio Test
GNSS	Global Navigation Satellite System
gNB	gNodeB
GPS	Global Positioning System
GPSDO	GPS Disciplined Oscillator
ISAC	Integrated Sensing and Communication
KPI	Key Performance Indicator
L-BFGS-B	Limited-memory BFGS Bound

LCS	Localization Service
LMF	Location Management Function
LOS	Line-of-Sight
LPP	LTE Positioning Protocol
LTE	Long Term Evolution
ML	Machine Learning
MITM	Man-in-the-Middle
MOEA/D	Multi-Objective Evolutionary Algorithm based on Decomposition
multi-RTT	multiple Round Trip Time
NF	Network Function
NLOS	Non-Line-of-Sight
Non-RT	Non Real Time
NR	New Radio
NR eCID	New Radio Enhanced CID
NRPPa	New Radio Positioning Protocol a
NSGA-II	Non-dominated Sorting Genetic Algorithm II
nRT	near Real Time
OAI	OpenAirInterface
OFDM	Orthogonal Frequency Division Multiplexing
OTA	Over-the-Air
OTDOA	Observed Time Difference of Arrival
PDSCH	Physical Downlink Shared Channel

PLMN	Public Land Mobile Network
PRS	Positioning Reference Signal
PSL	Positioning Service Level
PSS	Primary Synchronization Signal
QoS	Quality Of Service
RAIM	Receiver Autonomous Integrity Monitoring
RAN	Radio Access Network
RAT	Radio Access Technology
RDM	Range-Doppler Map
RE	Resource Element
RF	Radio Frequency
RFNoC	RF Network on Chip
RFSoC	RF System on Chip
RIC	RAN Intelligent Controller
RS	Reference Signal
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RTT	Round Trip Time
SBI	Service Based Interface
SCS	Subcarrier Spacing
SDR	Software-Defined Radio
SINR	signal-to-interference-plus-noise ratio

SL	Sidelink
SLPP	Sidelink Positioning Protocol
SNR	Signal-to-Noise Ratio
SPP	Samples per Packet
SRS	Sounding Reference Signal
SSB	Synchronization Signal Block
SSS	Secondary Synchronization Signal
TBS	Terrestrial Beacon System
TDD	Time Division Duplex
TDOA	Time Difference of Arrival
TDL	Tapped Delay Line
TIR	Target Integrity Risk
TOA	Time of Arrival
TRP	Transmit/Receive Point
TTA	Time-to-Alert
UE	User Equipment
UL-AOA	Uplink-Angle of Arrival
UL-TDOA	Uplink-Time Difference of Arrival
UMi	Urban Micro-cellular
USRP	Universal Software Radio Peripheral
WLAN	Wireless LAN

Acknowledgements

I wish to acknowledge all the colleagues and co-authors whose expertise, discussions, and shared efforts contributed to the research presented here. The author acknowledges the use of AI-based language tools for improving readability, grammar, and stylistic consistency of the manuscript. Some parts of this dissertation are derived from material previously published or under review, co-authored with colleagues during the course of my doctoral studies. Figures, tables, and text are excerpts from the publications listed in Chapter 1.

Vita

September 13, 1998	Born, Vicenza, Italy
2020	Bachelor Degree in Information Engineering Final mark: 101/110 University of Padua, Padua, Italy
2022	Master Degree in ICT for Internet and Multimedia Engineering Final mark: 110/110 cum laude University of Padua, Padua, Italy
2022–Current	PhD Student in Cybersecurity University of Rome "Tor Vergata", Rome, Italy IMT School for Advanced Studies Lucca, Lucca, Italy

Publications

1. G. Focarelli, S. Zanini, G. Bianchi, and S. Bartoletti, "Physical Layer Threats to 5G Positioning: Impact on TOA-Based Methods," in *IEEE International Conference on Communications Workshops (ICC Workshops)*, 2024, pp. 926–931
2. S. Zanini, L. Petrucci, I. Palamà, G. Bianchi, and S. Bartoletti, "Towards End-to-end Implementation of 5G Positioning with Off-the-shelf Devices," in *IEEE 100th Vehicular Technology Conference*, 2024
3. R. Lo Cigno, F. Gringoli, S. Bartoletti, M. Cominelli, L. Ghiro, and S. Zanini, "Communication and Sensing: Wireless PHY Layer Threats to Security and Privacy for IoT systems, and possible Countermeasures," *MDPI - Information*, 2025
4. S. Zanini, G. Focarelli, I. Palamà, A. Rivitti, G. Bianchi, and S. Bartoletti, "Experimental Viability of Full-Frame 5G Meaconing Attacks," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2025, pp. 1–3
5. G. Focarelli, S. Zanini, I. Palamà, A. Rivitti, S. Bartoletti, and G. Bianchi, "WIP: Parrots in the Air: Experimental Validation of Full-Frame Meaconing in 5G Systems," in *IEEE 26th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2025, pp. 118–121
6. L. Petrucci, S. Zanini, I. Palamà, N. B. Melazzi, and S. Bartoletti, "Localization in 5G and beyond: A multi-objective approach for accuracy, latency, and resilience," *IEEE Transactions on Mobile Computing*, pp. 12771–12783, 2025.
7. I. Palam'a, G. Focarelli, S. Zanini, G. Bianchi, and S. Bartoletti, "Blind Deception in ISAC via Full-Frame OFDM Replay," in *Proceedings of the ACM Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization*, 2025, pp. 25–32
8. G. Focarelli, S. Zanini, I. Palamà, G. Bianchi, and S. Bartoletti, "Positioning Security in 5G and Beyond: Model and Detection of Physical Layer Threats", *IEEE Transactions on Wireless Communications*, vol. 25, pp. 1048–1061, 2026.
9. S. Zanini, S. Bartoletti, G. Focarelli, I. Palama, and G. Bianchi, "Location Security in 5G and Beyond: Potential Threats and Countermeasures," *IEEE Communications Magazine*, pp. 1–7, 2026.

Abstract

The advent of 5th Generation (5G) positioning, standardized within rd Generation Partnership Project (3GPP), has introduced high-accuracy and low-latency localization capabilities, enabling a wide range of safety-critical applications such as autonomous vehicles, healthcare, and emergency management. Despite major advances in accuracy and latency, the resilience and security of 5G positioning remain underexplored. This gap is critical, as without trustworthy location information even the most accurate systems cannot be deployed in any safety-critical scenarios.

This dissertation addresses this challenge by investigating resilience of 5G positioning making three main contributions, involving optimization framework, physical-layer security, and experimental validation. First, we introduce an optimization problem that formulates the localization process as a multi-objective optimization problem, jointly addressing accuracy, latency, resilience, and resource efficiency. To support this analysis, we developed a 3GPP-compliant location management function and integrated it into an end-to-end testbed, enabling experimental results that provide valuable insights into the trade-offs of the optimization problem. Second, we develop a comprehensive analysis of the 5G threat landscape, identifying physical-layer attacks as a critical challenge for positioning integrity. In particular, we investigate spoofing attacks on timing-based localization methods by examining both the underlying estimation process and the attacker's ability to manipulate time-of-arrival measurements. To mitigate such threats, we propose two complementary detection strategies: a simple approach exploiting intrinsic signal properties,

and a semi-supervised learning for anomaly detection based on Gaussian mixture model. Simulation results in standard-compliant scenarios demonstrate that both techniques significantly improve detection performance. Third, building on the simulation study, we provide experimental validation in which, to the best of our knowledge, we demonstrate the first successful meaconing/replay attack on an entire 5G frame using an end-to-end 5G testbed composed by commercial-off-the-shelf and software-defined radio devices. The results show that timing estimates can be stealthily manipulated while preserving an active communication link, thereby exposing a critical physical-layer vulnerability with potentially far reaching implications for the security of 5G positioning. This attack poses a threat not only to current 5G deployments but also to emerging paradigms as integrated sensing and communication, where we demonstrate its impact on sensing performance.

Overall, this dissertation highlights that resilience and security are fundamental, not peripheral, requirements for critical applications. These applications depend on positioning services that must remain reliable even under challenging conditions, including intentional malicious actions, making robustness and trustworthiness essential.

Chapter 1

Introduction

The advent of 5th Generation (5G) technology has fundamentally transformed cellular network capabilities, opening unprecedented opportunities for advanced localization services [1]–[3]. These improvements are particularly relevant in scenarios where traditional Global Navigation Satellite System (GNSS) based systems, such as Global Positioning System (GPS), fail to provide reliable accuracy, for instance, in indoor environments, dense urban deployments, or geopolitically sensitive areas subject to intentional disruptions like jamming [4]–[7]. With the introduction of the Localization Service (LCS) in 3rd Generation Partnership Project (3GPP) Release 16 [8], 5G positioning has been proposed as a complement or even an alternative to GNSS, supporting applications such as autonomous driving, emergency response, and industrial automation [9]–[11].

Before the advent of 5G, localization technologies were typically developed for specific use cases, relying on centralized computation and operating under relatively modest performance requirements. The introduction of 5G, however, has considerably raised expectations for cellular positioning, particularly with respect to latency and accuracy. To address these demands, network architectures have been progressively restructured by introducing dedicated functions and decentralizing computationally intensive tasks such as position estimation, moving LCS closer

to the User Equipment (UE). This architectural shift reduces latency between the UE and the 5G Core, but at the same time introduces new challenges related to the management of distributed resources and the safeguarding of sensitive data. Consequently, enabling effective localization in 5G networks requires achieving a careful balance between accuracy, low latency, efficient resource utilization, and resilience against errors and malicious attacks. Importantly, among these objectives, resilience and security are not auxiliary constraints but fundamental enablers: without them, even the most accurate positioning systems cannot be trusted in safety-critical contexts [12]–[15].

While existing literature extensively covers general 5G network security, it primarily focuses on communication aspects such as encryption and access control, and the specific security challenges related to positioning remain underrepresented. Bridging this gap requires a comprehensive analysis of the 5G localization process, identifying potential threats, and formulating effective countermeasures against the attacks. Initial research efforts have been made to address security threats in cellular-based positioning, highlighting adversarial risks and privacy considerations [12], [14], [16], [17]. For instance, studies have explored threats in vehicular applications [18], privacy regulations like general data protection regulation [19]. Despite these advancements, significant challenges persist in ensuring the security and integrity of 5G positioning systems, especially at the physical layer, where high-level mechanisms are not sufficient. Adversaries can exploit vulnerabilities in localization mechanisms to mislead autonomous systems, create safety hazards, or even influence legal decisions by manipulating geolocation data.

In addition, recent standardization efforts and technological advancements are further amplifying both opportunities and challenges in the field. For instance, Sidelink (SL) positioning introduced in 3GPP Release 18 [20] and the emergence of open RAN initiatives such as O-RAN [21] are reshaping the telecommunications landscape by promoting openness, flexibility, and enhanced positioning accuracy [1], [8], [22], [23]. In parallel, the 3GPP is actively progressing the standardization of the Integrated Sensing and Communication (ISAC) paradigm for 5G and

future 6G systems [24], [25]. The aim is to integrate communication and sensing capabilities within a unified framework, leveraging common spectrum and hardware resources to simultaneously support data transmission and radar-like environmental sensing [26].

These innovations enable the development of novel applications across multiple domains, including rail transport, maritime operations, unmanned autonomous systems, and healthcare. Nevertheless, they concurrently expand the attack surface and introduce new potential security threats. Within this context, the dissertation addresses the security of 5G positioning systems.

1.1 Research Objectives and Contributions

The primary objective of this dissertation is to investigate the security of 5G positioning, with a particular focus on identifying vulnerabilities and developing countermeasures against adversarial threats. At the same time, the research also addresses the broader challenge of 5G positioning in general, by assessing the feasibility of End-to-End (E2E) implementations and introducing a novel multi-objective optimization framework. Finally, the work also has an experimental dimension, providing not only theoretical models and simulations but also practical validation using a fully operational 5G system. The contributions are threefold and can be summarized as follows

The first contribution is an in-depth study on the feasibility of implementing an E2E 5G positioning procedure using commercial Commercial Off The Shelf (COTS) devices and open-source projects. This work, presented in Chapter 2, includes both an experimental assessment of positioning performance, enabled by our implementation of a 3GPP-compliant Location Management Function (LMF) [27], and the introduction of a framework that formulates the 5G positioning problem as a multi-objective optimization problem [28]. Unlike traditional approaches that aim at a single optimum, this formulation highlights the inherent trade-offs among key objectives such as accuracy, latency, resource utilization, and, most critically, resilience.

The second contribution provides a comprehensive security analysis of 5G positioning systems. In Chapter 3, we develop a threat taxonomy and examine the potential attacks that may target different architectural components [29]. Building on this foundation, Chapter 4 focuses specifically on physical-layer vulnerabilities, with emphasis on timing-based attacks [17], [30]. We introduce a detailed mathematical model illustrating how an adversary can overshadow reference signals to manipulate Time of Arrival (TOA) estimates, thereby corrupting position computation. To counter such threats, we propose two detection mechanisms, evaluated through 3GPP-compliant simulations, which demonstrate the ability to reliably distinguish legitimate from malicious signals.

Finally, the third contribution delivers, to the best of our knowledge, the first experimental demonstration of a meaconing attack in a fully operational 5G system [31], [32]. We show that the proposed attack, named *the parrot*, can tamper with TOA measurements while preserving the communication channel, thus avoiding service disruption or Denial of Service (DoS). This experimental validation, described in Chapter 5, bridges the gap between the theoretical models and simulations of Chapter 4 and their realization in practice. In addition, the impact of the mentioned attack on the ISAC scenario is analyzed using the same testbed [33].

1.2 Dissertation Outline

Figure 1 depicts the structure of the dissertation as previously described, highlighting the sections on background and contribution, as well as the division between simulation and experimental work.

The remainder of this dissertation is structured as follows:

- **Chapter 2** pursues a dual objective: first, it offers a comprehensive background on the principles of positioning in 5G systems, including the state-of-the-art in their implementation and the design of an experimental testbed. Second, it formulates a multi-objective optimization model aimed at addressing the 5G localization problem.

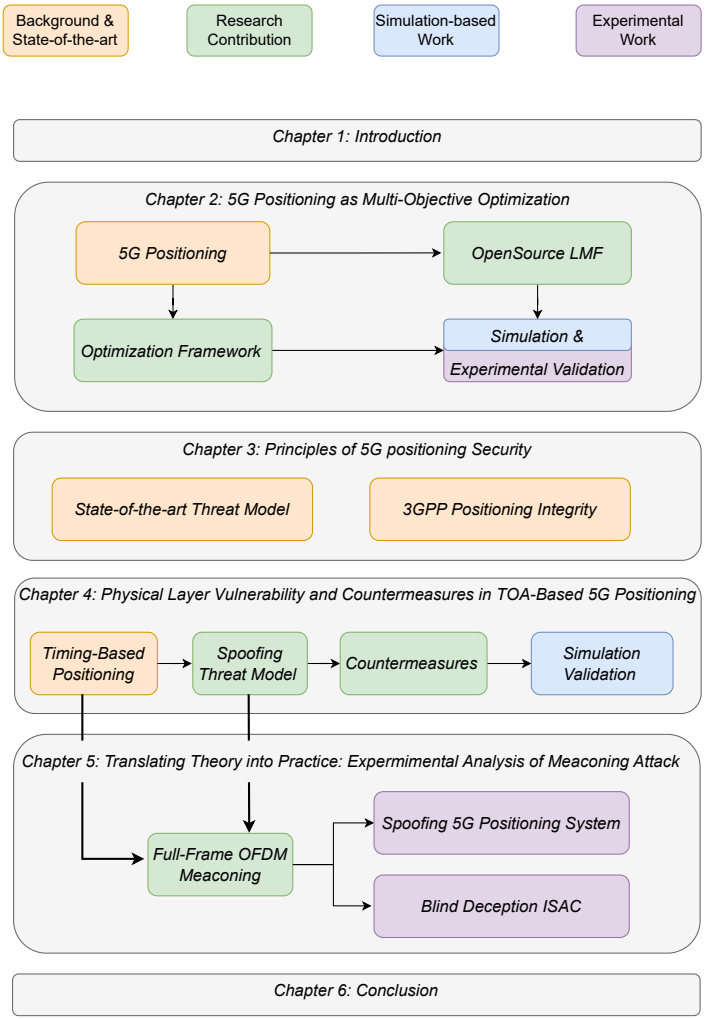

Figure 1: Schematic overview of the thesis.

- **Chapter 3** provides an overview of the security challenges in 5G

positioning systems by highlighting vulnerabilities in architectures (3GPP and O-RAN) and in the localization procedures, and reviews recent 3GPP standard developments concerning positioning integrity.

- **Chapter 4** examines physical-layer attacks on 5G and beyond positioning systems, with a particular focus on timing-based methods. It introduces a formal framework for modeling security threats at the physical layer and presents mitigation strategies employing cross-correlation analysis and Gaussian Mixture Model (GMM), which are validated through simulation and shown to significantly reduce integrity risks under attack conditions, thereby providing a foundation for the development of resilient location-based services in mobile networks.

- **Chapter 5** explores full-frame meaconing attacks on 5G positioning systems, building upon the physical-layer vulnerabilities analyzed in the previous chapter. It experimentally demonstrates, using COTS and Software-Defined Radio (SDR) devices, how entire 5G frames can be received, delayed, and amplified to introduce controlled TOA biases without disrupting ongoing communications, thereby revealing critical vulnerabilities in timing-based localization methods, including the ISAC framework.

- **Chapter 6** synthesizes the outcomes of this work, providing a comprehensive summary of the principal contributions and examining their implications alongside the key findings and results derived throughout the study.

1.3 List of Publications

In the following, we list all the materials published, and under review, throughout the course of the PhD program. Some sections of the upcoming chapters will include figures and direct excerpts from these listed publications.

Conference

- G. Focarelli, **S. Zanini**, G. Bianchi, and S. Bartoletti, "Physical Layer Threats to 5G Positioning: Impact on TOA-Based Methods," in *IEEE International Conference on Communications Workshops (ICC Workshops)*, 2024, pp. 926–931
- **S. Zanini**, L. Petrucci, I. Palamà, G. Bianchi, and S. Bartoletti, "Towards End-to-end Implementation of 5G Positioning with Off-the-shelf Devices," in *IEEE 100th Vehicular Technology Conference*, 2024
- **S. Zanini**, G. Focarelli, I. Palamà, A. Rivitti, G. Bianchi, and S. Bartoletti, "Experimental Viability of Full-Frame 5G Meaconing Attacks," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2025, pp. 1–3
- G. Focarelli, **S. Zanini**, I. Palamà, A. Rivitti, S. Bartoletti, and G. Bianchi, "WIP: Parrots in the Air: Experimental Validation of Full-Frame Meaconing in 5G Systems," in *IEEE 26th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2025, pp. 118–121
- I. Palam'a, G. Focarelli, **S. Zanini**, G. Bianchi, and S. Bartoletti, "Blind Deception in ISAC via Full-Frame OFDM Replay," in *Proceedings of the ACM Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization*, 2025, pp. 25–32

Journal

- L. Petrucci, **S. Zanini**, I. Palamà, N. B. Melazzi, and S. Bartoletti, "Localization in 5G and beyond: A multi-objective approach for accuracy, latency, and resilience," *IEEE Transactions on Mobile Computing*, pp. 12771–12783, 2025.
- G. Focarelli, **S. Zanini**, I. Palamà, G. Bianchi, and S. Bartoletti, "Positioning security in 5G and beyond: Model and detection of physical layer threats," *IEEE Transactions on Wireless Communications*, pp. 1048–1061, 2026.

- **S. Zanini**, S. Bartoletti, G. Focarelli, I. Palama, and G. Bianchi, "Location Security in 5G and Beyond: Potential Threats and Countermeasures," *IEEE Communications Magazine*, pp. 1–7, 2026.

- S. Bartoletti, G. Focarelli, I. Palamà, **S. Zanini**, N. B. Melazzi, and G. Bianchi, "Practical Blind Full-Frame Replay Attacks on OFDM-Based ISAC Systems," *IEEE Journal on Selected Areas in Communications*, **UNDER REVIEW** Submitted Date: Aug. 2025

I have also co-authored the following works which are not included in this dissertation:

- R. Lo Cigno, F. Gringoli, S. Bartoletti, M. Cominelli, L. Ghiro, and **S. Zanini**, "Communication and Sensing: Wireless PHY Layer Threats to Security and Privacy for IoT systems, and possible Countermeasures," *MDPI - Information* 2025

Chapter 2

5G Positioning as Multi-Objective Optimization

This chapter serves a dual purpose. First, it provides a detailed technical background on 5th Generation (5G) positioning, covering the underlying principles, relevant architectures, protocols, methods, and performance metrics defined by 3rd Generation Partnership Project (3GPP) and O-RAN specifications. Second, it frames 5G positioning as a multi-objective optimization problem, setting the stage for the analysis and modeling presented herein. The discussion begins with an overview of positioning concepts, followed by a review of state-of-the-art implementation solutions and an experimental assessment of currently supported features, enabled by our implementation of a 3GPP-compliant Location Management Function (LMF). Building on this foundation, we introduce an optimization system model that captures latency, accuracy, resource usage, and resilience costs, and examine the resulting trade-offs, architectural considerations, and positioning strategies. The chapter concludes with a case study, both simulated and experimental, illustrating the practical implications of the proposed multi-objective framework.

2.1 Background: 5G Positioning

In this section, we present the details of 5G positioning by considering two distinct architectures: the 3GPP and O-RAN frameworks. We then describe the main positioning protocols, methods, and modes, followed by an outline of the end-to-end localization procedure. Finally, we introduce the performance metrics used to evaluate and compare positioning solutions.

2.1.1 3GPP Architecture

General Framework

The 3GPP introduces Localization Services (LCSs) starting from Release 16, which involves estimating the position of the target using the 5G network and relative cellular signals [1], [8], [22], [23]. Figure 2 shows the general architecture of the LCS in 5G networks, with the involved entities being the Gateway Mobile Location Center (GMLC), Access And Mobility Function (AMF), LMF, gNodeBs (gNBs), and User Equipment (UE). Indeed, 5G positioning leverages the new LMF, positioning protocols

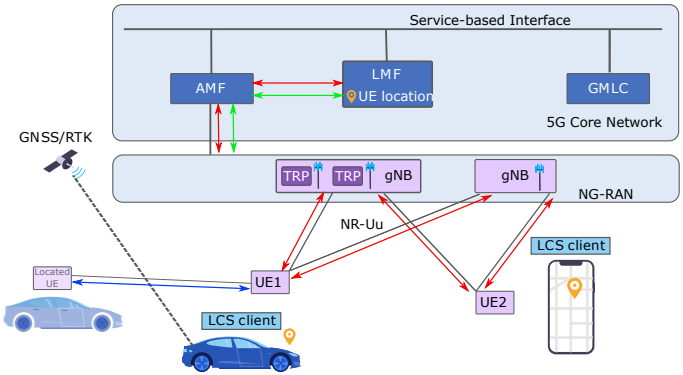

Figure 2: LCS/5G positioning architecture. The arrows indicate the protocol interactions between network entities (LPP in red, SLPP in blue, and NRPPa in green).

(New Radio Positioning Protocol a (NRPPa) and LTE Positioning Proto-

col (LPP), the latter already present in Long Term Evolution (LTE) systems), and specific references signals used exclusively for positioning purposes (Positioning Reference Signal (PRS) and Sounding Reference Signal (SRS)). The AMF and GMLC are necessary for forwarding messages between the LMF and the UE/gNBs, and for handling location requests received from external Application Function (AF) or LCS clients, respectively. The LMF is the central and key system element, as it is the Network Function (NF) responsible for the overall management procedure related to the position estimation of the target UE. Key tasks involve selecting a suitable positioning method and mode based on the use-case requirements and Quality Of Service (QoS). Such decisions affect the entire procedure since they affect accuracy, latency, security, message exchanges, and the number of involved entities, potentially increasing the attack surface. Once measurements have been acquired, specific algorithms are implemented to process these inputs and produce the final position estimate.

Sidelink Framework

Starting from Release 18, as outlined in TS 23.586, 3GPP introduced Sidelink (SL) positioning and relative Sidelink Positioning Protocol (SLPP), allowing the possibility of using the direct communication between two or more UEs for obtaining positioning measurements and localizing the target UE as illustrate in Figure 2. A key technical component in SL positioning is the PC5 reference point, a communication interface specifically designed to facilitate direct communication between UEs. This interface enables UEs to transmit and receive signals directly to and from each other, bypassing the traditional cellular network infrastructure essential for applications like vehicle-to-everything, where real-time information exchange is crucial. SL positioning facilitates the determination of a target UE's position, even if it lacks a direct network connection, by measuring the relative distance and direction to Located UEs, i.e., devices in known positions that serve as anchors. The 3GPP introduced the SL Positioning Server UE, a new entity that can be either the target UE or the Located UE. This server plays a key role in supporting the SL positioning

procedure, including computing the position estimation.

2.1.2 O-RAN Architecture

Unlike the 3GPP architecture, the O-RAN architecture provides a more flexible positioning framework. The O-RAN positioning use case [34], [35] utilizes this flexible approach to improve local indoor positioning reducing latency. As shown in Figure 3, the O-RAN Local Indoor Positioning architecture integrates positioning functions directly within the Radio Access Network (RAN) through a positioning xApp deployed in the near Real Time (nRT) RAN Intelligent Controller (RIC).

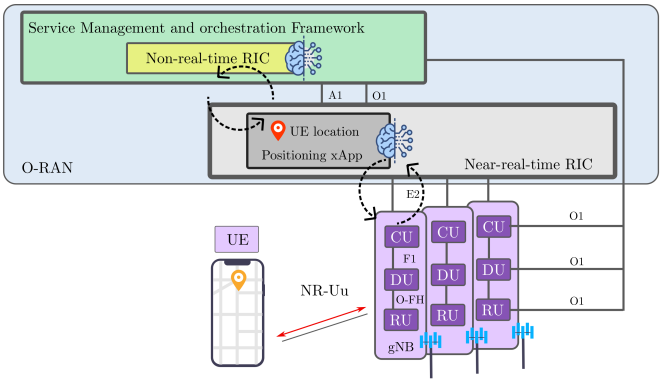

Figure 3: O-RAN Local Indoor Positioning Architecture. This architecture integrates positioning functions within the RAN through a positioning xApp deployed in the nRT RIC.

In the illustrated setup, the positioning xApp calculates the position and, optionally, the speed of the UE based on measurements obtained via the E2 interface. Integrating the positioning function into the RAN substantially decreases latency compared to traditional approaches where positioning computations are handled by the LMF within the core network. This reduction is critical for applications that demand real-time or near-real-time location data. The architecture comprises the nRT RIC, E2 nodes, and, depending on the selected solution, the Non Real Time

(Non-RT) RIC. The nRT RIC identifies the location measurement capabilities of E2 nodes and subscribes to the required measurements based on chosen positioning algorithms and QoS requirements. The inclusion of the Non-RT RIC adds flexibility, as it can supply Artificial Intelligence (AI)/Machine Learning (ML) models for positioning algorithms, train these models using historical data, and deploy them to the nRT RIC for real-time inference. The flexibility of the O-RAN solution leads to increased system variability by allowing significant changes in the number of involved entities, the algorithms used, and the volume of exchanged messages.

2.1.3 Positioning Protocols

The LMF gathers positioning information of the UE, directly from the UE or from the gNBs using two specific positioning protocols: LPP and NRPPa, defined in [36], [37] respectively.

- **LPP:** is used by the LMF to interact directly with the target. It facilitates the exchange of positioning capabilities of the UE, assistance data needed for obtaining measurements, or computing the location estimation, which may be requested using specific messages.
- **NRPPa:** is used by the LMF to communicate with the gNBs. It is used for exchanging the configuration of reference signals needed for obtaining measurements and, in general, all the necessary data for estimating the position of the UE.
- **SLPP:** is used by the target UE to communication directly with other UEs for obtaining positioning measurements and localizing the target UE.

2.1.4 Positioning Methods and Modes

The LMF evaluates the UE capabilities, which are sent by the UE via a specific LPP message, alongside the QoS requirements of the location request to select the most suitable methods and modes for location estimation.

Modes Supported

The selection of modes implies the entity responsible for obtaining measurements, and/or computing the position estimation. Indeed, the 3GPP standard in [8] defines four positioning modes:

- **UE-Assisted.** The UE is responsible for collecting the measurements while the network does the computation through the LMF.
- **UE-Based.** The UE is responsible for both collecting the measurements and computing the location with the support of the assistance data received from the network.
- **Standalone.** The UE obtains the measurements and computes the location without any support from the network. In this case, the UE relies on technologies independent from cellular systems, like GPS.
- **Network-Based.** The network obtains the measurements and computes the location estimation of the UE.

Methods

Several positioning methods are delineated in TS 38.305 [22], which differ for the type of measurement used and the technology they rely on (i.e., both Radio Access Technology (RAT) and RAT-independent) as follows:

- **LTE:**
  - Enhanced CID (eCID) - Estimates the cell ID and signal timing of the nearest base station for location approximation.
  - Observed Time Difference of Arrival (OTDOA) - Utilizes the Time Difference of Arrival (TDOA) signals from multiple base stations to triangulate position.
- **New Radio (NR):**

- New Radio Enhanced CID (NR eCID) - An enhanced version of eCID for NR networks, improving accuracy with advanced signal processing.
- multiple Round Trip Time (multi-RTT) - Employs Round Trip Time (RTT) measurements of signals between the device and multiple base stations for distance estimation. Geometrically, each RTT measurement corresponds to a circumference, and the UE's position is estimated at the intersection of at least three circumferences
- Downlink-TDOA and Uplink-TDOA - Measures the downlink and uplink TDOA of PRS and SRS, respectively, for precise location triangulation. Geometrically, each TDOA measurement leads to a hyperbolic curve, and the UE location is determined by the intersection of at least two hyperbolas.
- Downlink-Angle of Departure (AOD) and Uplink-Angle of Arrival (AOA) - Determines the position through the angle of departure and arrival of signals in downlink and uplink scenarios, respectively. The UE's location is estimated by determining the relative direction between the UE and the gNB and finding the intersection of curves derived from these angle measurements.

- **RAT-Independent:**
  - Network Assisted-Global Navigation Satellite System (GNSS) - Enhances GNSS accuracy with assistance data from cellular networks.
  - Wireless LAN (WLAN), Bluetooth - Leverages the proximity to WLAN access points and Bluetooth beacons for indoor positioning.
  - Terrestrial Beacon System (TBS) - Trilateration based on timing measurements from the target to several ground-based transmitters.

– Sensor-based - Utilizes inertial sensors of the device (e.g., accelerometer, gyroscope) for movement tracking and position estimation.

The localization process integrates these techniques with advanced ML and AI algorithms. According to 3GPP TR 38.843, AI applied to the new radio air interface primarily targets three key areas: enhanced channel state information feedback, optimized beam management, and improved positioning accuracy.

2.1.5 End-to-End Localization Procedure

This section presents two procedures corresponding to two cases of End-to-End (E2E) localization execution, differing in the entity responsible for collecting the positioning measurements.

Case 1: UE-Driven Estimation

In scenarios where the UE takes the initiative (including UE-Based, UE-Assisted, and Standalone modes), the LPP protocol facilitates the completion of the positioning estimation process. Using the UE-Assisted mode as an example scenario, where the UE collaborates with network entities to perform localization, Figure 4 depicts the sequence of messages exchanged E2E among the involved entities to complete the localization task.

Case 2: Network-Driven

In the Network-Based mode, the gNBs collect the necessary measurements. Here, the LMF mainly utilizes NRPPa messages for interaction with the RAN. Figure 5 illustrates the positioning estimation procedure involving the LMF's collection of positioning data from multiple gNBs facilitated by NRPPa messaging, as defined in TS 38.305 [22].

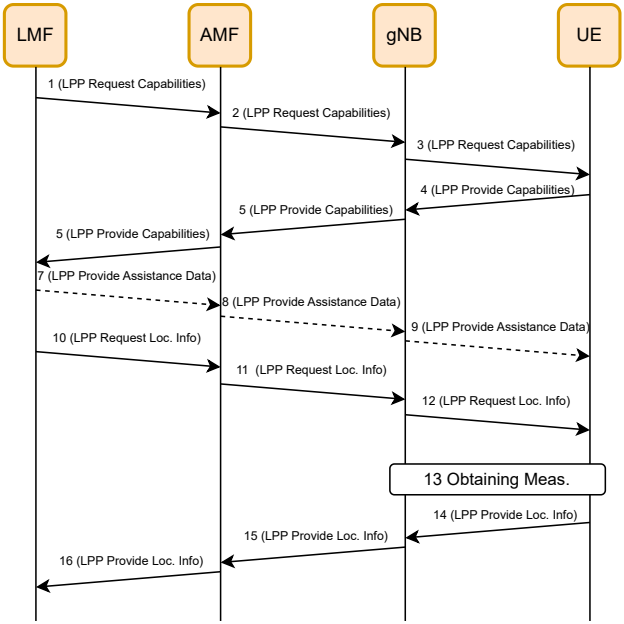

Figure 4: Message flow for E2E localization procedure in UE-driven estimation (Case 1). Orange elements are available with some restrictions or with necessary implementations/modifications.

2.1.6 Performance Metrics

The 3GPP defines several Key Performance Indicators (KPIs), including security-related metrics [22], [38], [39]. The main ones include *positioning accuracy*, which is the degree of conformance of the estimated position with the true one, referring to the true error as $\epsilon = \|\hat{\mathbf{p}}_{\text{ue}} - \mathbf{p}_{\text{ue}}\|$; *availability*, which is the percentage of time when the service is active and satisfies the requirements; and *latency*, expressed as the time passed between the request and the computation of the position estimation. Depending on the operational scenario, 5G systems should be able to provide positioning services according to the seven 3GPP Positioning Service Level (PSL), defined starting from Rel. 17 [39]. These KPIs are subsequently mapped to the PSL which are summarized in Table 1. Levels 1–2 target an error

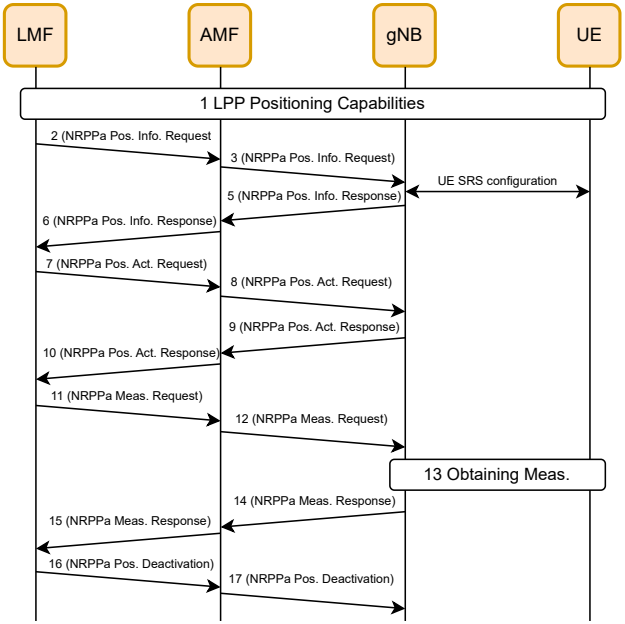

Figure 5: Message flow for E2E localization procedure in network-driven estimation (Case 2). Orange elements are available with some restrictions or with necessary implementations/modifications.

range of 3 to 10 meters, while levels 3–6 require a more stringent accuracy between 0.3 and 3 meters, depending on the scenario. Concerning latency, requirements range from 1 second for the initial levels to as low as 15 ms and 10 ms for levels 4 and 6, respectively. These PSL requirements form the foundation for the multi-objective optimization problem described later in this chapter.

2.2 Experimenting with an End-to-End 5G Positioning System

In this section, we describe the state of the art of both commercial and open-source implementations for the entities involved in the localization

Table 1: Definition of the PSL as specified by the 3GPP in [39]

PSL	Accuracy [m]		Latency [ms]	Availability [%]
	Horizontal	Vertical		
1	10	3	1000	95
2	3	3	1000	99
3	3	2	1000	99
4	1	2	15	99.99
5	0.3	2	1000	99
6	0.3	2	10	99.9

procedure, i.e., the LMF, the core network, the RAN, and the UE. Figure 4 and Figure 5 illustrate the message exchange between the entities in two different cases, with the entities' color indicating the actual implementations' state. It is worth noting that, to the best of our knowledge and at the time of publication, there is only a preliminary version of the LMF within the OpenAirInterface (OAI) core network, supporting only the NRPPa procedures, for 5G positioning experimentation. In this section we present our proposed solution for the LMF and we investigate both open-source projects and commercial products to implement other entities.

2.2.1 Location Management Function

The LMF is the main function responsible for the LCS and 5G positioning procedure. We now briefly describe our implementation of the network function compliant with the 3GPP standard and then the integration of our solution with the open core networks, Free5GC and OAI. The LMF is deployed as a docker container within all the other NFs as shown in Figure 6.

The proposed LMF can be logically divided into three functional modules as illustrated in Figure 6: *Communication*, *Controller*, and *Localization Algorithms*. The *Communication* module manages, on one hand, the services provided by the LMF within the Service Based Interface (SBI), which are utilized by other NFs, such as the AMF during the estima-

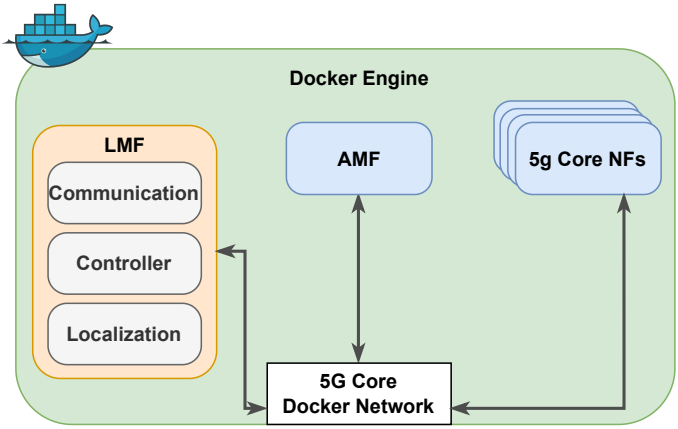

Figure 6: General schema of our LMF within the core network deployed as a docker containers

tion of the UE position, as outlined by the 3GPP in [40]. Simultaneously, this module implements the logic for utilizing the services of the AMF (*Namf_communication*), as defined in [41], to forward LPP and NRPPa messages to UE and gNB respectively. The *Controller* module contains all the required functionalities for managing the internal procedures and coordinating the other two modules. Indeed, after receiving the LPP/NRPPa message extracted by the Communication module, the Controller handles the body of the message and initiates the corresponding procedure to conclude the localization process. Once the positioning measurements are available at the LMF, acquired either by the UE or the gNB depending on the chosen methods and mode, the *Localization Algorithms* module calculates the estimated position. Several localization algorithms may be available in this module and one is selected to estimate the UE's position based on the collected measurements.

In a nutshell, the *Controller* module manages the overall internal procedure, the *Communication* one handles the communication with the SBI, and the *Localization Algorithms* computes the estimated location once the location measurements are available to the LMF.

2.2.2 Core Network

The LMF is connected within the other NFs of the core network via the SBI and communicates with the AMF using the *Namf_communication* services to estimate the location of the target UE, as illustrated in Figure 6. Specifically, the services involved during the procedure include: (i) *N1N2MessageTransfer* for the downlink of LPP/NRPPa messages; (ii) *N1MessageNotify* for the uplink of LPP messages; *N2InfoNotify*; and (iii) *NoNUEN2InfoNotify* for the uplink of NRPPa messages. Currently, three open-source projects enable the deployment of a complete 5G core network: Open5GS, Free5GC, and OpenAirInterface.

- **Open5GS** implements the core network for LTE and 5G networks using C language [42]. The open-source project is compliant with 3GPP Release 17. However, the open5GS does not support the positioning functionalities, so it does not forward the LPP and NRPPa messages needed for the estimation procedure.

- **Free5GC** implements the 5G core network using Go language [43]. It is compliant with 3GPP Release 15 and 16. The positioning functionalities required for the LMF to exchange messages with the target UE and gNB are not currently integrated into the actual version of the AMF.

- **OAI** project is written in C, and it provides the implementation of the 5G core network complaint with the NR 15/16 release [44]. Unlike the other two open-source core networks, it partially supports the specific services necessary for the estimation of the target UE. Indeed, the AMF can forward only NRPPa messages and not LPP.

To summarize, only the core of OAI currently supports positioning functionalities (only the forward of NRPPa messages). As Open5GS does not support the positioning protocols, it is not possible to integrate our LMF in this core network. As for Free5GC, a modified AMF is incorporated into the core network to achieve a full integration with our LMF. The modified AMF enables the forwarding of both LPP and NRPPa mes-

sages in the uplink and downlink direction required to complete the estimation of the target position.

2.2.3 Radio Access Network

There are two possibilities to deploy a gNB composing the RAN: (i) utilize Software-Defined Radio (SDR) with open-source projects and (ii) utilize commercial tools.

Open-source SDR-based Solutions

- **srsRAN** provides RAN gNB solution compliant with 3GPP with features up to NR Release 15 [45]. srsRAN is written in C and C++, is distributed under the GNU AGPLv3 license, and supports the most popular SDR platforms. srsRAN does not support 5G positioning signals (i.e., PRS and SRS) and protocols (i.e., NRPPa).

- **OAI** provides NR Release 15/16 compliant UE implementation [44]. It's written in C and is distributed under the OAI Public License. OAI supports the most commonly used SDR platforms (e.g., Ettus Universal Software Radio Peripheral (USRP) and LimeSDR). In recent times, OAI implemented both downlink PRS and uplink SRS positioning signals, providing Time of Arrival (TOA) estimation based on Channel Impulse Response (CIR) and finer TOA estimation using IDFT with up to 16x oversampling for CIR. It allows receiving downlink PRS from multiple gNBs synchronized via GPS Disciplined Oscillator (GPSDO). Unlike srsRAN, OAI supports 5G positioning signals and protocols. Specifically, it supports the NRPPa procedures related to the UL-TDOA methods where the multiple gNBs obtained the measurements.

Commercial Tools

There are many commercial tools that provide gNB implementations compliant with different releases of 3GPP. Here we focus on the Amarisoft Callbox Mini, which is the one used in our testbed.

- **Amarisoft Callbox Mini** provides a release 17 full software gNB [46]. Callbox Mini supports 5G positioning signals (i.e., PRS and SRS) and protocols (i.e., NRPPa), albeit focusing only on eCID and OTDOA positioning methods. The Callbox Mini facilitates various device testing scenarios, from initial development stages to pre-deployment network testing.

2.2.4 User Equipment

As for the RAN, there are two possibilities for deploying the UE: (i) utilize SDR with open-source projects such as srsRAN or OAI and (ii) utilize Commercial Off The Shelf (COTS) UEs.

Open-source SDR-based solutions

- **srsRAN** provides UE implementations compliant with 3GPP Release 15 [45]. As for the gNB, srsRAN UE supports the most popular SDR platforms and does not support 5G positioning functionalities.

- **OAI** provides UE implementations compliant with 3GPP Release 15 and 16 [44]. Also in this case, OAI UE supports the most commonly used SDR platforms and 5G positioning signals but does not support LPP protocol.

Commercial solution

- **COTS UE** entails utilizing commercial smartphones. Depending on the brand, the characteristics and features of the UE may vary, including the positioning capabilities as evidenced by the preliminary results obtained within our testbed, discussed in the following section.

2.3 Experimental Positioning Assessment

Table 2 summarizes the current status of support the 5G positioning (LPP/NRPPa protocol and positioning signals) functionalities by the entities involved in the E2E localization procedure, as illustrated in Sec. 2.2.

Table 2: Summary of the state of the art of the entities involved in E2E localization, in the upper table the Core Network entities while in bottom RAN and UE entities.

(a) Summary of the state of the art of the entities of the core network involved in E2E localization

5G Functionalities		**Core network**		
		Open5GS	Free5GC	OAI
Protocols	LPP	No	Yes[1]	No
	NRPPa	No	Yes[1]	Yes

Note: 1. Using our modified AMF version.

(b) Summary of the state of the art of the entities of the RAN and UE involved in E2E localization

5G Functionalities		**RAN**			**UE**		
		srsRAN	OAI	Amarisoft	srsRAN	OAI	COTS UE
Protocols	LPP				No	No	Yes[1]
	NRPPa	No	Yes[2]	Yes[2]			
Positioning Signals		No	Yes	Yes	No	Yes	Yes

Note: 1. Depending on the COTS UE
Note: 2. Not all NRPPa functionalities are implemented.

It can be noted that the E2E testing described in Sec. 2.1 requires the integration of different solutions from open-source projects and/or commercial products. Here we present the different combinations used in our work to test the positioning capabilities of multiple COTS UEs.

2.3.1 Experimental Testbed

We develop a testbed to implement the two localization procedures described in Sec. 2.1 by integrating the following components:

- **LMF and Core Network** is implemented in Python and deployed as a docker container within Free5GC and OAI core networks.
- **RAN** comprises a single gNB, based on the Amarisoft Callbox mini or the OAI project, empowering a USRP X310 SDR device [47] as radio transceivers. USRP X310, with UBX 160 daughterboard, are radio devices capable of tuning over a wide radio frequency range, from 10MHz to 8 GHz, and thus cover all NR FR1 frequency bands with up to 400 MHz of instantaneous bandwidth. The radio transceivers feature vertically oriented VERT2450 antennas.
- **COTS UEs** are utilized as the target UEs, specifically employing different commercial smartphones of several brands, like Google Pixel 6, Oneplus Nord 5G, Huawei P40 PRO, and Oneplus 8 PRO.
- **Server** Core network and RAN, in the open-source case, are running in a Dell EMC PowerEdge R640 server, powered by 2x Intel Xeon Silver 4110 CPU with 8 cores @2.10 GHz (max 3.00 GHz), running Ubuntu 18.04 LTS with 5.17 Linux kernel.

2.3.2 Results

The initial phase of the E2E localization procedure, considering both cases mentioned in Figure 4 and Figure 5, is the discovery of the positioning capabilities of the target UEs carried out by the LMF by sending a specific LPP message. However, we need to check the support of the protocol at the UE side before starting the 5G positioning procedure. To verify if the devices support the LPP, we first analyze the general capabilities of the UE when initiating the authentication and registration request to the core network. Specifically, we inspect the uplink NAS messages (*RegistrationRequest*) sent to the AMF by the UE, where the *5GMM Capabilities* field indicates whether or not it supports the LPP. Observing the results using multiple commercial devices, we found that even if LPP support started in 3GPP Release 9 and was updated in Release 15 for 5G, only one COTS UE, i.e., the Google Pixel 6, supports the LPP, as illustrated in Table 3.

Table 3: List of the COTS UEs that support or less the LPP protocol

UE	LPP Support	BaseBand / 3GPP Release
Google Pixels 6	Yes	Samsung Exynos 5123 / 15
Oneplus Nord 5G	No	Qualcomm Snapdragon X52 / 15
Huawei P40 PRO	No	HiSilicon Balong 5000 / 15
Oneplus 8 PRO	No	Qualcomm Snapdragon X55 / 15

We then assessed the positioning capabilities of the only UE supporting LPP protocol. To this end, we analyzed the first message exchanged in the E2E localization procedure. The LMF sends a LPP *Request Capabilities* to the target UE, including the list of positioning methods, among those listed in Sec. 2.1, that it wants to comprehend. The UE replies for each requested technique with the method's relative capabilities, including additional information such as the type of measurements it supports. This information assists the LMF in the decision-making process regarding the method and mode of the estimation of the target position.

Table 4: Summary of the LPP capabilities for the COTS UE that supported the protocol.

Positioning methods		COTS UE
		Google pixels 6
Non-Cellular	Assisted-GNSS	Yes
LTE	eCID	Yes
	OTDOA	Yes
NR	NR eCID	Yes
	multi-RTT	No
	DL-AOD	No
	DL-TDOA	No
	UL-TDOA	No
	UL-AOA	No

The result of the Google Pixel 6 positioning assessment is summarized in Table 4. Note that, as expected, the majority of supported methods relies on LTE signals (eCID and OTDOA), with only one based on NR signals (NR eCID), and the last one independent of the cellular network

(Assisted-GNSS).

2.4 Multi-Objective Problem and Trade-off Discussion

We now define the system model, the multi-objective optimization problem and explore potential solutions, while discussing the impact of architectural and implementation choices on the corresponding performance indicators.

2.4.1 System Model

Figure 7 illustrates the entire localization process, highlighting key components, input parameters, and their influence on the system model's cost function. Input parameters can be either fixed, determined by the selected system and its configuration (e.g., LCS architecture or Radio Frequency (RF) settings), or variable, such as the positioning mode, methods, and number of gNBs.

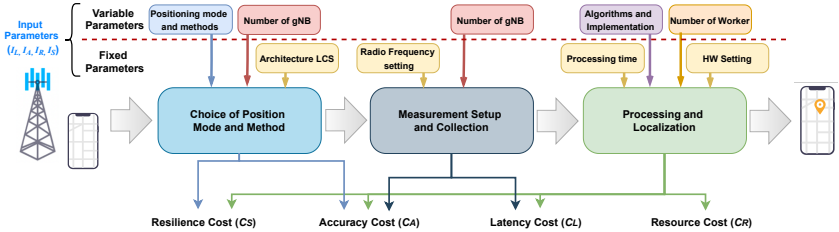

Figure 7: Overall flow of the Localization Service Process, highlighting the key components and parameters involved in the decision-making and computation phases.

The diagram is divided into three main sections: (i) *Choice of Positioning Mode and Methods*: The positioning method and mode of operation are selected based on system requirements and environmental conditions. (ii) *Measurement Setup and Collection*: Positioning measurements are obtained, influenced by factors such as the number of gNBs and the

RF settings. (iii) *Processing and Localization*: Based on the measurements obtained in the previous step, position estimation is computed depending, for example, on the selected and implemented algorithm.

This section introduces the system model for the localization problem in 5G and beyond, incorporating multiple key performance indicators and expressing their costs in terms of the system's fundamental parameters. In particular, we focus on latency, accuracy, resource usage, and resilience against security threats.

Latency Cost

The latency response time comprises the latency times introduced by the involved components in the estimation procedure. Figure 8 shows the breakdown of total latency [48] into different components described in the following.

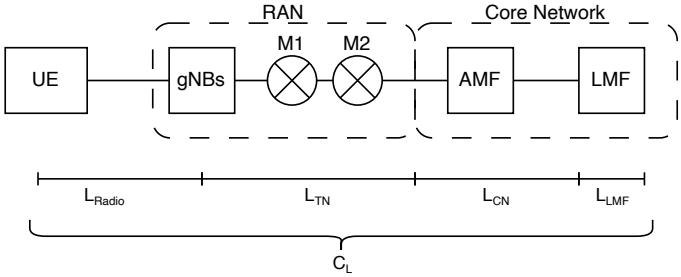

Figure 8: Breakdown of Latency Components in 5G Localization. This model illustrates the latency contributions from the UE, RAN, and the core network involved components.

- **Radio (L_{Radio})** is the delay introduced by the radio, its value depends on *(i)* the number of messages exchanged between the UE and the gNB ($N_{\text{msg}}^{\text{LPP}}$); *(ii)* the propagation time for each of exchanged message ($T_{\text{prop,UE-gNB}}$); *(iii-iv)* the radio processing time of the messages in the UE ($T_{\text{proc,UE}}^{\text{radio}}$) and in the gNB ($T_{\text{proc,gNB}}^{\text{radio}}$). The value of the term L_{Radio} is represented by Eq. (2.1).

$$L_{\text{Radio}} = N_{\text{msg}}^{\text{LPP}} \cdot (T_{\text{prop,UE-gNB}} + T_{\text{proc,UE}}^{\text{radio}} + T_{\text{proc,gNB}}^{\text{radio}}) \tag{2.1}$$

- **Transport Network ($L_{\mathbf{TN}}$)** is the delay introduced by the communication between the gNBs and the 5G Core, through the network nodes (M1 and M2 in Figure 8), as described in Eq. (2.2). The value of this term is the sum of *(i)* the propagation time from the gNBs to the 5G Core Network ($T_{\text{prop,gNB-CN}}$) and *(ii-iii)* the message networking processing time in the gNB ($T^{(\text{net})}_{\text{proc,gNB}}$) and in the 5G Core ($T^{(\text{net})}_{\text{proc,CN}}$), multiplied by the number of the exchanged message which corresponds to the sum of LPP and NRPPa messages ($N_{\text{msg}} = N^{\text{LPP}}_{\text{msg}} + N^{\text{NRPPa}}_{\text{msg}}$).

$$L_{\text{TN}} = N_{\text{msg}} \cdot (T_{\text{prop,gNB-CN}} + T^{(\text{net})}_{\text{proc,gNB}} + T^{(\text{net})}_{\text{proc,CN}}) \tag{2.2}$$

- **Core Network ($L_{\mathbf{CN}}$)** is the result of the delay introduced by message forwarding from the 5G Core to the AMF ($T_{\text{prop,AMF-LMF}}$) plus the delay of the computation of the message in the AMF ($T_{\text{proc,AMF}}$) and in the LMF ($T_{\text{proc,LMF}}$).

$$L_{\text{CN}} = N_{\text{msg}} \cdot (T_{\text{prop,AMF-LMF}} + T_{\text{proc,AMF}} + T_{\text{proc,LMF}}) \tag{2.3}$$

- **LMF Latency ($L_{\mathbf{LMF}}$)** is introduced by the LMF during the execution of the positioning procedure. The LMF latency depends on: *(i)* the selected localization algorithm and its configuration parameters ($A_{\text{algo,imp}}$); and *(ii)* the number of gNBs (N_{gNB}), which influences the number of available measurements and consequently the complexity of the computation. The time complexity of the localization algorithms is not modeled analytically, but it is implicitly captured within the latency cost function. In particular, the execution time of each algorithm implementation ($A_{\text{algo,imp}}$) is evaluated experimentally.

Accuracy Cost

The accuracy in our model is defined following the criteria presented in Sec. 2.1, compliant with the 3GPP standard. In this context, the accu-

racy of the PSL is defined as the 95-percentile of the error between the estimated position ($\hat{\mathbf{p}}_{\text{ue}}$) and the true one ($\mathbf{p}_{\text{ue}}$).

The true error is computed as follows

$$\mathbf{e} = |\mathbf{p}_{\text{ue}} - \hat{\mathbf{p}}_{\text{ue}}| \tag{2.4}$$

The accuracy of the estimation depends on several factors, such as the quality, type, number of measurements, and the class of algorithm used in the computation. The terms that we take into consideration in our accuracy model are the number of measurements, therefore the number of gNBs (N_{gNB}) involved in the localization procedure, and the type of algorithms ($A_{\text{algo,imp}}$). Since the model prioritizes comparing various algorithm implementations and the configurations of the entities involved in the estimation process rather than accounting for measurement quality, specific parameters, such as RF settings (e.g., bandwidth and Subcarrier Spacing (SCS)), are kept constant and excluded from our case study analysis. Accuracy is influenced by N_{gNB}, increasing the number of measurements increases the total information of the system, thus improving position estimation. Still, on the other hand, the size of the system increases, resulting in an increase in time for the computation. However, different algorithms solve non-linear systems in various ways, resulting in varying levels of accuracy and latency regarding the size of the system. In practical scenarios, the selection of gNBs for localization could also be influenced by link reliability metrics. Selecting a subset of gNBs based on their reliability may help ensure consistent communication quality [49]. However, reducing the number of participating gNBs also reduces the number of available measurements, which can negatively affect localization robustness against attacks and errors, as illustrated in Figure 13. This highlights a trade-off between prioritizing highly reliable links and maintaining resilience through measurement diversity.

Resource Cost

The resource cost represents the computational resource required to calculate the target UE position. Two key factors influence this resource cost: (i) the type of algorithm used, whether it can be parallelized, and

(ii) the time used to complete the computation. Parallelizable algorithms typically have higher resource costs because they distribute the computational load across multiple processors or cores. This enables them to achieve better accuracy in the same amount of time compared to non-parallelizable algorithms. The increased resource expenditure allows for more complex and precise calculations, making parallelizable algorithms more effective for accurate location determination. Non-parallelizable algorithms, while potentially having lower immediate resource costs, may not reach the same accuracy levels within the same time constraints due to their sequential processing nature. Therefore, despite the higher resource cost, parallelizable algorithms are often preferred for their ability to deliver higher accuracy more efficiently.

$$C_{\mathrm{R}} = N_w \cdot A_{\text{algo,imp}} \tag{2.5}$$

Eq. 2.5 shows the resource cost, N_w is the number of workers used in the parallelized algorithm, each worker performs a subsection of the total computation, if the algorithm is not parallelizable N_w value is 1, and the $A_{\text{algo,imp}}$ term is the selected algorithm and method. It should be noted that an increase in the number of workers will result in an additional overhead cost associated with the distribution of the information required for the computation and the aggregation of the final results. Consequently, an increase in the number of workers does not necessarily result in a performance improvement and may even cause performance to deteriorate.

Resilience Cost

The security of the positioning system is modeled through the resilience cost (C_{S}), which quantifies the system's robustness against attacks and its ability to detect anomalies in a timely manner. This function integrates two key factors: (i) robustness against measurement tampering, (ii) vulnerability due to the attack surface and readiness to trigger integrity alerts.

- **Robustness Against Tampering Attacks.** The process of obtaining

measurements is fundamental to the overall positioning procedure due to the Over-the-Air (OTA) transmission of reference signals required for gathering location data. During this phase, the system is susceptible to surface attacks, where third-party entities can manipulate the signals transmitted by the UE or the gNB. Such manipulations can introduce significant errors in the position estimation, as demonstrated by recent studies [12], [13], [30].

The impact of tampered measurements can be mitigated by increasing the number of gNBs N_{gNB}, i.e., the number of measurements, involved in the estimation process.

A larger number of measurements can compensate for any erroneous data introduced by malicious entities, thereby enhancing the robustness and accuracy of the system. However, this approach introduces additional latency, as it increases the size of the non-linear systems to be resolved and extends the required computation time, depending on the algorithm used ($A_{\text{algo,imp}}$).

- **Privacy and Attack Surface.** The attack surface expands with the number of entities, N_{ent}, involved in the localization procedure. More components obtaining position measurements and forwarding messages between the function in charge of estimating UE position (i.e., the LMF or the dedicated xAPP) and the UE/gNB increase the potential points of vulnerability. For example, in the O-RAN architecture, since the Core Network is not involved in the localization process, the security associated with the localization process is greater since the possibly compromised entities involved are decreased. Nonetheless, considering the components between the RAN and the core network, it is unlikely that they would be malicious, thereby reducing the likelihood of successful attacks from these elements.

  Instead of relying on an absolute numerical metric, the resilience cost (C_{S}) is determined using a relative ranking approach. This ranking depends on two parameters: a higher gNBs which enhances redundancy and resilience, and a lower (N_{ent}) which mini-

mizes the attack surface and improves privacy.

Note that ensuring the readiness to provide positioning integrity alerts is essential for maintaining system resilience. This involves quickly detecting and reporting anomalies or manipulations in measurement data. Reducing communication latency enables faster alert issuance, improving the positioning system's overall integrity and reliability.

2.4.2 Multi-Objective Optimization Problem

We formulate the multi-objective optimization problem from the systems model mentioned in the previous section. The $C_{\mathrm{L}}, C_{\mathrm{A}}, C_{\mathrm{R}},$ and C_{S} represent, respectively, the cost function of latency, accuracy, resource usage, and security, which are to be minimized. The inputs to these cost functions, denoted as $I_{\mathrm{L}}, I_{\mathrm{A}}, I_{\mathrm{R}},$ and I_{S} correspond to the factors influencing each respective cost function, as defined in Sec. 2.4.1 and summarized in Table 5.

We present both a no-preference multi-objective formulation, treating all objectives equally, and a PSL-based scalarized version, which weights objectives according to the PSL requirements, i.e., latency, accuracy, resource, and security ($R_{\mathrm{L}}, R_{\mathrm{A}}, R_{\mathrm{R}},$ and R_{S}). These requirements can be adjusted according to the specific needs of the target application. For instance, autonomous driving scenarios may require sub-meter accuracy within 100 ms, as defined by the PSL specified in the 3GPP standards [10], [39]. In other domains, less stringent constraints may be sufficient. Since these objectives can conflict with one another, excessively tight requirements may lead to infeasible solutions. In the results section, for both optimization models, the requirements are set according to the specifications defined by the 3GPP in the PSL.

The convergence of the multi-objective optimization in our model is performed over a finite and discrete set of configurations. We adopt a brute-force evaluation of all feasible parameter combinations, ensuring the complete exploration of the global Pareto front. Therefore, convergence is inherently guaranteed by construction. For larger solution

Table 5: Input parameters (I_L, I_A, I_R and I_S) for the cost functions. The symbols $\uparrow$ and $\downarrow$ denote a monotonic increase and decrease of the cost function, respectively, while the symbol $\sim$ indicates am algorithm-dependent impact.

Cost Function	Input Parameters (Decision Variables)	Sign
Latency $C_L(I_L)$	• The number of gNBs and the chosen positioning mode and method, which both affect the number of exchanged messages ($N_\mathrm{gNB}, N_\mathrm{msg}$)	$\uparrow$
	• Processing times (UE, gNB, Core, LMF)	$\uparrow$
	• Chosen algorithm ($A_\mathrm{algo,\,imp}$)	$\sim$
Accuracy $C_\mathrm{A}(I_\mathrm{A})$	• Number of gNBs (N_gNB)	$\downarrow$
	• Positioning algorithm and its implementation ($A_\mathrm{algo,\,imp}$)	$\sim$
Resources $C_\mathrm{R}(I_\mathrm{R})$	• Number of parallel workers (N_w)	$\uparrow$
	• Type of algorithm ($A_\mathrm{algo,\,imp}$)	$\sim$
Resilience $C_\mathrm{S}(I_\mathrm{S})$	• Number of gNBs (N_gNB)	$\downarrow$
	• Number of involved network entities (N_ent)	$\uparrow$
	• Algorithm robustness ($A_\mathrm{algo,\,imp}$)	$\sim$
	• Latency for triggering alerts (C_L)	$\uparrow$

spaces, heuristic optimization methods such as Non-dominated Sorting Genetic Algorithm II (NSGA-II) [50] or Multi-Objective Evolutionary Algorithm based on Decomposition (MOEA/D) [51] could be considered; however, their convergence properties would depend on the specific algorithm and are beyond the scope of this work.

No-Preference

The multi-objective optimization problem with different requirements can be defined as

$$\begin{aligned} \min_{I} \quad & C_\mathrm{L}(I_\mathrm{L}),\, C_\mathrm{A}(I_\mathrm{A}),\, C_\mathrm{R}(I_\mathrm{R}),\, C_\mathrm{S}(I_\mathrm{S}) \\ \text{s. t.} \quad & C_\mathrm{L}(I_\mathrm{L}) < R_\mathrm{L},\, C_\mathrm{A}(I_\mathrm{A}) < R_\mathrm{A}, \\ & C_\mathrm{R}(I_\mathrm{R}) < R_\mathrm{R},\, C_\mathrm{S}(I_\mathrm{S}) < R_\mathrm{S} \end{aligned} \tag{2.6}$$

In this way, the possible solutions within this optimization problem are those that minimize one of the objectives included in Eq. (2.6), while the others may not be optimal but must satisfy the specified requirements. While our formulation remains general, a weighted sum of all objectives could be adopted to tailor the optimization to specific application needs.

PSL Based - Scalarized

In this optimization problem, the objective function to minimize considers only the weighted sum of accuracy and latency costs, with each cost function weighted by a factor dependent on the maximum of the requirements (i.e., R_{A} and R_{L}). While resource and security, in addition to the accuracy and latency costs, must also meet the PSL requirements, they are not included in the objective function.

$$\begin{aligned} \min_{I} \quad & \alpha_L C_{\mathrm{L}}(I_{\mathrm{L}}) + \alpha_A C_{\mathrm{A}}(I_{\mathrm{A}}) \\ \text{s. t.} \quad & C_{\mathrm{L}}(I_{\mathrm{L}}) < R_{\mathrm{A}},\ C_{\mathrm{A}}(I_{\mathrm{A}}) < R_{\mathrm{A}}, \\ & C_{\mathrm{R}}(I_{\mathrm{R}}) < R_{\mathrm{R}},\ C_{\mathrm{S}}(I_{\mathrm{S}}) < R_{\mathrm{S}}, \\ & \alpha_L = \frac{1}{R_{\mathrm{L}}},\ \alpha_A = \frac{1}{R_{\mathrm{A}}} \end{aligned} \tag{2.7}$$

2.4.3 Trade-Off Discussion

Optimization Considerations of Architectural Framework

In Sec. 2.1, we presented two main architectures for cellular-based positioning: one based on 3GPP specifications and the other utilizing the new O-RAN paradigm. The choice between these architectures can influence the factors involved in the multi-objective optimization problem associated with the positioning procedure. To minimize the cost function in this trade-off scenario, one effective strategy is to reduce the latency component, which can be achieved by adopting the O-RAN paradigm (see Figure 3). Indeed, unlike the 3GPP architecture depicted in Figure 2,

the O-RAN approach reduces latency by assigning the overall management of the positioning procedure to a dedicated xApp with capabilities comparable to the LMF. This shift transfers operational control from the core network to the RAN, where the xApp is deployed within the nRT RIC.

The main advantage of the defined use case [34], [35] is the reduction of the total latency needed for the estimation procedure. This is achieved by eliminating the propagation delays between the RAN and LMF while maintaining the radio latency unchanged. This modification does not impact the accuracy or resource requirements of the estimation process, as these factors are determined by the algorithm type and the number of measurements rather than the specific location of the computation. Additionally, security considerations are affected by the decision to use the O-RAN architecture rather than the 3GPP framework. Indeed, replacing the LMF with a dedicated xApp introduces new security dynamics and mitigates certain concerns by involving different entities in the localization procedure. With core network functions excluded from this scenario, core network-related positioning threats are eliminated. However, physical threats related to communication between the target UE and the RAN, such as spoofing attacks, remain unchanged from the 3GPP case. Excluding the core network reduces communication latency, enabling faster alert triggering and enhancing the overall security of the positioning system. Furthermore, this change decreases the attack surface, thereby strengthening the system's resilience against threats.

Thus, focusing specifically on the positioning procedure, adopting the O-RAN paradigm over the 3GPP approach offers significant advantages in terms of latency optimization. On the other hand, considering the entire system, the O-RAN paradigm may introduce challenges that are not present in the 3GPP architecture, such as AI/ML security threats [52], but this is out of the scope of this analysis.

Optimization Considerations of Positioning Modes and Methods

The LMF is responsible for determining the positioning method and mode, taking into account the capabilities of both the UE and the network. This

decision significantly influences the parameters of the multi-objective optimization problem. Different methods, as specified by 3GPP in [22], involve obtaining diverse types of measurements during the localization process, such as angle, time, and cell information. These measurement types influence the algorithm's accuracy, with time and angle measurements typically providing higher precision than cell-based information like NR eCID. Another essential factor in mode selection is the latency cost, as different modes necessitate varying numbers of message exchanges between the entities involved in the procedure. For example, [53] analyzes the time required to perform the E2E localization estimation across various modes, as summarized in Table 6.

Table 6: E2E Latency Costs for Different Positioning Modes and Methods [53]. The table highlights the range of latency values in milliseconds.

Position Modes and Methods	**E2E Latency [ms]**
UE Assisted DL-TDOA/DL-AOD	222.5-353
UL-TDOA and UL-AOA	149-322
Downlink NR E-CID	88-198
Uplink NR E-CID	59-125.5
UE Assisted Multi-RTT	288.5-486

A comparison between downlink and uplink scenarios (the first four cases) highlights notable differences, particularly in UE-Assisted (UE-based) and Network-Based scenarios. In uplink scenarios, the NRPPa protocol is utilized more frequently than LPP, resulting in fewer message exchanges between the LMF and the target UE. This reduction lowers latency costs by eliminating the radio term. The advantages of uplink are independent of the estimation technique used. However, the time required to obtain measurements varies depending on the type of measurement. For instance, the E2E latency for NR eCID, whether in uplink or downlink, is generally lower than for methods utilizing angle or time data. On the other hand, the multi-RTT technique enhances accuracy by reducing synchronization complexity among multiple gNBs but increases the overall time needed to collect time measurements from both the UE and the gNB.

The choice of mode and method also impacts the terms of security and resources. Different methods and modes lead to different security threats and attack surfaces. For instance, trusted entities like the target UE can potentially manipulate location information within the positioning protocol's messages. Regarding resource terms, the selection of the position mode determines whether the UE or the LMF is responsible for computing the location estimation. This choice affects the resource capabilities and constraints in the optimization problem, thereby influencing the associated cost function.

Optimization Considerations of Position Algorithms and Implementation

The type and implementation of the algorithm used in the estimation process of the target UE affect various cost functions in the model. Here, we provide an overview of some algorithms that can be used to compute the location of a target UE, followed by a discussion of how these choices impact the optimization problem. The case studies section provides a more detailed evaluation of these algorithms. In this analysis, we explore two primary methods for position estimation: a non-linear algorithm based on gradient descent and a Brute Force (BF) approach.

The *Non-Linear Algorithm* are efficient in terms of computational resources, making them suitable for real-time scenarios. However, they may suffer from convergence to local minima, particularly when initial conditions are not ideal. The study considers the following methods:

- **Conjugate Gradient (CG):** One of the most popular alternatives to the gradient descent method, uses the conjugate gradient algorithm to minimize the scalar function of one or more variables [54]. CG, assuming exact arithmetic, converges in at most n steps, where n is the size of the matrix of the system.
- **Broyden–Fletcher–Goldfarb–Shanno (BFGS):** Minimizes a scalar function of one or more variables using the BFGS algorithm [48], an iterative method for solving unconstrained nonlinear optimization problems

- **Limited-memory BFGS Bound (L-BFGS-B):** is an optimization algorithm in the family of quasi-Newton methods that approximates the BFGS using a limited amount of computer memory [55]. It is particularly effective for solving optimization problems with constraints on the limits of variables, as it considers these constraints during the optimization process.

- **Newton-CG**: combines the Newton method with the Conjugate Gradient technique [56]. It converges to the minimum by approximating the Hessian matrix to find the search direction of the gradient descent.

Methods like CG and BFGS offer a balance between computational efficiency and accuracy, but can be sensitive to the starting points.

Employ a *Brute Force Grid Based Algorithm* strategy to minimize a function over a given range, this approach aims to find the global minimum of the function by computing the value of the function at each point of a multidimensional grid of points. Due to the exponential increase in the number of grid points, the BF approach is computationally inefficient in terms of time and memory usage. Indeed, the execution of the minimization function may take a long time and/or incur memory limitations, even with coarse grid spacing and even with moderate-sized problems.

The choice of algorithm to be used affects the system performance; as described by the model in the previous section, a trade-off must be found between latency, performance, resources, and security. Regarding the first approach, different methods result in varying levels of accuracy and latency, depending on the type of algorithm used as a baseline. A clear discussion point is the trade-off between latency and accuracy when considering only the BF approach. In fact, this approach achieves higher accuracy in estimation, but the time required to obtain the results increases. However, latency can be reduced by increasing the number of workers during the computation while still satisfying resource constraints. This trade-off in the implementation of the estimation algorithm is further explored in Sec. 2.5.1, where it is evaluated through several nu-

merical simulations.

2.5 Case Study

This section presents the proposed system model and an implementation of the multi-objective optimization problem presented in Sec. 2.4.2 through simulation and experimental results. First, sample-level simulations conducted in a standard scenario are used to evaluate the impact of different positioning algorithms and their implementation on multiple performance indicators, focusing on accuracy and resource cost. Then, we experimentally assess the latency of an E2E localization procedure using the uplink TDOA positioning method, utilizing the SRS [57]. The simulation results and experimental data are then combined to discuss a single case study in which the trade-off between latency, accuracy, resilience, and resources is evaluated.

2.5.1 Simulation Settings and Results

We investigate how different algorithmic approaches and implementations ($A_{\text{algo, imp}}$) impact performance indicators. Using Python [58], we implemented and evaluated all the algorithms mentioned in Sec. 2.4.3, using TDOA measurements, relying on the PRS [57].

Simulation Settings

The sample-level simulation is set up as follows:

- **3GPP Scenario:** The chosen scenario is the 3GPP outdoor UMi [59], the gNBs inter-space distance is set to 200m within an area of 800m by 800m, and the target UE is randomly located as shown in Figure 9.

- **5G NR signaling:** The PRS is configured with a carrier frequency of 3.4 GHz, a bandwidth of 100 MHz, and a SCS of 60 kHz [57]. This configuration is chosen to ensure high-accuracy positioning

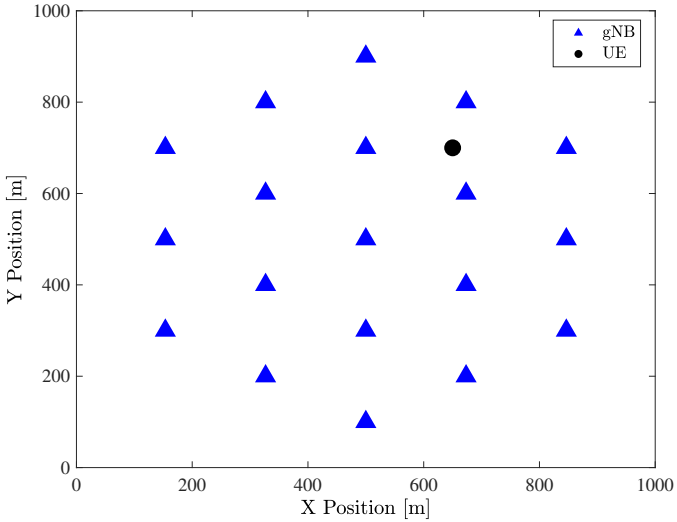

Figure 9: Urban Micro-cellular (UMi) Simulation Configuration. This configuration follows the 3GPP specification [59] with gNB inter-space distances set to 200m within an 800m by 800m area.

in 5G networks. The channels between the target UE and the gNBs are assumed to be in a Line-of-Sight (LOS) condition.

- **Algorithms:** Algorithms are implemented using the Scipy [60] module, leveraging the optimize sub-module to vary $A_{\text{algo, imp}}$, described in 2.4.3.

- **Server:** The served used is a Dell EMC PowerEdge R640 powered by 2x Intel Xeon Silver 4110 CPU with 8 cores @2.10 GHz (max 3.00 GHz), running Ubuntu 18.04 LTS with 5.17 Linux kernel.

Results

Figure 10 shows the positioning error for the target UE using the methods mentioned in 2.4.3. The x-axis shows the number of iterations performed by the algorithm, while the y-axis displays the error measured in meters on a logarithmic scale. Initially, when the number of iterations

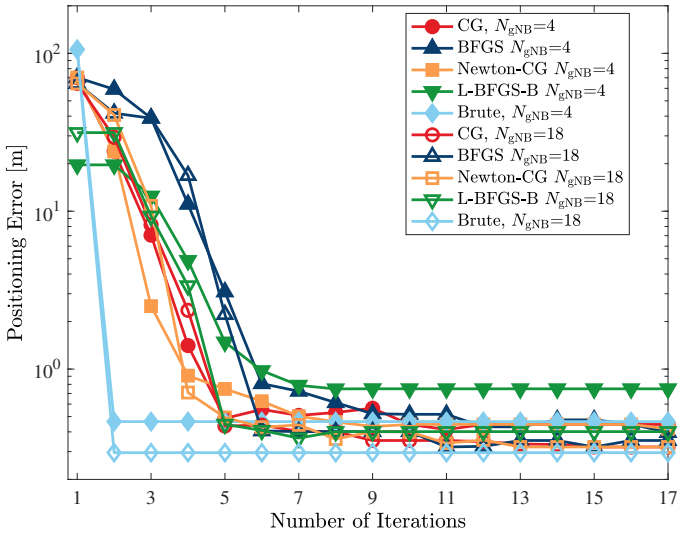

Figure 10: Position Estimation Error vs. Number of Iterations. Comparison of brute force and non-linear algorithms using 4 gNBs (full markers) and 18 gNBs (empty markers). The y-axis shows the error in meters on a logarithmic scale.

is low, the position estimation error is high across all methods. As the number of iterations increases, the error decreases and stabilizes, converging to a minimum value determined by the chosen algorithm and configuration.

The graph compares position estimation errors for configurations using 4 gNBs (represented by full markers) and 18 gNBs (represented by empty markers). As shown in Figure 7, both the number of gNBs and the number of workers significantly influence the performance. Specifically, increasing the number of gNBs reduces the error and results in higher algorithm latency. The BF algorithm (shown in light blue) demonstrates very low error rates even from the initial iterations, highlighting its high accuracy. In contrast, non-linear algorithms (such as CG, BFGS, Newton-CG, and L-BFGS-B) require more iterations to stabilize and do not reach the same level of accuracy as the BF method.

Figure 11 and Figure 12 illustrates the position estimation latency ver-

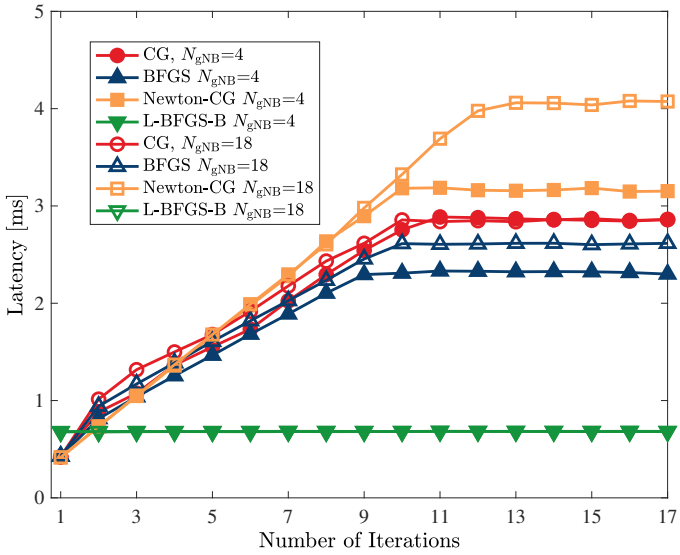

Figure 11: Position Estimation Latency vs. Number of Iterations for Non-Linear. The full markers represent the case with 4 gNBs while the empty one is 18 gNBs.

sus the number of iterations for non-linear algorithms and the number of workers for the brute force algorithm, respectively, showing a significant difference in the latency performance of the two types of algorithms.

The latency, shown in Figure 11, ranges from approximately 0.8 to 4.5 ms, depending on the specific algorithm used. In this case, latency is a monotonic function of the number of iterations, steadily increasing as the number of iterations increases, until convergence is reached. Notably, only the L-BFGS-B method remains unaffected by the number of iterations or the number of gNBs due to its simplified Hessian inverse computation, using the most recent gradients instead of the full gradient history.

In contrast, Figure 12 displays the latency of the BF algorithm, ranging from 50 to 160 ms, influenced by the number of workers. The analysis focuses on two cases: when the number of iterations $N_{\text{iter}} = 2$ and when $N_{\text{iter}} > 2$. Here, latency is not a monotonic function of the number of

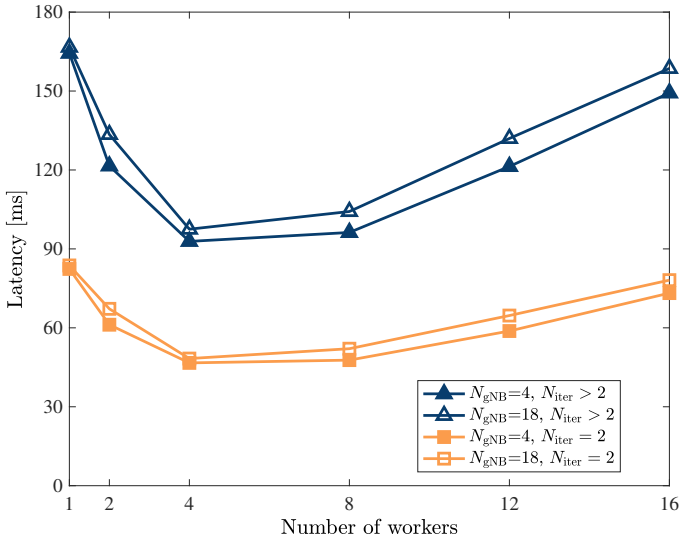

Figure 12: Position Estimation Latency vs. Number of Workers for Brute Force Algorithms. The full markers represent the case with 4 gNBs while the empty one is 18 gNBs.

workers. Increasing the number of workers initially decreases latency. Still, beyond a certain threshold (in our case, $N_{\text{w}} = 4$), the overhead of managing additional workers outweighs the benefits of parallel computation, causing an increase in latency. Both approaches show increased latency with a higher number of gNBs, reflecting the added computational complexity. The non-linear algorithms exhibit a significant increase in latency with more iterations, except for L-BFGS-B. The brute force algorithm's latency, influenced by worker count, demonstrates the importance of balancing parallelization costs against computational gains.

As the optimization is performed over a finite and discrete set of configurations, convergence is ensured by design. For the localization step, Figure 11 and Figure 12 show the convergence behavior of non-linear algorithms (BFGS, L-BFGS-B), which are faster but sensitive to initialization. In contrast, the brute-force method guarantees convergence to the global minimum, at the cost of higher computational effort.

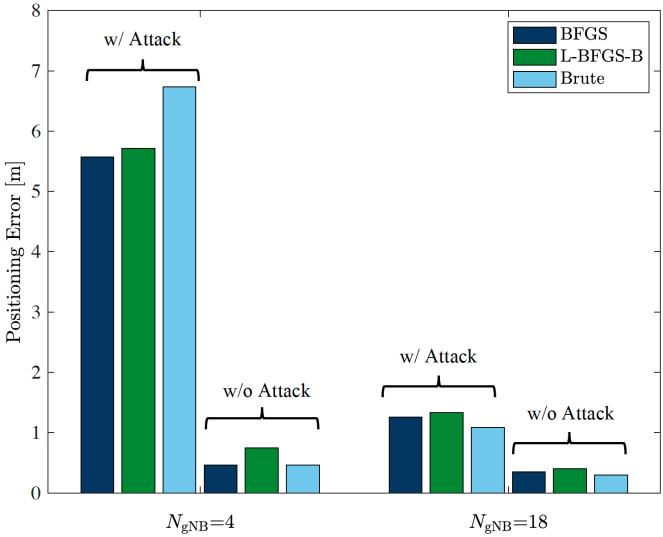

Figure 13: Positioning Error w/ and w/o attack for different algorithms (BFGS, L-BFGS-B, and Brute Force) and gNB configurations (4 and 18).

To evaluate the robustness of the algorithms against tampering attacks, we selected three methods: BFGS, L-BFGS-B, and the BF with 4 workers. The tampering attack was simulated by introducing a time offset equivalent to a 15 meter error in one of the TOA measurements, resulted in erroneous TDOA values. Figure 13 shows the positioning error for three different algorithms (BFGS, L-BFGS-B, and BF) in scenarios with and without a tampering attack on one of the gNBs, considering configurations with 4 and 18 gNBs.

The bar plot clearly demonstrates the attack's impact and the effect of the number of gNBs on positioning accuracy. Under attack conditions with 4 gNBs, the positioning error increases by approximately 5 to 6 meters. In contrast, with 18 gNBs, the error increases by only about 1 meter. As shown in the flow diagram Figure 7, the number of gNBs influences the selection of the positioning method and mode, which in turn affects the resilience cost. As expected, the error decreases as the number of gNBs increases, improving the system's robustness against tampering

attacks. This highlights the importance of having more measurements to mitigate the adverse effects of attacks on positioning accuracy.

2.5.2 Experimental Setting and Results

End-to-End latency is evaluated in an experimental scenario by performing the E2E 5G localization within our testbed, using the uplink TDOA method as described in [22].

Experimental Testbed

The testbed includes four main elements: the LMF and the core network, the RAN, COTS UE, and the server.

- **LMF and Core network:** Due to the lack of open-source LMF implementations, we developed a 3GPP-compliant LMF using Python, available at [61]. Our LMF communicates with the target UE using LPP and with gNBs using NRPPa, in compliance with the 3GPP standards [36], [37]. The LMF connects to the core network via the SBI, as depicted in Figure 2, and communicates exclusively with the AMF through its exposed services. For user position estimation, the AMF utilizes services provided by the LMF, as detailed in [40], [41]. Our LMF is integrated with various open-source 5G core network projects, i.e., *free5GC* [43] and OAI core network [44]; for more details, refer to [27]. Integration required modifications to the AMF handler to support the forwarding of LPP and NRPPa messages.
- **RAN:** Our testbed includes a gNB based on the OAI project, featuring NRPPa functionalities. We utilized Ettus USRP X310 SDR devices [47] as radio transceivers. These devices support a wide frequency range from 10 MHz to 8 GHz, covering all NR FR1 bands with up to 400 MHz of instantaneous bandwidth. The transceivers are equipped with vertically oriented VERT2450 antennas.
- **COTS UE:** The target UE utilized in our localization testbed is the Google Pixel 6.

- **Server:** We used the same server from the simulation case study to deploy our RAN and core network.

Results

Within the described testbed, we performed the E2E localization procedure, focusing on the time required for each step of the estimation process. The messages exchanged between the involved entities are illustrated in Figure 14. Furthermore, this figure illustrates the diverse timers employed throughout the latency analysis, along with the corresponding delta times.

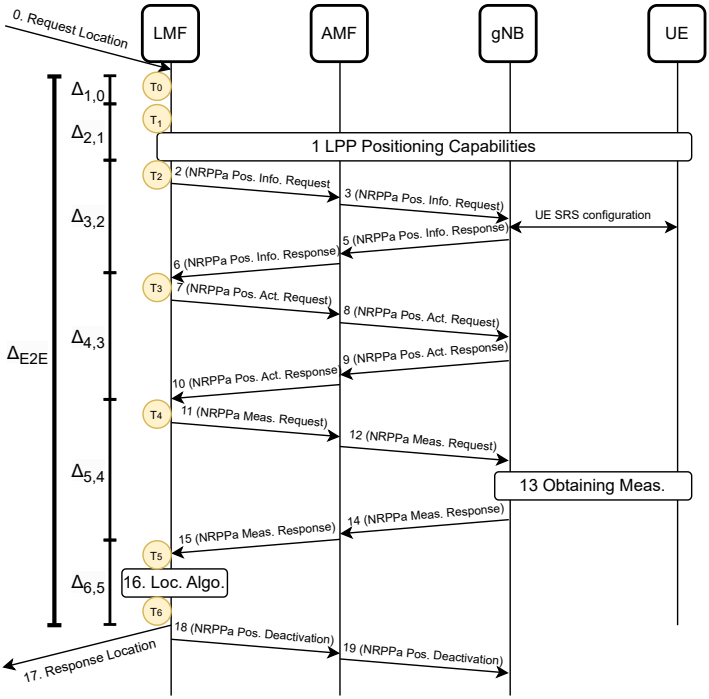

Figure 14: End-to-End Localization Procedure using UL-TDOA. Illustration of message exchanges and timing involved in the UL-TDOA method, with yellow circles indicating the different timers in the estimation process.

Table 7 summarized the latency analysis results, highlighting the operations involved and the time required for each step.

Table 7: End-to-End Latency Results for UL-TDOA Method. Summary of the time required for each step in the UL-TDOA localization procedure, including the mean delta time for handling NRPPa messages and LPP requests.

Operation	Loc. Handler	LPP Pos. Cap.	NRPPa Pos. Info.	NRPPa Pos. Act.	NRPPa Meas.	Algo.	E2E
Delta	$\Delta_{1,0}$ [ms]	$\Delta_{2,1}$ [ms]	$\Delta_{3,2}$ [ms]	$\Delta_{4,3}$ [ms]	$\Delta_{5,4}$ [ms]	$\Delta_{6,5}$ [ms]	Δ_{E2E} [ms]
Mean	9.21	231.02	12.39	8.38	7.82	11.02	279.85

From the analysis, it is evident that the time needed to handle each NRPPa message is around 7/8 ms, except for the first message, which requires more time due to the configuration of the SRS signal necessary for estimation. The time required for handling the LPP request/response capabilities is around 231 ms. Consequently, the E2E latency is approximately 280 ms.

Despite these factors, the experimentally measured latency successfully meets some PSL requirements [39], specifically satisfying the PSL 1-4 latency requirements. It should be emphasized that the delta time for handling LPP position capabilities messages is considered reasonable because it is derived using a commercial COTS UE, which processes and responds to requests as the standard specified. The OTA propagation time in this case study can be considered negligible since the entire testbed is situated within a single room. However, the remaining latency measurements are obtained using the OAI gNB open-source project. It should be highlighted that, specifically for positioning purposes, the implementation of NRPPa functionalities within OAI is still in its preliminary stages. While acknowledging this limitation, the experimental results obtained from this testbed are nonetheless encouraging and demonstrate the potential of the evaluated system.

2.5.3 Trade-off Optimization Model Analysis

We can draw several conclusions from the results of the two case studies. In the simulation case study, we primarily investigate the trade-off

between accuracy and latency. In the experimental case study, we evaluate the time required to perform a complete E2E localization procedure using network-based methods. By analyzing these two cases and applying the proposed multi-objective optimization model, we can determine which combinations of algorithm and implementation (i.e., $A_{\text{algo,imp}}$ and number of workers N_{w}), and network configuration (i.e., number of gNBs N_{gNB}) can meet the 3GPP standardized PSLs requirements.

Feasible Solutions

Figure 15 shows all the feasible points that satisfied the different PSLs requirements represented by the shaded regions.

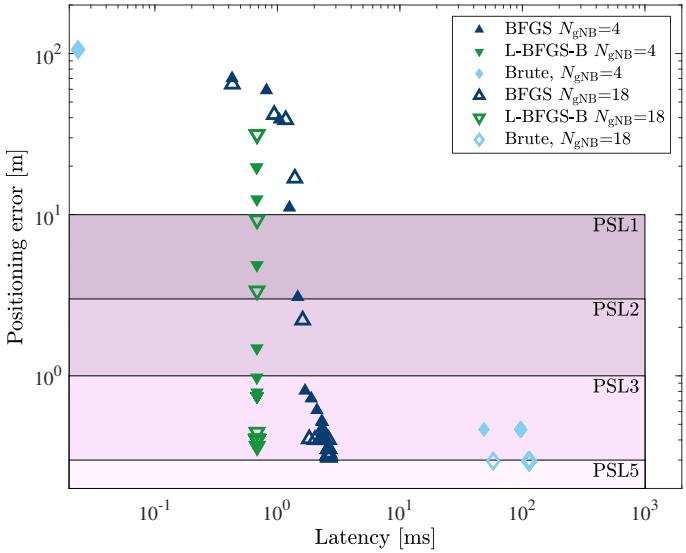

Figure 15: Position Estimation Error vs. Latency. Comparison of brute force and non-linear algorithms using 4 gNBs (full markers) and 18 gNBs (empty markers).The different shaded regions represent the various PSL requirements in terms of latency and accuracy. Both axes are on a logarithmic scale.

For the lower PSLs 1, 2, and 3, all combinations of the algorithms considered in the simulation case study meet the accuracy and latency requirements. For PSL 5, where accuracy is more critical than latency,

only the BF algorithm with $N_{\text{gNB}} = 18$ satisfies the requirements of the localization service. Instead, for PSLs 4 and 6, which have stringent latency requirements, i.e., 10/15 ms, no combination of $A_{\text{algo,imp}}$, N_{w}, and N_{gNB} meets the criteria, as the UE positioning capabilities exchange ($\Delta_{2,1}$) alone takes approximately 231 ms. Table 8 summarizes the discussed results.

Table 8: PSL Satisfaction by Localization System Configurations. Comparison of non-linear and brute force algorithms with 4 and 18 gNBs in meeting the accuracy and latency requirements for different PSLs.

PSL	Requirement		Algorithm			
			Non-linear		Brute Force	
	Accuracy	Latency	4 gNB	18 gNB	4 gNB	18 gNB
1	10m	1000ms	All methods	All methods	All N_{w}	All N_{w}
2	3m	1000ms	All methods	All methods	All N_{w}	All N_{w}
3	1m	1000ms	All methods	All methods	All N_{w}	All N_{w}
4	1m	15ms	None	None	None	None
5	0.3m	1000ms	None	None	None	All N_{w}
6	0.3m	10ms	None	None	None	None

Pareto Efficient Solutions

Within our multi-objective optimization problem, there is not a single optimal solution, but rather multiple solutions. Therefore, we present a set of Pareto efficient solutions, i.e., points where no cost function can be improved without causing a deterioration in at least one other objective [62], for the two optimization problems described in Sec. 2.4.2.

Figure 16 shows all the feasible solutions within the requirement of PSL 1. The Pareto efficient solutions for the no-preference optimization problem are highlighted in yellow, while those for the scalarized problem are shown in green. Additionally, the dashed circular line includes feasible and efficient solutions that meet the PSL 5 requirement. Some points within this dashed circle are colored yellow with green outlines, indicating that they are Pareto solutions of the no-preference problem under the PSL 1 constraint and the scalarized problem under the PSL 5 requirement.

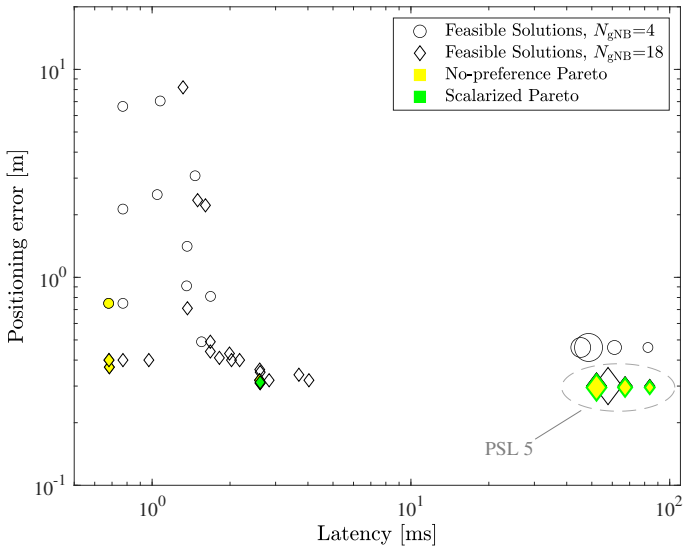

Figure 16: Feasible and Pareto efficient solutions with requirements of PSL 1 and 5 (dashed circle) of No-preference (in yellow) and Scalarized (green) optimization problem, where the dimension of the point indicates the number of workers.

In the no-preference optimization problem, represented by the yellow solutions, the L-BFGS-B and BF algorithms were used. The lower latency solutions are achieved with L-BFGS-B and configurations of 4 and 18 gNBs, with the 4 gNB setup leading to the minimum latency. The other solutions, using the BF approach with 18 gNB and varying the number of workers (1, 2, and 4), achieve the minimum positioning error but have significantly higher latencies.

For the scalarized optimization problem, the green solutions represent the Pareto efficient points. The BFGS algorithm with 18 gNBs under the PSL 1 constraint results in a positioning error of 0.32 m and a latency of 2.60 ms. Under the PSL 5 constraint, the BF algorithm with 18 gNB and different worker configurations (1, 2, and 4) achieves Pareto solutions, with the configuration using 4 workers reaching a latency of 52.13 ms and a positioning error of 0.29 m.

2.6 Summary and Outlook

This chapter provided a general background on 5G positioning, outlining its principles, architectures, and protocols, and was complemented by an experimental assessment based on both open-source and commercial implementations. By integrating the proposed LMF with 3GPP-standard protocols and leveraging full RAN and core network functionalities, we carried out extensive tests with a variety of commercial off-the-shelf UEs. These experiments evaluated supported signals, positioning modes, and protocols, offering a realistic view of the current capabilities and maturity of 5G positioning solutions.

In addition this chapter provides a model to frame cellular localization and beyond as a multi-objective optimization problem. This approach offers a valuable framework for designing efficient and reliable location services in 5G and beyond, enabling informed trade-offs between latency, accuracy, resource use, and resilience in 5G and future networks. Through simulations, we assess the performance of different algorithms and system parameters, revealing inherent trade-offs among these factors and including architectural aspects. Experimental results further validate the model by measuring end-to-end latency for the Uplink TDOA procedure using COTS equipment. The findings show that, while basic requirements are satisfied by various configurations, achieving higher service levels demands a more specific implementation of algorithms and system configurations. Moreover, our proposed model provides valuable guidance in selecting the optimal configuration and algorithm implementation to meet specific performance requirements and constraints.

It is essential to recognize that 5G positioning is not solely a matter of achieving high accuracy or minimizing latency. As positioning capabilities are increasingly integrated into critical and sensitive applications, aspects such as security become equally important. While this chapter has primarily addressed the technical foundations, experimental readiness, and performance trade-offs of 5G positioning, the following chapters will turn to a central and emerging challenge in this domain: ensur-

ing the (physical-layer) security of 5G positioning systems. Tackling this dimension is crucial to deliver trustworthy, resilient, and secure location services in future cellular-networks.

Chapter 3

Principles of 5G Positioning Security

Initially, 5th Generation (5G) positioning focused primarily on accuracy and latency as mentioned in the previous Chapter. Then, its scope has expanded to include reliability and integrity, emphasizing the need and the urgency of researching adversarial localization strategies and developing robust countermeasures against location security threats in 5G networks. However, the security challenges of cellular-based positioning, particularly in 5G, remain underexplored compared to the well-researched domain of Global Navigation Satellite System (GNSS). The inherent complexities of cellular networks, with their distinct measurements, protocols, and entities, require dedicated security analysis to uncover critical vulnerabilities and devise effective countermeasures. The 5G localization service relies heavily on physical-level measurements of reference signals, such as time, power, and angle, which are exchanged among multiple network entities through dedicated protocols. While these measurements are processed through various localization methods to enhance flexibility and precision, they simultaneously broaden the system's attack surface.

In this context, this Chapter aims to raise awareness of the adversarial threats targeting 5G positioning services by presenting a detailed secu-

rity analysis.

3.1 5G Positioning Threats

This section provides a detailed taxonomy of potential threats to the 5G localization services. It highlights the security risks associated with various positioning methods and architectures, including 3rd Generation Partnership Project (3GPP) and O-RAN frameworks, and explores emerging applications like sidelink positioning.

3.1.1 Taxonomy of Positioning Threats

5G positioning systems face various security threats, which can be categorized into the following three primary types: Tampering attacks, Poisoning attacks and Jamming attacks.

Tampering

Tampering attacks involve altering or manipulating data, which affects three key data types: (i) signal measurements (e.g., angle, time, or cell ID); (ii) the estimated location of the target User Equipment (UE) or (iii) anchor nodes (gNodeBs (gNBs) and UEs) information used as assistance location data. We categorize tampering into logical and physical types:

- **Logical Tampering:** Modifies measurements or location estimates within the payload of positioning protocols. For example, a malicious node in the network might alter Round Trip Time (RTT) or Time Difference of Arrival (TDOA) values.
- **Physical Tampering:** Alters the physical properties of signals. For instance, spoofing attacks introduce intentional delays to manipulate timing measurements.

Figure 17 presents a geometric overview of a representative (non-exhaustive) set of New Radio (NR)-based positioning methods and demonstrates how a single corrupted uplink TDOA measurement can distort

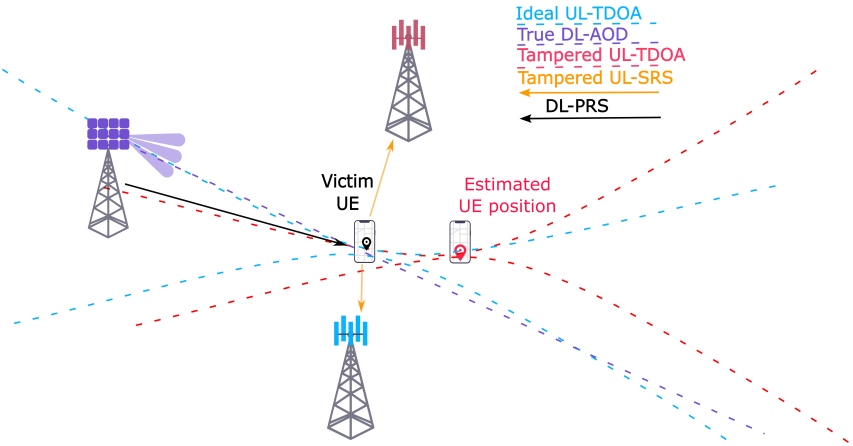

Figure 17: Geometric example of a representative (non-exhaustive) set of 5G-based positioning methods. Tampering a single uplink TDOA measurement shifts the estimated position of the target UE.

the estimated target position. Indeed, these alterations can distort the hyperbolic curves (indicated by tampered uplink TDOA in the figure), leading to significant UE's location estimation errors.

Poisoning of Training Datasets

Poisoning attacks are malicious manipulations of training data to compromise the integrity and reliability of the Artificial Intelligence (AI)/Machine Learning (ML)-based localization algorithms [63]. These attacks inject carefully crafted malicious data, such as distorted signal strength or manipulated location measurements, into the training dataset. Their goal is to deceive the model during learning, causing it to form incorrect associations between features and location clues, which leads to inaccurate predictions or misclassifications.

Jamming

Jamming attacks are a disruptive form of interference that significantly impact positioning systems by artificially increasing the channel noise to

degrade the signal-to-noise ratio, thereby disrupting the accurate transmission and reception of positioning signals. Such attacks can lead to service interruptions and, in severe cases, cause a complete Denial of Service (DoS) for the entire positioning system, rendering it inoperable.

3.1.2 Architecture: Security Threats Aspects

This subsection explores the security challenges within 5G positioning architectures, focusing on 3GPP, O-RAN, and sidelink scenarios. It examines vulnerabilities in the core network, the expanded attack surface introduced by O-RAN's AI/ML integration, and trust issues in sidelink positioning's direct UE-to-UE communication.

3GPP Positioning: General Framework

Core networks and Network Functions (NFs) face three primary security threats that can compromise the localization process:(i) *DoS* attacks where, for example, internal NFs may reject or fail to forward localization requests; (ii) *Compromised Location Systems*, where malicious entities could infiltrate the network, introducing rogue components (e.g., the Access And Mobility Function (AMF) selecting a malicious Location Management Function (LMF)); and (iii) *Unauthorized Access*, where the localization procedure might be initiated without proper authorization, exposing sensitive positional data. While the likelihood of a malicious entity infiltrating the core network and attacking the 5G localization services is relatively low, given that NFs are physically secured and managed by trusted network operators, external communications and interactions with third-party entities significantly broaden the threat landscape. These interactions, such as obtaining measurements from untrusted UEs or gNBs, introduce vulnerabilities to attacks like *spoofing*, *jamming*, *wormholes*, and *Man-in-the-Middle (MITM)*. Compared to internal threats, external attacks from untrusted entities or third-party actors are more prevalent and pose a substantially higher risk.

3GPP Positioning: Sidelink Framework

Unlike traditional positioning methods Sidelink (SL) relies on measurements and location data from potentially untrusted entities, such as UEs, which creates notable security challenges. Trust issues arise as even Located UEs, though registered within the Public Land Mobile Network (PLMN), can act maliciously by providing falsified information, introducing delays, or transmitting inaccurate positional data, thereby compromising the localization process. The reliance on direct UE-to-UE communication increases the system's vulnerability to tampering, data manipulation, and other security threats. To mitigate these risks, 3GPP has established robust security protocols in TS 33.533, focusing on authorization, privacy, and integrity of both unicast and broadcast communications among UEs in SL positioning scenarios.

O-RAN Positioning

O-RAN introduces unique security challenges in addition to traditional threats faced by 3GPP positioning systems. A significant concern in O-RAN positioning is the vulnerability of AI/ML models to poisoning attacks. Attackers could poison these models by feeding them with malicious position data, leading to erroneous position estimations, where injected random data causes the model to output inaccurate or meaningless positions, or targeted misclassifications, where specific malicious location data causes the model to misclassify or estimate adversarially desired positions. Such attacks highlight the importance of robust safeguards to ensure the integrity and reliability of AI/ML-based positioning mechanisms.

3.2 Threat Model

Building on the attack surface and vulnerability analysis detailed in Section 3.1.1, this section presents a comprehensive analysis of specific attack scenarios targeting 5G positioning systems, under the assumption that the UE is configured to support this service. We first described the

potential threats posed by external entities, considering two levels of attacker capabilities: one with limited knowledge of the positioning configuration system, and the other without this limitation, i.e., the attacker knows the Positioning Reference Signal (PRS) configuration. Then, we analyze possible malicious behavior carried out by a trusted entity involved in the positioning procedure with the purpose of interfering with the service.

3.2.1 External Third-Party Attacker

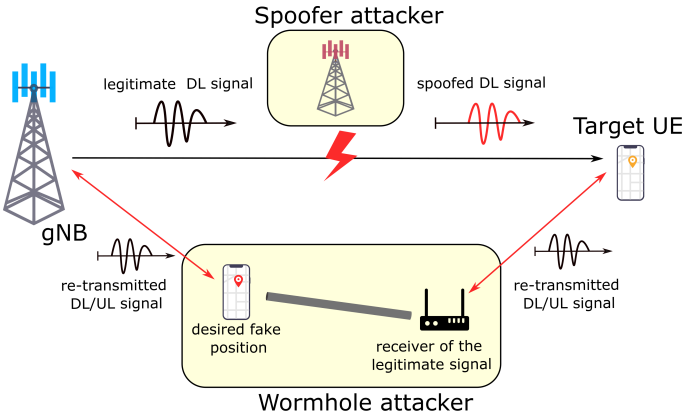

Figure 18: Third-party attacks. The upper part represents a spoofer attacker tampering the downlink signal from the gNB to the victim UE. The lower part shows the wormhole attacker that establishes two fake connections, one with the target UE and the other with the gNB.

Spoofing

A malicious third party external to the communication between the target UE and the LMF can perform a spoofing attack. In particular, the attacker attempts to modify the physical property of the signal transmitted by the UE or by the gNBs, leading to a physical tampering attack. This threat can affect all the positioning modes since the attack surface consists of the communication between the UE and the network. Figure 18

illustrates how the spoofer attacker acts on the communication between the target and the gNB by physically altering the signals in the air.

We analyze two attack strategies that a malicious third party may adopt to tamper with positioning measurements, based on their capabilities and knowledge of the reference signal's properties. The first, requiring low capabilities, is a meaconing attack where the attacker does not know the specific PRS configuration but is aware of the carrier frequency. By retransmitting an entire 5G frame, including the PRS, with higher power and a controlled delay, the attacker exploits the capture effect to overshadow the legitimate signal. This introduces spurious peaks in the correlation function and biases the Time of Arrival (TOA) estimate, as demonstrated in [12]. The second, requiring high capabilities, is a spoofing attack where the adversary has knowledge of the PRS configuration. As shown in [14], the attacker forges the PRS signal alone, without affecting data traffic, by leveraging the absence of two-way authentication. This allows selective manipulation of timing measurements through precomputed delay injections, misleading the receiver to estimate a false position.

Wormhole & Man-in-the-middle

The wormhole attack is a major threat to wireless networks, including 5G positioning. The goal of this attack is to alter the original signal propagation path by creating a rogue tunnel, thereby fooling the system into perceiving a different path than the legitimate one. To better understand the attack architecture, Figure 18 shows the principle of a wormhole attack on the localization systems. As shown in the figure, the attacker establishes two fake connections (both uplink and downlink) and creates the rogue tunnel that undermines the time or angle measurements. In addition to the wormhole attack, a potential threat is posed by the MITM attack. The attacker inserts himself into the communication channel between the user and the gNB, gaining the ability to view and manipulate the exchanged messages. However, given the encryption and integrity protection of 5G positioning messages, the main capabilities are limited to physical tampering, achieved by retransmitting signals from an alter-

native malicious location, as in the wormhole attack.

3.2.2 Malicious Anchor

Target UE

When the UE acts as the malicious node, potential threats include manipulating positioning measurements and data to target either the network or the entity requesting the localization service. In this context, the UE's role in the localization process determines its attack method. For downlink techniques, it can tamper with the measurements at a logical level. Alternatively, when the final estimation is calculated by the target UE, the malicious UE can directly alter the result. These attacks result in erroneous location estimations by the LMF, either through falsified measurements or deliberate manipulation of the final computation.

Fake gNB

To realize a fake gNB, an attacker may first obtain the identities and broadcast information of legitimate gNBs through passive monitoring of control channels and public network information. Although it is highly unlikely that an attacker could operate an Radio Access Network (RAN) node with the full capabilities of a trusted one, we include such scenarios for completeness. In our security analysis, we consider two logical tampering attacks via a fake gNB. First, in uplink-based positioning methods, where the gNB collects measurements, a malicious gNB can alter these values, effectively complementing tampering carried out by a rogue UE. Second, by falsifying its reported location, a malicious gNB can distort the information provided via the *Transmit/Receive Point (TRP) Information Exchange* procedure in the New Radio Positioning Protocol a (NRPPa) protocol, directly affecting the final position estimation computed by the LMF.

Malicious Located UE

In the SL positioning scenario, a Located UE acts as an anchor node, i.e., its position is known and used to support the location estimation of the target. The Server UE relies on the anchors' location data to complete the positioning procedure and compute its own position. For instance, in the UE-Only operation SL mode, where the network does not participate in the estimation process, the Server UE lacks mechanisms to verify the data received from the Located UE. Consequently, any attacker registered within the PLMN can pose as a Located UE, supplying tampered measurements, delayed signals, or false location data. The impact

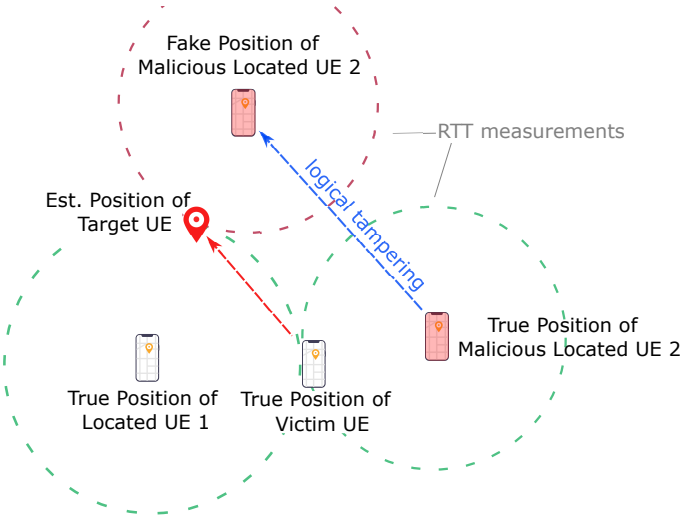

Figure 19: A logical attack by a UE in an RTT-based sidelink positioning procedure. The malicious UE 2 (red) falsifies its position report, leading to an incorrect location estimate for the target UE.

of such an attack is illustrated in Figure 19, where a logical tampering attack, specifically, a falsified position of the Located UE, adversely affects the final location estimation of the target UE.

3.2.3 Insider Threats

While not the primary focus of this chapter, we acknowledge for completeness the potential threats posed by malicious insiders with legitimate access privileges. Network administrators, LMF operators, or other trusted personnel could potentially manipulate positioning data, alter anchor node configurations, or leak location information while bypassing standard security controls. These threats are particularly dangerous as they operate within established trust boundaries and can circumvent protections designed for external attackers. Effective countermeasures against insider threats require cross-entity verification where possible, robust logging with tamper-evident records, and operational security policies including privilege separation and mandatory rotation of duties.

3.3 3GPP Positioning Integrity

Until now, we have analyzed potential threats to the 5G localization system, while now we discuss the 3GPP's efforts in standardizing positioning integrity. The initial standardization of 5G positioning by 3GPP focused on improving accuracy and other key performance indicators, with security receiving less attention [53]. However, starting from Release 17, the concept of positioning integrity was first introduced within the GNSS-based technique and then extended to all 5G methods in Release 18 . The 3GPP defines integrity as the level of trust in the estimated position, evaluated using various indicators to ensure reliability and safety against all possible sources of error, whether intentional or unintentional, during ongoing procedures. The main indicators include the *Alert Limit (AL)* (ϵ_{AL}), which defines the maximum allowable error, and the *Time-to-Alert (TTA)*, which specifies the maximum time that can elapse before reporting a positioning failure. The *Protection Level* represents the upper bound of the true positioning error, while the *Integrity Risk* (I_{r}) is defined as the probability that the error is larger than the AL without triggering an alarm in time, i.e.

$$I_{\mathrm{r}} = \mathbb{P}\{\epsilon > \epsilon_{\mathrm{AL}} \,\&\, \text{undetected}\} \tag{3.1}$$

While the *Target Integrity Risk (TIR)* defines the integrity requirement for a given use case, and the protection level is used to compute the actual integrity risk. This computation determines whether the integrity requirements are met, if they are not, the estimation is rejected as unreliable.

These Key Performance Indicators (KPIs) are fundamental for any positioning system, regardless of the underlying technology, as already demonstrated in GNSS solutions. A well-known approach is the Receiver Autonomous Integrity Monitoring (RAIM) framework, which, in addition to position estimation, computes protection levels and integrity risk to ensure the safe use of the derived localization data. The definition of integrity related KPIs within 3GPP positioning follows the same principle, aiming to achieve comparable levels of reliability and to enable secure and trustworthy operations in safety-critical scenarios. In the next chapter, focusing on a downlink-based use case, we investigate the security aspects of 5G positioning under a spoofing attack and demonstrate how anomaly detection methods can be employed to enhance integrity monitoring and improve the overall integrity risk.

3.4 Summary and Outlook

In this chapter, we conducted an in-depth analysis of the security vulnerabilities affecting 5G positioning systems, focusing on both 3GPP and O-RAN architectures. We explored a range of adversarial attack scenarios specific to these frameworks and demonstrated their potential impact on localization accuracy. Additionally, we examined ongoing advancements in standardization to detect and mitigate these security threats.

In conclusion, this work highlights the urgent need to address security challenges within 5G positioning architectures in order to ensure reliable performance. Building on this foundation, the next chapter focuses on one of the most critical and pervasive threats: spoofing attacks targeting timing-based positioning methods such as downlink/uplink TDOA, and multi-RTT. We will investigate their mechanisms, potential impact, and the design of detection strategies aimed at strengthening the integrity and trustworthiness of location-based services.

Chapter 4

Physical Layer Vulnerabilities and Countermeasures in TOA-Based 5G Positioning

Building on the discussion of threats to 5th Generation (5G) localization services presented in the previous chapter, this chapter opens with a concise review of prior work on timing-based spoofing attacks, highlighting the most relevant contributions and observed vulnerabilities. This related work sets the stage for a deeper investigation into the physical-layer threats, which are particularly critical as higher-level security mechanisms offer limited protection against malicious actors at this level. With this context, we first describe the complete procedure for obtaining position estimates based on timing measurements, establishing the necessary foundation for the analysis of spoofing attacks. We then introduce a mathematical framework for modeling attacks on the Positioning Reference Signal and present two complementary strategies for anomaly detection. The chapter concludes with 3rd Generation Partnership Project (3GPP)-compliant simulations, examining the impact of overshadowing attacks on the localization process under both Line-of-Sight (LOS) and

Non-Line-of-Sight (NLOS) conditions, and evaluating the effectiveness of the proposed detection methods in mitigating integrity risks.

4.1 Related Work

Timing estimation is crucial for multiple 5G positioning methods, such as those based on the estimation of Round Trip Time (RTT) and Time Difference of Arrival (TDOA). In these cases, the Time of Arrival (TOA) of the received signal is estimated by cross-correlating the received signal with the transmitted one, which is known or reconstructed, and by performing a peak search over the resulting correlation function [64]–[69]. Recent studies demonstrate how manipulating the signals during the wireless propagation can introduce additional peaks in the correlation, thus altering the time measurements obtained and consequently resulting in erroneous positioning estimation as shown in previous chapter and in Figure 17. This outcome can lead to potentially fatal results in safety-critical scenarios [12], [14], [15]. Research efforts have been directed toward providing secure positioning services and studying the security aspects of localization based on 5G cellular networks [12], [14]–[16], [70]. In particular, as mentioned in Chapter 3 5G positioning is susceptible to various physical layer threats that can undermine the acquisition of positioning measurements by the target User Equipment (UE) or the gNodeBs (gNBs): jamming, spoofing, and the wormhole attack. In the jamming case, a malicious third party interferes with the communication between the UE and gNBs, disabling the positioning service [71]. Such intentional interference is not strictly related to positioning but is a more general threat for 5G systems as it also disrupts communication services.

In the spoofing case, a malicious third party can transmit fake reference signals to modify the physical properties of the signals transmitted by the UE or the gNB. A well-known example in the literature is Global Positioning System (GPS) spoofing, where an attacker manipulates the GPS signal to alter the estimated position of the target UE as desired [72]. Recent works also demonstrated experimentally how the New Ra-

dio (NR) signals are vulnerable to spoofing attacks [12], [16], [73]. An example implementation of a spoofing attack is the signal overshadowing attack, where the attacker transmits a high-power crafted signal at a specific time-frequency position within the transmission channel [15]. This attack exploits the capture effect [74], where the receiver prioritizes the stronger signal among overlapping ones. As a result, the attacker can alter the messages received by the UE in the downlink (by the gNB in the uplink) by overwriting parts of the legitimate signal from the gNB (from the UE).

In [14], the authors demonstrate the feasibility of spoofing reference signals during the measurement process without disrupting the communication service. An attacker, by sniffing and analyzing the legitimate channel, can infer the configuration of the reference signal (i.e., time-domain and frequency-domain allocation, periodicity, and offset) and subsequently craft specific radio resources dedicated to positioning reference signals. The feasibility of such attacks has also been demonstrated through real-world implementations, in which full-frame meaconing replays are executed using commercial Software-Defined Radios (SDRs) and Field Programmable Gate Arrays (FPGA)-based low-latency processing platforms [31], [32]. In these scenarios, prior knowledge of the Positioning Reference Signal (PRS) configuration is not required, as the attacker retransmits the entire received downlink signal, including both reference signals and user data. Reported replay delays as low as 30μs enable successful execution of the attack without disrupting ongoing communications. These experimental findings validate the practical viability of overshadowing and replay-based spoofing in realistic 5G deployments. Similarly, a wormhole attacker can create a rogue path for the signal [75]. This is achieved by capturing the uplink/downlink signals and replaying them from another position, thereby altering timing or angle measurements.

Preliminary efforts have focused on detecting these threats. In Global Navigation Satellite System (GNSS), Receiver Autonomous Integrity Monitoring (RAIM) ensures positioning integrity and mitigates faulty measurements by leveraging redundancy information to identify and ex-

clude faults, such as through solution separation and statistical tests [76]. This concept extends to 5G systems for computing protection levels and upholding integrity [77]. RAIM not only addresses errors from sources like multipath or NLOS conditions but also detects tampering and spoofing attacks.

The V-Range system proposed in [12] offers a method to secure timing measurements by using shortened Orthogonal Frequency Division Multiplexing (OFDM) symbols, thus increasing temporal resolution. Additionally, the authors propose performing integrity checks at both the physical and data levels, such as inspecting energy variance and comparing received data with expected symbols, to ensure high precision and resilience against overshadowing attacks.

In [14], the authors proposed neural network-based defenses against 5G PRS spoofing attacks. Utilizing hardware features for content-agnostic authentication, these techniques are designed to protect 5G non-encrypted broadcast channels and signals, such as the PRS. Specifically, I/Q features are transformed into I/Q images and then processed by neural networks for pattern recognition. These preliminary promising results highlight the critical importance of addressing location security. However, using shortened symbols might limit the flexibility of the 5G positioning system in terms of signal configuration, and neural networks require dedicated hardware and complex signal processing. Additionally, a general framework for performance assessment in the presence of timing-based attacks is still lacking.

4.2 5G Positioning Model

In this section, we describe all the steps needed for the estimation of localization, from the generation of the Reference Signal (RS) to the estimation of TOA and the formulation of the localization problem.

4.2.1 Reference Signals

The 3GPP defines both the RSs, i.e., the PRS and Sounding Reference Signal (SRS), and the associated reception procedures in [57], [78]. In the downlink localization procedure, the UE takes care of the measuring process and the PRS is used for the ranging operation with the gNBs. The PRS is specifically designed for localization: it is a Gold sequence with high auto-correlation and low cross-correlation properties. These characteristics enhance timing accuracy for position estimation. The PRS sequence and the relative mapping in Resource Elements (REs) (k, l) in the OFDM grid, with k representing the subcarrier and l the OFDM symbol within a slot depends on multiple parameters. Higher-layer protocols provide these parameters, configured by the Location Management Function (LMF) based on the UE and network capabilities (via LTE Positioning Protocol (LPP) capabilities messages [36]). In this way, only the target UE and the gNBs can generate the correct PRS sequence and the REs mapping to obtain the timing measurements. Although this analysis focuses on the downlink PRS procedure, the same principles apply to uplink positioning, where the UE transmits the SRS for timing measurements at the gNB. The SRS sequence is also defined by pseudo-random sequences and follows similar resource element mapping rules, mirroring the procedure used for the PRS.

4.2.2 TOA Estimation

Considering the downlink procedure, the PRS transmitted by the i-th gNB, with $i = 1, \cdots, N_{\text{gNB}}$ is modulated using the OFDM as follows:

$$s_i(t) = \sum_{k=0}^{N-1} S_i^{(k,l)} \cdot e^{j2\pi \frac{kt}{T}}, \quad 0 \leq t < Ti = 1, \cdots, N_{\text{gNB}} \tag{4.1}$$

where N is the total number of subcarriers and T is the symbol time, where $S_i^{(k,l)}$ is defined as

$$S_i^{(k,l)} = \begin{cases} a_i^{(k,l)} & l \in \mathcal{L}_{\text{PRS}} \\ X_i^{(k,l)} & l \in \mathcal{L}_{\text{DATA}} \end{cases} \text{for } i = 1, \cdots, N_{\text{gNB}} \tag{4.2}$$

where $a_i^{(k,l)}$ is the PRS symbol while $X_i^{(k,l)}$ is the data symbol. These symbols are non-zero only when $l \in \mathcal{L}_{\text{PRS}}$ or $l \in \mathcal{L}_{\text{DATA}}$.

In downlink-based positioning, the UE receives the combined PRSs transmitted by all the gNBs participating in the procedure. The received signal can thus be expressed as:

$$r(t) = \sum_{i=1}^{N_{\text{gNB}}} r_i(t) + w(t) \tag{4.3}$$

where $w(t)$ is the receiver noise modeled as additive white Gaussian process with variance σ_w^2; $r_i(t)$ is the signal component related to the i-th transmitting gNB. We focus in the following derivations on a single signal component. Considering a multipath scenario (see, e.g., the 3GPP link-level channel model in [59]), the i-th signal component can be expressed as

$$r_i(t) = \sum_{n=1}^{N_{\text{p}}} \alpha_n s_i(t - \tau_n) \tag{4.4}$$

where τ_n and α_n are the delay and complex amplitude of the n-th multipath component, respectively, with $n = 1, 2, \ldots, N_{\text{p}}$. The receiver processes the incoming signal to estimate the TOA of each PRS. To this scope, a reference sequence of PRS for each gNB and the corresponding modulated signal $\tilde{s}_i(t)$ is generated locally as:

$$\tilde{s}_i(t) = \sum_{k=0}^{N-1} a_i^{(k,l)} \cdot e^{j2\pi \frac{kt}{T}}, \quad 0 \leq t < T \tag{4.5}$$

Then, the UE computes the discrete cross-correlation between the locally generated PRS and the received signal over an observation window of duration MT_{sym}. Let $r[n] = r(nT_s)$ denote the sampled version of the

received signal $r(t)$ with sampling time T_s. The cross-correlation is

$$\begin{aligned} R_i[n] &= \sum_{m=0}^{MN_{\text{sym}}} r[m]\tilde{s}_i^*[m-n] \\ &= \sum_{j=0}^{N_{gNB}} \sum_{n=0}^{N_{\text{p}}} \alpha_{nj} \sum_{m=0}^{MN_{\text{sym}}} s_j[m - \lfloor \tau_{nj}/T_{\text{s}} \rfloor]\tilde{s}_i^*[m-n] \\ &\quad + \sum_{m=0}^{MN_{\text{sym}}} w[m]\tilde{s}_i^*[m-n]\,. \end{aligned} \tag{4.6}$$

As the PRS sequences used by different gNBs are orthogonal, the cross-correlations between $s_j[m]$ and $\tilde{s}_i^*[m]$ are null for $j \neq i$. Therefore, we can rewrite

$$R_i[n] = \sum_{n=0}^{N_{\text{p}}} \alpha_n \mathring{R}_i[n - \lfloor \tau_n/T_{\text{s}} \rfloor] + z[n]\,. \tag{4.7}$$

where $N_{\text{sym}} = \lfloor T_{\text{sym}}/T_{\text{s}} \rfloor$ and $\mathring{R}_i[n] = \sum_{m=0}^{MN_{\text{sym}}} s_i[m]\tilde{s}_i^*[m-n]$, which corresponds to the discrete autocorrelation function when $\tilde{s}_i[m] = s_i[m]\ \forall n$ (i.e., when the local copy of the transmitted signal is the same as the true transmitted one); $z[n]$ is the noise component after correlation. This operation is performed by the UE for each PRS received from the N_{gNB} gNBs involved in the positioning procedure. Once the cross-correlation is computed, the TOA can be estimated in multiple ways [69]. The most common procedures are the following: *i) Max*: the TOA is defined as the time delay corresponding to the highest peak; *ii) P-Max*: the TOA is selected from the first peaks among P largest in the correlation; *iii) Simple Thresholding*: the TOA is estimated by selecting the first peak that exceeds a pre-computed threshold. Without loss of generality, in the rest of the Chapter we focus on the first solution for TOA estimation, i.e.

$$\hat{m} = \arg\max_m R_i[m] \tag{4.8}$$

and $\hat{\tau}_i = \hat{m}T_{\text{s}}$.

4.2.3 Localization Problem

Once the TOA estimation is complete, TDOA or RTT are computed, eliminating any dependence on synchronization between the gNBs and the UE. In TDOA methods, each TDOA measurement is the difference between two TOAs. Using the j-th gNB as reference node, the i-th TDOAs is computed as

$$t_{ji} = \hat{\tau}_j - \hat{\tau}_i \quad \text{for } i = 1, \cdots, N_{\text{gNB}} \setminus \{j\} \tag{4.9}$$

The resulting system of $N_{\text{gNB}} - 1$ equations is used to estimate the user position $\hat{\mathbf{p}}_{\text{UE}} = [\hat{x}_{\text{UE}}, \hat{y}_{\text{UE}}]$, with the i-th equation defined below

$$\begin{aligned} &\sqrt{(x_j - x_{\text{UE}})^2 + (y_j - y_{\text{UE}})^2} \\ &- \sqrt{(x_i - x_{\text{UE}})^2 + (y_i - y_{\text{UE}})^2} = ct_{ji} \end{aligned} \tag{4.10}$$

where c is the speed of light.

On the other hand, using the multiple Round Trip Time (multi-RTT) method, the localization measurements are computed as the sum of the two DL and UL TOAs, plus the RS processing time, i.e., τ_{proc}. For the i-th gNB, the RTT is computed as

$$t_{\text{RTT},i} = \hat{\tau}_{\text{DL},i} + \hat{\tau}_{\text{UL},i} + \tau_{\text{proc}} \quad \text{for } i = 1, \cdots, N_{\text{gNB}} \tag{4.11}$$

These measurements result in a system of N_{gNB} equations. The i-th equation is defined as

$$\sqrt{(x_i - x_{\text{UE}})^2 + (y_i - y_{\text{UE}})^2} = c\frac{t_{\text{RTT},i}}{2} \tag{4.12}$$

The estimated position of the target UE $\hat{\mathbf{p}}_{\text{UE}} = [\hat{x}_{\text{UE}}, \hat{y}_{\text{UE}}]$ is obtained by resolving the non-linear problem in (4.10) or (4.12).

4.3 Timing-based Threats to 5G Positioning

In this section, we consider two examples of spoofing attacks, perpetrated by a malicious third-party actor in the downlink Localization Service (LCS) process. Figure 20 illustrates the case where the attacker tampers with the PRS from a single gNB. The extension to the uplink case is straightforward.

The two spoofing attacks we present are:

- *Replay attack mode*: the attacker performs an overshadowing attack on the entire downlink signal (data and PRS), i.e., it intercepts and replays a delayed copy of the downlink signal with a higher power to hide the legitimate signal.
- *Forged PRS mode*: the attacker manipulates only the PRS, keeping data symbols unaltered. This enables disruption of the positioning system while preserving the integrity of data communication between the victim UE and the gNB, ensuring stealthiness throughout the communication.

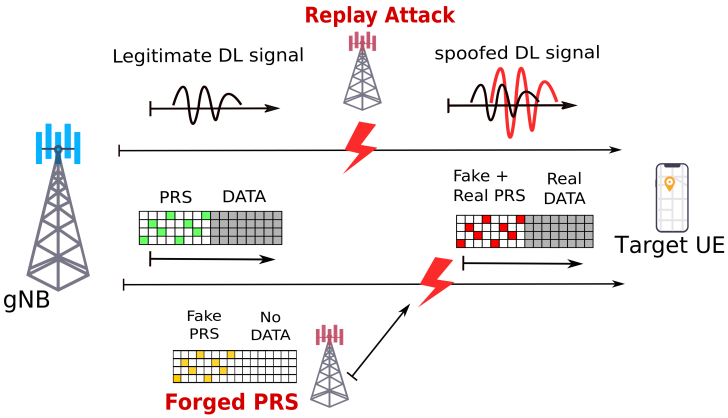

Figure 20: Two examples of spoofing attacks on the downlink signals: top) the replay attack mode, where both PRS and data signals are overshadowed. bottom) the forged PRS spoofing mode, where only the PRS is manipulated.

The feasibility and impact of these physical-layer spoofing attacks critically depend on the relative geometry between the attacker, the legitimate transmitter and receiver, as well as the directionality of the communication links, particularly in systems employing beamforming such as 5G NR. In practical localization scenarios, the gNB cannot steer highly directional beams toward the UE prior to determining its position. Therefore, initial positioning procedures typically rely on wide or exploratory

beams, making it feasible for a strategically placed adversary to intercept and replay the relevant signals. While the feasibility of replay attacks is constrained under tightly focused beamforming, such configurations are generally applied only after initial positioning is completed, at which point the UE's location is already known and spoofing is less impactful.

4.3.1 Overshadowing - Replay Attack

The attacker can exploit the overshadowing - replay attack to tamper the TOA measurements by only re-transmitting the legitimate signals delayed and amplified, including both PRS and data [12]. The attacker's received signal, $u_i(t)$, is the signal originally transmitted by the i-th legitimate gNB.[1] Such a signal is retransmitted as $s_{\mathrm{A}}(t)$ after being delayed by δ and amplified by a factor G_{A}, where

$$s_{\mathrm{A}}(t) = \begin{cases} 0 & \text{if } t < \delta \\ G_{\mathrm{A}} u_i(t-\delta) & \text{if } t \geq \delta \end{cases} \tag{4.13}$$

Here,

$$u_i(t-\delta) = \sum_{h=1}^{H_{\mathrm{p}}} \beta_h s_i(t-\delta-\psi_h) + w_{\mathrm{A}}(t) \tag{4.14}$$

where ψ_h and β_h account for the multipath effects between the legitimate gNB and the attacker. The total signal received by the target UE is the result of the superposition between the legitimate signals, $r_{\text{leg}}(t) = \sum_{i=1}^{N_{\text{gNB}}} r_i(t)$ and the malicious one

$$r(t) = r_{\mathrm{A}}(t) + r_{\text{leg}}(t) + w(t) \tag{4.15}$$

Considering the multipath propagation effect

$$r_{\mathrm{A}}(t) = \sum_{q=1}^{Q_{\mathrm{p}}} \gamma_q G_A \sum_{h=1}^{H_{\mathrm{p}}} \beta_h s_i(t-\delta-\theta_q-\psi_h) + w_{\mathrm{A}}(t) \tag{4.16}$$

[1] Here we assume the attacker is able to distinguish the signal from a single gNB, e.g., by means of a directive antenna.

where γ_q and θ_q represent the amplitude and delay of the q-th multipath component between the attacker and the victim UE and w_{A} is the Gaussian noise. After a rearrangement of amplitudes and delays, such that $\zeta_l = \gamma_q \beta_m$ and $\vartheta_l = \theta_q + \psi_m$ the malicious component can be rewritten as

$$r_{\mathrm{A}}(t) = G_{\mathrm{A}} \sum_{l=1}^{L_{\mathrm{p}}} \zeta_l s_i(t - \delta - \vartheta_l) + w_{\mathrm{A}}(t) \tag{4.17}$$

The resulting cross-correlation includes an additional term introduced by the attack

$$\begin{aligned} R_i[n] = & \sum_{m=0}^{MN_{\mathrm{sym}}} r_{\mathrm{leg}}[m] \tilde{s}_i^*[m-n] \\ & + \sum_{m=0}^{MN_{\mathrm{sym}}} r_{\mathrm{A}}[m] \tilde{s}_i^*[m-n] + z[n] \end{aligned} \tag{4.18}$$

where the first term represents the discrete cross-correlation of the legitimate signal, and the second term corresponds to the attacker's contribution. From eq. (4.17), the cross-correlation due to the attacker's signal can be expressed as

$$\begin{aligned} & \sum_{m=0}^{MN_{\mathrm{sym}}} r_{\mathrm{A}}[n] \tilde{s}_i^*[m-n] = \\ & \quad = G_{\mathrm{A}} \sum_{l=1}^{L_{\mathrm{p}}} \zeta_l \sum_{m=0}^{MN_{\mathrm{sym}}} s_i[m - \lfloor \delta / T_{\mathrm{s}} \rfloor - \lfloor \vartheta_l / T_{\mathrm{s}} \rfloor] \tilde{s}_i^*[m-n] \\ & \quad + \sum_{m=0}^{MN_{\mathrm{sym}}} w_{\mathrm{A}}[m] \tilde{s}_i^*[m-n] \end{aligned} \tag{4.19}$$

Considering the noise term as negligible, which is a particularly realistic assumption as an attacker would use a directive antenna to ensure high

Signal-to-Noise Ratio (SNR), we can approximate (4.18) as

$$R_i[n] = \sum_{n=1}^{N_\mathrm{p}} \alpha_n \mathring{R}_i[n - \lfloor \tau_n / T_\mathrm{s} \rfloor] + G_\mathrm{A} \sum_{l=1}^{L_\mathrm{p}} \zeta_l \mathring{R}_i[n - \lfloor \delta / T_\mathrm{s} \rfloor - \lfloor \vartheta_l / T_\mathrm{s} \rfloor] + z[n] \tag{4.20}$$

This expression accounts for the multipath effects between the gNB and UE, the gNB and the attacker, as well as the attacker and UE, along with the amplification and delay introduced by the attacker. Thus, the peak of the cross-correlation depends on all these multipath parameters. Considering, the case of LOS scenario, where the first path of the multipath (τ_1, α_1) of the legitimate channel is the strongest and resolvable, and assuming $\mathring{R}_i[0]$=$\max_n \mathring{R}_i[n]$, the peak of the cross-correlation is

$$\max R_i[n] = \max\{\alpha_1 \mathring{R}_i[0], G_\mathrm{A} \zeta_1 \mathring{R}_i[0]\} \tag{4.21}$$

Consequentially, the TOA τ_i is estimated erroneously when

$$G_\mathrm{A} \zeta_1 = G_\mathrm{A} \gamma_1 \beta_1 > \alpha_1 \tag{4.22}$$

and the TOA error is equal to $|\delta + \vartheta_1 - \tau_1|$. When (4.22) is not satisfied, the legitimate signal prevails on the malicious one, and the TOA is correctly estimated. Note that (4.22) is a necessary but not sufficient condition for an attack to be successful. Indeed, the delay δ introduced in the retransmission might be bounded depending on the specific implementation, see, e.g., [12].

4.3.2 Selective Spoofing - Forged PRS

In the selective spoofing attack, the malicious entity needs to acquire critical information to execute the attack successfully, i.e., to craft the malicious PRS to be spoofed. Specifically, the attacker must know all the higher-layer parameters related to the PRS configurations, which are necessary for the correct generation, mapping, and scrambling of the PRS sequence into the REs as defined in [57]. Additionally, the attacker needs

to obtain timing information from the gNB to prepare the injection of the PRS at the subframe and symbol level [14]. Within this assumption, the attacker is able to generate the malicious PRS introducing an arbitrary delay δ and gain G_{A}.

$$s_{\mathrm{A}}(t) = G_{\mathrm{A}}\tilde{s}_i(t-\delta) \tag{4.23}$$

The UE receives a combined signal that includes all transmissions, including the malicious one, as shown in (4.15). Following the same procedures outlined in Section 4.3.1, the correlation peak of the maliciously forged PRS will be identified as the TOA measurement. As for the previous case, the attack is successful (i.e., the TOA measurement is tampered) when (4.22) is satisfied.

4.4 Attack Detection Methods

In this Section, we formalize the hypothesis testing for attack detection, highlighting channel statistics-based methods' limitations; then we present two potential approaches. As a first approach, the information contained in the correlation of the signal with the known PRS sequence (time of arrival or maximum amplitude) is used without prior knowledge or Machine Learning (ML). The second approach employs the Gaussian Mixture Model (GMM) to leverage the TOA-maximum amplitude relationship. Figure 21 provides an overview of the proposed system model and threat detection framework.

4.4.1 Hypothesis Testing for Attack Detection

The detection of an attack can be obtained by analyzing the signal received at the victim UE. A binary hypothesis test can be defined with the following definition:

- $\mathcal{H}_0$: no attack is present. The received signal at the UE depends on the legitimate signal from the gNB and the receiver noise:

$$r(t) = r_{\mathrm{leg}}(t) + w(t) \tag{4.24}$$

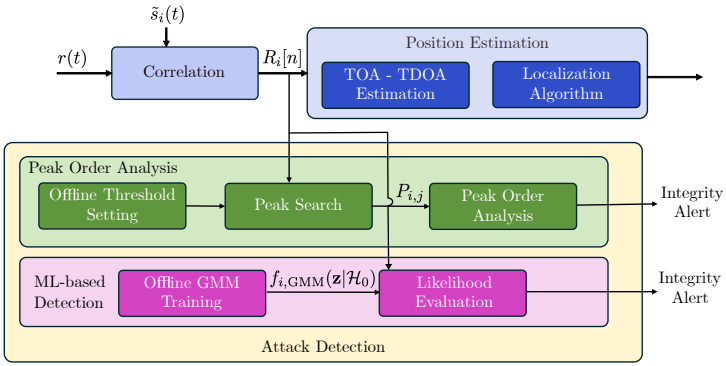

Figure 21: High-level overview of the 5G positioning system under spoofing threats. The diagram illustrates the main stages of the localization procedure (transmission of reference signals, correlation, TOA estimation, and position computation) and the integration of the proposed detection methods.

where $r_{\text{leg}}(t)$ is the legitimate signal received from the gNB and propagating through the channel, including multipath effects.

- $\mathcal{H}_1$: an overshadowing attack is present. The received signal includes both the legitimate signal and the spoofed signal introduced by an attacker:

$$r(t) = r_{\text{leg}}(t) + r_{\text{A}}(t) + w(t) \tag{4.25}$$

where $r_{\text{A}}(t)$ is the spoofed signal introduced by the attacker after receiving the legitimate one, incorporating multipath effects between the gNB and the attacker, as well as between the attacker and the UE.

Both the null hypothesis ($\mathcal{H}_0$) and the alternative hypothesis ($\mathcal{H}_1$) involve multiple channel parameters, which are generally unknown and difficult to model accurately in practical scenarios. If the channel statistics are considered as deterministic and unknown, we can define $\boldsymbol{\Theta}_0$ and $\boldsymbol{\Theta}_1$ as

the vectors of channel parameters, i.e.

$$\begin{aligned}\boldsymbol{\Theta}_0 &= \left[\tau_1, \alpha_1, \tau_2, \alpha_2, \ldots, \tau_{N_\mathrm{p}}, \alpha_{N_\mathrm{p}}, \sigma_\mathrm{w}\right] \\ \boldsymbol{\Theta}_1 &= \left[\boldsymbol{\Theta}_0, G_\mathrm{A}, \delta, \vartheta_1, \zeta_1, \vartheta_2, \zeta_2, \ldots, \vartheta_{N_\mathrm{p}}, \zeta_{N_\mathrm{p}}\right]\end{aligned} \tag{4.26}$$

As the two hypotheses are nested and depend on multiple unknown parameters, we can define the Generalized Likelihood Ratio Test (GLRT) as:

$$\Lambda(r(t)) = \frac{\max_{\boldsymbol{\Theta}_1} \; p(r(t) \,|\, \mathcal{H}_1, \boldsymbol{\Theta}_1)}{\max_{\boldsymbol{\Theta}_0} \; p(r(t) \,|\, \mathcal{H}_0, \boldsymbol{\Theta}_0)} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \xi \tag{4.27}$$

where $\Lambda(r(t))$ is the test statistic; $p(r(t) \,|\, \mathcal{H}_0, \boldsymbol{\Theta}_0)$ is the likelihood of observing $r(t)$ under $\mathcal{H}_0$; $p(r(t) \,|\, \mathcal{H}_1, \boldsymbol{\Theta}_1)$ is the likelihood of observing $r(t)$ under $\mathcal{H}_1$; and ξ is the decision threshold, determined by the desired false alarm rate. Considering the vector of received signal samples $\mathbf{r}$, the likelihood function under $\mathcal{H}_0$ results in

$$\begin{aligned}\ln p(\mathbf{r} \,|\, \mathcal{H}_0, \boldsymbol{\Theta}_0) \propto \Bigg(& -\frac{2}{\sigma_\mathrm{w}^2} \sum_{n=1}^{N_\mathrm{p}} \alpha_n R_i[\lfloor \tau_p / T_\mathrm{s} \rfloor] \\ & + \frac{1}{\sigma_\mathrm{w}^2} \sum_{n=1}^{N_\mathrm{p}} \alpha_n^2 \mathring{R}_i^2[0] \\ & + \frac{2}{\sigma_\mathrm{w}^2} \sum_{n<q} \alpha_n \alpha_q \mathring{R}_i^2[\lfloor (\tau_n - \tau_q)/T_\mathrm{s} \rfloor] \Bigg)\end{aligned} \tag{4.28}$$

Under $\mathcal{H}_1$, the likelihood function is

$$\begin{aligned}p(\mathbf{r} \,|\, \mathcal{H}_1, \boldsymbol{\Theta}_1) \propto \Bigg(& -\frac{2}{\sigma_\mathrm{w}^2} \sum_{n=1}^{N_\mathrm{p}} \alpha_n R_i[\lfloor \tau_n / T_\mathrm{s} \rfloor] + \frac{1}{\sigma_\mathrm{w}^2} \sum_{n=1}^{N_\mathrm{p}} \alpha_n^2 \mathring{R}_i^2[0] \\ & + \frac{2}{\sigma_\mathrm{w}^2} \sum_{n<q} \alpha_n \alpha_q \mathring{R}_i^2[\lfloor (\tau_n - \tau_q)/T_\mathrm{s} \rfloor] \\ & - \frac{2G_\mathrm{A}}{\sigma_\mathrm{w}^2} \sum_{l=1}^{L_\mathrm{p}} \zeta_l R_i[\lfloor (\delta + \vartheta_l)/T_\mathrm{s} \rfloor] + \frac{G_\mathrm{A}}{\sigma_\mathrm{w}^2} \sum_{l=1}^{L_\mathrm{p}} \zeta_l^2 \mathring{R}_i^2[0] \\ & + \frac{2G_\mathrm{A}^2}{\sigma_\mathrm{w}^2} \sum_{l<q} \zeta_l \zeta_q \mathring{R}_i^2[\lfloor (\tau_l - \tau_q)/T_\mathrm{s} \rfloor] \Bigg)\end{aligned} \tag{4.29}$$

Computational Limitations To solve the GLRT in (4.27) using (4.28) and (4.29), we need to maximize the likelihood for each hypothesized amplitude and time delay, corresponding to potential signal paths under the two hypotheses, i.e. finding the maximum likelihood estimate for $\boldsymbol{\Theta}_0$ and $\boldsymbol{\Theta}_1$ [66]. This process is non-tractable in general and can be computationally expensive unless prior knowledge about the channel is utilized. Traditional methods for deriving Constant False Alarm Rate (CFAR) thresholds often assume prior knowledge of channel statistics under $\mathcal{H}_0$ or use predefined distributions (e.g., log-normal), but these approaches fail to capture the intricate, real-world multipath and NLOS conditions encountered in 5G [79]–[81]. This makes deriving CFAR thresholds for hypothesis testing even more challenging, as multipath variability and dynamic channel effects complicate the modeling of signal statistics. For what concerns $\mathcal{H}_1$, together with the channel statistics also the attacker delay and gain should be known, i.e., δ and G_{A}, which is a highly unrealistic assumption. A possible solution is to learn channel statistics under $\mathcal{H}_0$, i.e. using semi-supervised methods. In this case, the test statistic is typically the likelihood of the observed data under $\mathcal{H}_0$

$$\tilde{\Lambda}(r(t)) = \hat{p}(r(t) \,|\, \mathcal{H}_0) \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} \xi \tag{4.30}$$

where $\hat{p}(r(t) \,|\, \mathcal{H}_0)$ is the distribution function learned through a ML algorithm, e.g. using autoencoders or density estimation approaches [82], [83]. However, even this solution is impractical in 5G scenario, as this approach would require the collection of large databases of received signal samples, which are costly to build and prone to inaccuracies due to the dynamic and unpredictable nature of real channels. Furthermore, for many positioning methods, only the output of the correlator or the likelihood function is accessible, which limits the granularity of statistical analysis. To address these limitations, in the following sections, we propose two sub-optimal detection approaches:

1. **Peak Order Analysis without Machine Learning:** This approach analyzes the output of the correlator to detect anomalies by examining the order and magnitude of correlation peaks. While simple

and computationally efficient, this method is expected to perform reliably only in LOS conditions between the UE and the gNB. In NLOS conditions, it may lead to a higher rate of false alarms due to the influence of multipath reflections, but it still serves as an indicator of potential errors.

2. **Semi-supervised Anomaly Detection:** This method leverages the correlator's output to construct test statistics and applies machine learning techniques, such as GMM, to identify patterns and anomalies in the signal. By focusing on the correlator's output rather than the entire waveform, this approach reduces complexity and latency, while adapting to dynamic multipath conditions without relying on rigid statistical assumptions about the channel. Indeed, deep learning methods could serve as an alternative to the GMM model for density estimation, as neural network-based approaches have the potential to capture more complex patterns in the data. This could provide a robust solution for physical layer attack detection, offering a different perspective to the GMM model. We selected the GMM approach in this work because it is easily explainable, allowing for greater interpretability of the results compared to more complex deep learning models.

4.4.2 Peak Order Analysis

When the i-th gNB is under attack, the correlation function at the receiver $R_i[n]$ presents multiple peaks: those due to the multipath propagation of the legitimate signal and those due to the multipath propagation of the attacker's signal. If the gNB is in LOS with the UE, the strongest peak is also the first one and corresponds to the direct path between the gNB and the UE. By definition of the overshadow, the first path of the attacker's signal is delayed compared to the legitimate one, i.e. $\tau_1 < \theta_1$. Therefore, in LOS conditions, if the strongest peak is not the first peak in time, then an attack can be detected. We define, for the i-th gNB, the two strongest correlation peaks as $P_{i,1} = R_i[m_1]$ and $P_{i,2} = R_i[m_2]$, with the assumption of $P_{i,1} > P_{i,2}$. In this way, we use $m_1 - m_2$ as test

statistic. In particular, when $m_1 \leq m_2$, we infer that $P_{i,1}$ corresponds to the legitimate signal of the i-th gNB, leading to the correct estimation of the TOA, whereas when $m_1 > m_2$, an attack is detected. Identifying the attack can trigger an alert, thus reducing the integrity risk. Nevertheless, such a preliminary detection strategy is expected to be ineffective if the gNB is in NLOS with the user. Indeed, in this case, the first path might not be the strongest one as the direct path is blocked. This would lead to a higher false positive rate and a lower probability of detection of the attack.

Alternatively, the maximum peak amplitude of the correlation can be compared with a specific threshold previously selected. Indeed, there is the assumption that a data set obtained in a safe scenario is available in order to compute the optimal threshold by analyzing the distribution of the amplitude of the correlation. Since the attacker amplifies the overshadowing signal, detection occurs if the gain of the received signal exceeds the threshold. The selection of the threshold is fundamental to achieving the desired balance between detection and false positives of the method. From the signals coming from the i-th gNB, we obtain N_{train} PRS measurements and corresponding correlations $\{R_{i,j}[m]]\}_{j=1}^{N_{\text{train}}}$ with peak amplitude

$$P_{i,j} = \max_m R_{i,j}[m] \tag{4.31}$$

with $j = 1, \cdots, N_{\text{train}}$. Then a distribution analysis of these peaks is performed to select the threshold as

$$\xi_i = Q_p\{\mathcal{P}_{i,\text{train}}\} \tag{4.32}$$

where $\mathcal{P}_{i,\text{train}} = \{P_{i,j}\}_{j=1}^{N_{\text{train}}}$ is the dataset containing the N_{train} larger peak amplitudes and the operator $Q_p\{\mathcal{D}\}$ denotes the p-th percentile for the elements of the dataset $\mathcal{D}$. Once the training is complete and the threshold ξ_i is computed, it is possible to detect the anomalies on the TOA measurements obtained for the i-th gNB. Indeed, for each new PRS measurement, the method returns the under-attack status if the peak amplitude of the cross-correlation overcomes the threshold: $\tilde{P}_i \geq \xi_i$.

4.4.3 GMM-based Time-Amplitude Analysis

Building upon the hypothesis testing framework, we now introduce a complementary approach for detecting attacks using GMMs. Unlike the hypothesis test, which focuses solely on signal characteristics, the GMM-based method leverages both time and amplitude data from cross-correlation functions to detect spoofing. GMMs are probabilistic models that assume data points are generated from a mixture of a finite number K of Gaussian distributions, each with unknown parameters. They are well-suited for spoofing detection due to their capability to model complex distributions with multiple subpopulations, enabling precise anomaly detection without requiring labeled training data.

Previous studies have shown the effectiveness of GMMs [84] as countermeasures against spoofing in GNSS [85]–[88]. Our approach introduces a novel method that seamlessly integrates with the 3GPP positioning procedure, eliminating the need for additional signal processing. The key concept is to leverage the inherent relationship between time estimates and their corresponding peak amplitudes derived from the cross-correlation function, which are standard metrics for estimating TOA and TDOA in 5G. Specifically, the method models the distribution of correlation peaks in PRS measurements to identify deviations in the TOA-peak amplitude relationship, which indicates the presence of spoofing attacks.

Our goal is to determine if the received PRSs have been tampered with by identifying anomalies from the modeled legitimate TOA-peak amplitude channel-related relationship. The proposed method is articulated in the following two phases.

Training Phase

During the training phase, PRS measurements are collected in a secure environment, i.e. in a default condition without any attacks. This dataset is used to train the GMM, modeling the normal behavior of the PRSs. For the i-th gNB, the steps involved are the following: (i) Collect a large set PRS measurement correlations $\{R_{i,j}[m]\}_{j=1}^{N_{\text{train}}}$ with corresponding pairs

of TOA and peak amplitudes

$$\mathbf{z}_{i,j} = [\tau_{i,j}, P_{i,j}] \tag{4.33}$$

(ii) Train the GMM with K components on this dataset to estimate the parameters of the model using the Expectation-Maximization (EM) algorithm. The GMM is represented as a weighted sum of the K Gaussian components:

$$f_{i,\text{GMM}}(\mathbf{z}|\mathcal{H}_0) = \sum_{k=1}^{K} p(\mathbf{c}_k)\,\mathcal{N}(\mathbf{z}|\boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k, \mathcal{H}_0) \tag{4.34}$$

where $\mathcal{N}(\mathbf{z}|\boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k, \mathcal{H}_0))$ is the probability density function of the k-th Gaussian component and $p(\mathbf{c}_k)$ are the mixture weights. Specifically, $p(\mathbf{c}_k)$, $\boldsymbol{\mu}_k$, and $\boldsymbol{\Sigma}_k$ are estimated by maximizing the joint log-likelihood function for the training dataset, e.g. by using the EM algorithm [89].

Detection Phase

The detection phase starts for each new PRS measurement. For each signal measurement at the i-th gNB, $\tilde{\mathbf{z}}_i = [\tau_i, P_i]$, the likelihood $\tilde{\Lambda}_i(\tilde{\mathbf{z}}_i)$ is compared to a threshold ξ_i in order to detect anomalies caused by spoofing attacks on the i-th gNB.

$$\tilde{\Lambda}_i(\tilde{\mathbf{z}}_i|\mathcal{H}_0) = f_{i,\text{GMM}}(\tilde{\mathbf{z}}_i|\mathcal{H}_0) \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} \xi \tag{4.35}$$

As for Section 4.4.1, the threshold ξ_i is set to achieve the desired balance between detection probability and false alarm rate. As an example, we consider the dataset of likelihood values from each measurement of the training dataset, i.e. $\mathcal{L}_{i,\text{train}} = \{\Lambda(\mathbf{z}_{i,j})\}_{j=1}^{N_{\text{train}}}$. The threshold ξ_i is set as

$$\xi_i = Q_p\{\mathcal{L}_{i,\text{train}}\} \tag{4.36}$$

where p represents a specific percentile.

4.5 Case Study

This section presents the case study used to evaluate the performance of a 5G positioning system in the presence of spoofing attacks. In particular, we assess the positioning accuracy varying the attack extent. Then, we evaluate the effectiveness of the proposed detection methods presented in Sec. 4.4 in reducing the integrity risk of the positioning system when it is under attack.

4.5.1 Simulation Settings

The simulations have been carried out in MATLAB by configuring a standard scenario, a standard multipath fading channel model, and varying the attack configuration.

Scenario Configuration

The selected scenario is an indoor environment that includes the deployment of 12 gNBs with an inter-site distance equal to 20 m within a total area of 120 m by 50 m, according to the 3GPP specification [59]. The position of the target UE is drawn randomly within the area according to a uniform distribution. The position of target UE is estimated by leveraging downlink PRSs transmitted by the multiple gNBs. The TDOA positioning method is employed and the position estimation is computed with a grid-based non-linear least square algorithm to solve the system of equations in (4.10). The chosen resolution for this simulation is 0.5 m for both the x and the y axes. While the positioning algorithm in this simulation treats all measurements equally and does not exclude unreliable ones, the presence of more gNBs than strictly required could improve positioning accuracy by incorporating consistency checks, such as RAIM, adapted to 5G positioning [90]–[94]. This could filter out unreliable measurements based on geometric constraints and also help counteract the spoofing attack. Additionally, methods like Kalman filtering or multi-hypothesis tracking could further improve measurement consistency and robustness. However, our primary focus in this Chapter is

on detecting spoofing attacks at the single-link level, using the existing measurements for anomaly detection, rather than developing positioning countermeasures.

Channel Configuration

The carrier frequency is set to $3.4\,\text{GHz}$ with a bandwidth of $100\,\text{MHz}$. The chosen bandwidth is selected to ensure high-precision positioning results, as a wider bandwidth allows for better time resolution and more accurate distance measurements, which is crucial for achieving precise positioning in 5G systems [95]. The Subcarrier Spacing (SCS) is $60\,\text{kHz}$, giving a symbol time (T_{sym}) equal to $16.67\,\mu s$. The correlation window observation is $4T_{\text{sym}}$, i.e. set $M = 4$. The channel has been modeled considering the path loss, the Additive White Gaussian Noise (AWGN), and the multipath propagation, as described in (4.4). The multipath has been simulated with the Tapped Delay Line (TDL) models defined in [59]. In the simulation, we consider both the LOS and NLOS conditions for the 12 gNBs with the Delay Spread (DS) set to $30\,\text{ns}$, i.e., short delay spread, to ensure a more realistic evaluation and to account for scenarios in which LOS conditions cannot be assumed. Specifically, in LOS scenario, all the gNBs use the TDL-E channel profile. For the NLOS case scenario, each gNB has a 50% chance of being in NLOS, with the TDL-A channel profile for the reference gNB, and the TDL-B/C for all the other gNBs. In the remaining 50% of cases, the gNB is in LOS with the TDL-E configuration. We used multiple TDL models and also introduced randomness to the channel taps by adding a uniformly distributed random component to the delay spread. Specifically, this random component follows a uniform distribution $\mathcal{U}(0, 1\,\text{ns})$, applied to a base delay spread of $30\,\text{ns}$. This adjustment introduces variability in the delay spread, enhancing the diversity of channel conditions to better reflect real-world propagation scenarios.

Attacker Configuration

In the simulation, we consider only one gNB under attack, even if the attack scenario could be extended to multiple gNBs. For each iteration, the attacker is randomly located between the gNB under attack and the target UE, as shown in Figure 22. In addition, the attacker is strategically

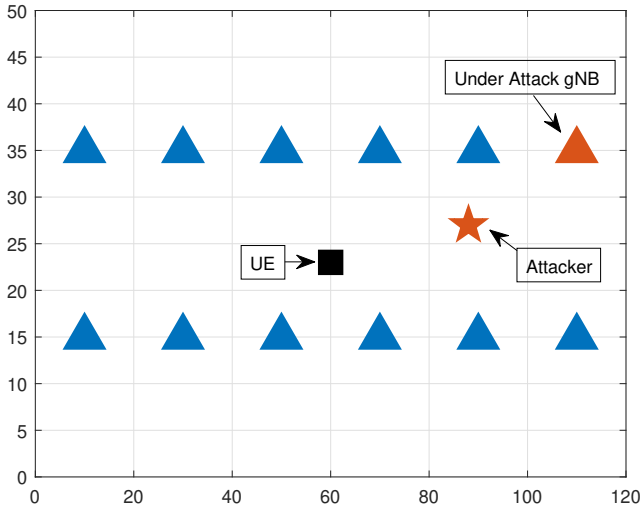

Figure 22: Attack scenario. The blue triangles indicate the locations of the involved gNBs. The attacker (orange star) is always located between the gNB under attack (orange triangle) and the UE (black square).

positioned in LOS conditions and configured with the TDL-D channel profile. This setup represents the worst-case scenario from the perspective of the target UE since a spoofer in NLOS conditions would have a significantly reduced impact. This is because, in NLOS scenarios, the spoofer's signal is weaker and more distorted, making it less likely to overshadow the legitimate LOS signal or significantly affect positioning accuracy. The attacker performs a replay-type overshadowing by delaying the received legitimate signal. The introduced delay δ and the gain G_{A} define the extent of the attack according to 4.3.1. In the sim-

ulation, we vary δ and G_{A}, considering $\delta = \{0.01\,T_{\mathrm{sym}}, 0.02\,T_{\mathrm{sym}}\}$, and $G_{\mathrm{A}} = \{50, 60, 70\}$ dB. G_{A} has been chosen to compensate for the path loss experienced along the distance between the gNB and the attacker.

4.5.2 Performance Evaluation

Figure 23 and Figure 24 show the Empirical Complementary Cumulative Distribution Function (ECCDF) of positioning errors under different overshadowing attack configurations for LOS and NLOS conditions, respectively. In both cases, as the attacker's gain increases, positioning

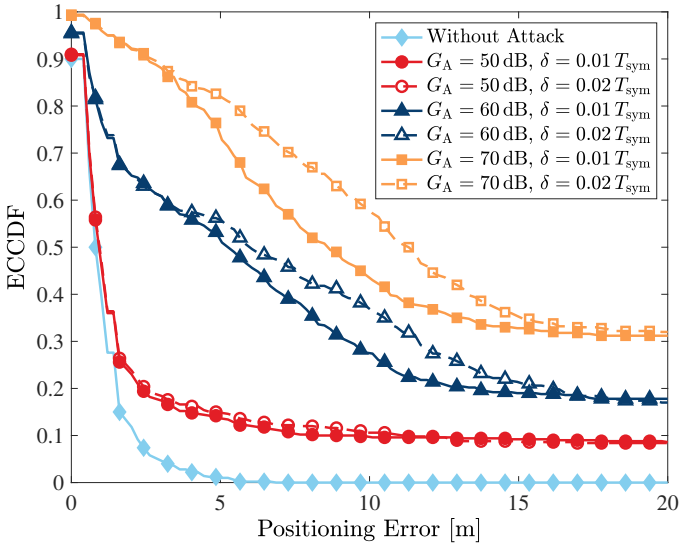

Figure 23: ECCDF of the positioning error considering different overshadow attack configurations. The performance is evaluated for LOS condition.

error also increases due to the stronger attacker signal, raising the probability of a successful attack. For a constant attacker gain, localization performance degrades more when the introduced delay is 2% of the symbol time, as greater delays increase the TDOA error and thus the UE position error. The 95-percentile positioning error defines Positioning Ser-

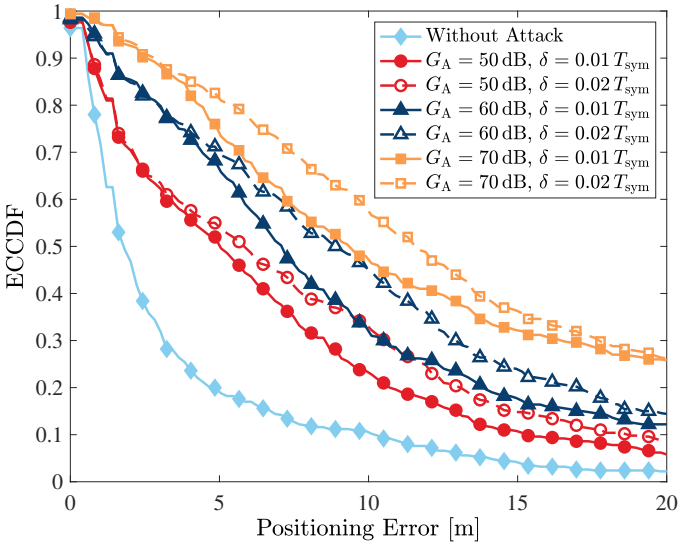

Figure 24: ECCDF of the positioning error considering different overshadow attack configurations. The performance is evaluated for NLOS condition.

vice Levels (PSLs) (see Sec. 2.1.6). It can be observed in Figure 23 and Figure 24 that, in the absence of an attack, the localization process in the simulated scenario can guarantee PSLs 1 and 2 only under LOS conditions, while, under attack, accuracy degrades making PSL compliance impossible.

We now evaluate the effect of the detection methods through the integrity risk. Measurements identified as compromised by the detection methods are excluded (see (3.1)) (in Section 3.3), and the integrity risk is then represented with the alert limit shown on the x-axis. The choice of the alert limit depends on the specific application requirements.

1a) Peak order analysis: Figure 25 shows the integrity risk using the peak order detection method for all attack configurations under both LOS and NLOS conditions. It can be observed that the positioning error is reduced for lower gains. In the case of an overshadow attack with $G_A = 50\,dB$ and $\delta = 1\%$ of T_{sym}, the probability of errors above $2\,m$

drops from 23% to 12% in LOS. With $G_{\mathrm{A}} = 60\,\mathrm{dB}$ and $\delta = 1\%$ of T_{sym} in LOS conditions, it reduces from 64% to 30%. Conversely, the detection method is less effective for higher gains, sometimes even worsening performance, as in the case with $G_{\mathrm{A}} = 70\,\mathrm{dB}$. Indeed, when G_{A} is significantly higher than the gain of the legitimate signal, the correlation peak P_2 is due to the multipath of the attacker's signal. In this case, since $P_1 > P_2$ and $t_1 < t_2$, the attack has success but goes undetected. In NLOS, the detection method becomes less effective due to the channel conditions. The probability of having a positioning error greater than 10 m reduces from 24% to 18% when $G_{\mathrm{A}} = 50\,\mathrm{dB}$ and $\delta = 1\%$ of T_{sym}, and remains the same (45%) when $G_{\mathrm{A}} = 60\,\mathrm{dB}$ and $\delta = 2\%$. The performance related to PSL improves, as we can now guarantee PSL 1 when $G_{\mathrm{A}} = 50\,\mathrm{dB}$ in LOS condition. For all the other overshadow attack configurations, the probability of the positioning error exceeding 10 m without detection remains above the requirement. It is important to mention that in NLOS conditions, there is a remarkable rate of false alarms above

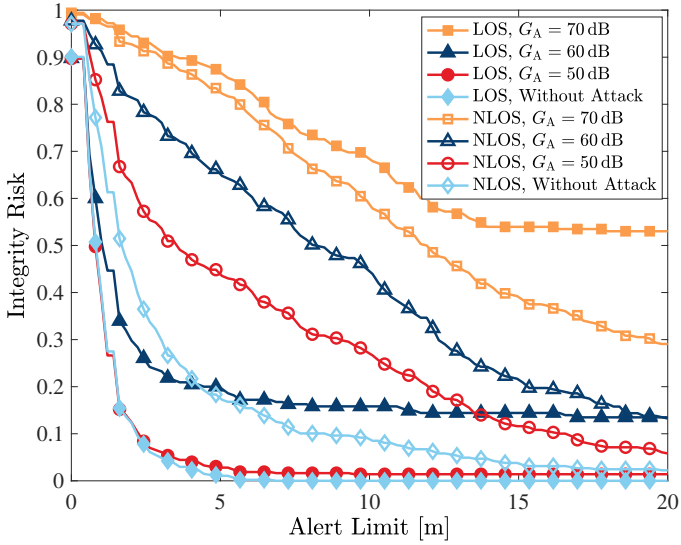

Figure 25: Integrity risk evaluated in LOS and NLOS conditions by varying G_A, after applying the peak order method. The attacker delay is 1% of T_{sym}.

10%. Therefore, we can consider this as a preliminary method, serving as a starting point for more advanced algorithms discussed below.

1b) Max amplitude analysis: To simplify the notation, in the following, we use ξ_p to denote $\xi_p = \xi_i$ in eq. (4.32) with p defining the percentile used for threshold setting. Unless otherwise stated, ξ_{95} is used.

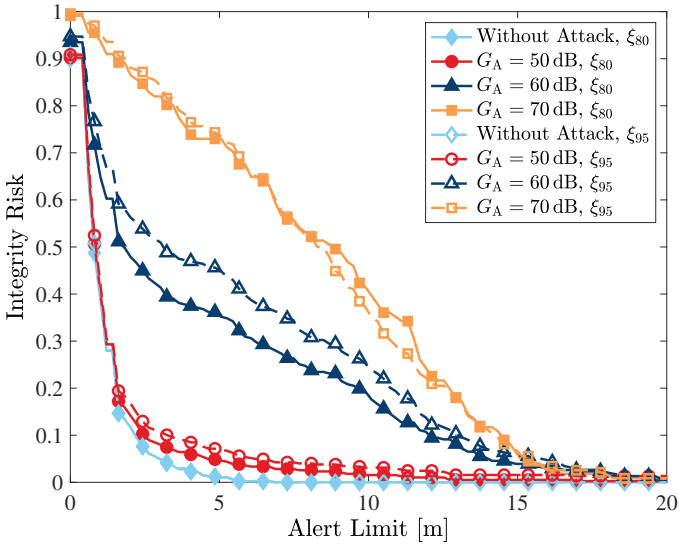

Figure 26: Integrity risk analysis in LOS conditions under various attacker gains (G_A), using the max amplitude method on correlation peaks with 80th (ξ_{80}) and 95th (ξ_{95}) percentiles thresholds. The attacker delay is 1% of the symbol time (T_{sym}).

Figure 26 and Figure 27 show the integrity risk with thresholds set at the 80-th and 95-th percentiles of the amplitude distribution in the absence of an attack, and the introduced attack delay is always the 1% of T_{sym}.

Comparing Figure 23 and 24 with Figures 26 and 27, we can observe that this detection method is particularly effective. For $G_{\text{A}} = 70\,\text{dB}$ and $\delta = 1\%T_{\text{sym}}$, integrity risk for errors above 15,m drops from 0.33 to 0.04 in LOS, and from 0.32 to 0.16 in NLOS with ξ_{80}. The performance is also enhanced for lower gains, even if less evident. By applying a threshold

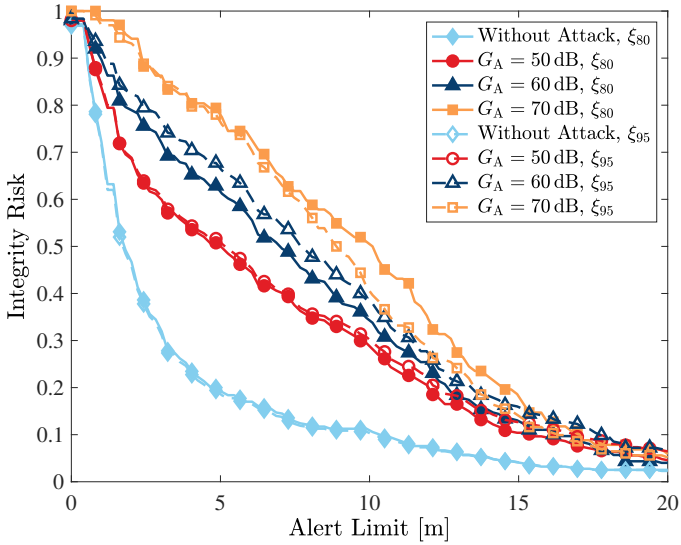

Figure 27: Integrity risk analysis in NLOS conditions under various attacker gains (G_A), using the max amplitude method on correlation peaks with 80th (ξ_{80}) and 95th (ξ_{95}) percentiles thresholds. The attacker delay is 1% of the symbol time (T_{sym}).

ξ_{95} when the attacker gain is $50\,\text{dB}$, the probability of having a positioning error greater than $15\,\text{m}$ decreases from 0.08 to 0.01 in LOS conditions, and from 0.14 to 0.12 in NLOS. Lower thresholds improve the likelihood of detecting the attack, thereby the integrity risk. Indeed, considering $G_{\text{A}} = 50\,\text{dB}$ as before, and now selecting ξ_{80}, we find that the probability of the error exceeding $15\,\text{m}$ is 0.005 in LOS conditions, and 0.1 in NLOS. However, it should be noted that setting a lower threshold led to an increased false positive rate. Threshold choice balances detection efficiency and false positives based on the requirements and the operational scenario. When the higher priority is to minimize false positives, a higher threshold should be selected at the cost of worsening the integrity risk. On the other hand, if a more efficient detection rate is preferred, the best choice is to lower the threshold, even if it will increase false positives.

The integrity risk is improved for higher attacker gains than the peaks

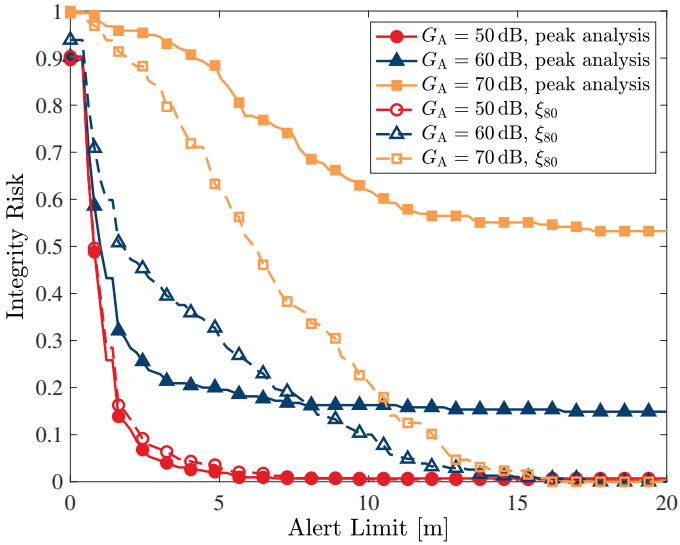

Figure 28: Comparison of detection methods in LOS conditions, with $\delta = 1\%$ of T_{sym}. The figure shows the integrity risk after applying peak order and ξ_{80}-threshold max amplitude methods.

order detection method. Figure 28 illustrates the comparison between the two methods under LOS conditions with $\delta = 1\%$ of T_{sym}, using ξ_{80} as the threshold for the maximum amplitude method. The detection rate is also improved in NLOS conditions: For $G_A = 70\,\text{dB}$, the detection rate applying the peak order analysis is around 31%, and it reaches 53.6% by involving the current solution, selecting a threshold equal to ξ_{95}. For all the other configurations, performance does not improve, as shown in Table 9. Therefore, relying solely on amplitude analysis is insufficient for achieving good results, making it necessary to use a method that simultaneously analyzes both the TOA and the maximum amplitude of the correlation peaks.

2) GMM-based detection method: In the latest proposed method presented in 4.4.3, we leverage the GMM to detect anomalies in the relationship between the TOA estimates and their corresponding peak amplitudes. First, we find the probability that each measurement does not

belong to the distribution obtained under safe conditions. Then, we compare the likelihood with a pre-selected threshold. To simplify the notation, in the following, we use ξ_p to denote $\xi_p = \xi_i$ in eq. (4.36) with p defining the percentile used for threshold setting. Unless otherwise stated, ξ_{95} is used.

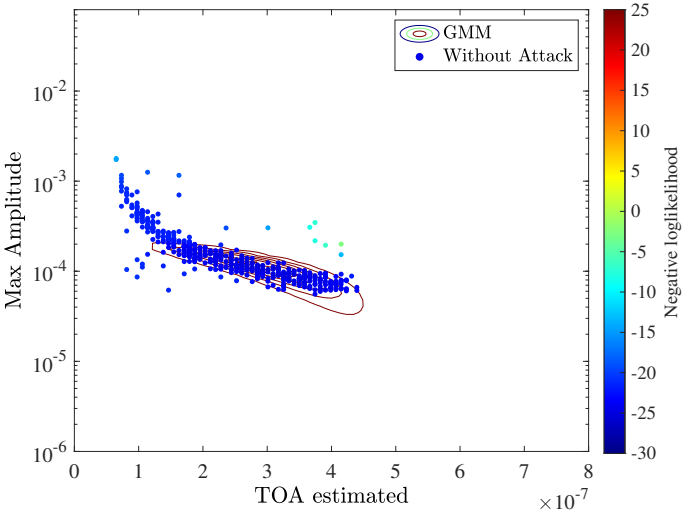

Figure 29: Negative log-likelihood obtained as GMM model in LOS condition.

Two GMMs are trained separately for LOS and NLOS scenarios. Figure 29 and Figure 30 illustrate these models without attacks, with TOA on the x-axis, correlation peak amplitudes (log scale) on the y-axis, and point color representing the value of the negative log-likelihood.

It's clearly visible that in the NLOS scenario, there is an evident division between the points in the distribution due to the dataset configuration: the channel is in NLOS condition 50% of the time, represented by lower amplitudes, and in LOS condition 50% of the time, aligning with the LOS distribution in Figure 29.

Under attack, it is evident how the measurements tend to shift towards higher gains and TOA values, deviating from the model. For $G_{\mathrm{A}} = 60\,\mathrm{dB}$ and $\delta = 1\%$ of T_{sym} case, illustrated in Figure 31 and Fig-

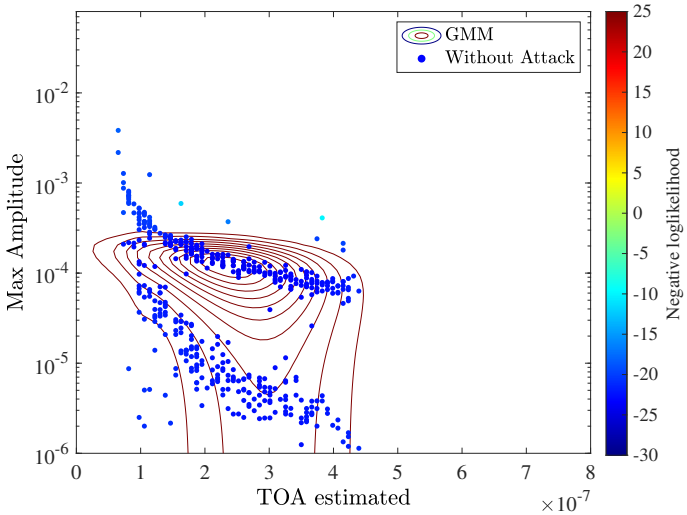

Figure 30: Negative log-likelihood obtained as GMM model in NLOS condition.

ure 33, the detection rate is 66% in LOS conditions and 61.2% in NLOS conditions, as reported in Table 9.

When the introduced delay δ is incremented to the 2% of T_{sym}, the shift in time becomes more accentuated, as illustrated in Figure 32 and Figure 34, increasing the detection rate to 66.2% in LOS and 81.6% in NLOS.

Table 9 reveals a common pattern: larger introduced delays lead to greater estimations errors, enhancing the effectiveness of the GMM method. Therefore, if attackers want to remain undetected, they must minimize delay, reducing their impact on the estimation. We can also notice from the table that increasing the attacker gain leads to an improved detection rate. For $G_{\text{A}} = 70\,\text{dB}$ and $\delta = 1\%$ of T_{sym}, detection reaches 100%. As stated in Table 9, the false positive rate is 3.6% in LOS and 11.8% NLOS scenarios. The results demonstrate that the method effectively identifies spoofing attacks by analyzing the relationship between the TOA estimates and their corresponding peak amplitudes, resulting in the best above the proposed methods.

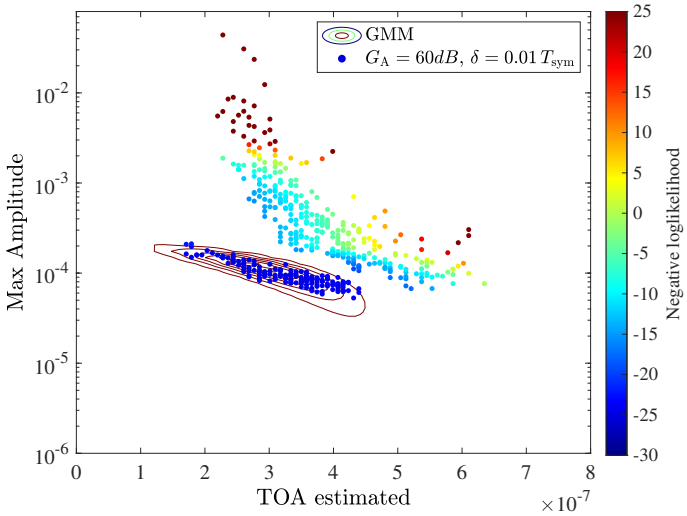

Figure 31: Negative log-likelihood obtained as GMM model in LOS condition with Attack setting: $G_{\mathrm{A}} = 60$ dB and $\delta = 1\%T_{\mathrm{sym}}$. The contour plots represent the GMM obtained without attack. The dots represent measured log-likelihood values.

One of the key strengths of our approach lies in its computational efficiency. Unlike Artificial Intelligence (AI)-based techniques for localization, our GMM-based method operates directly on standard metrics available at the output of the cross-correlation step in the 5G localization framework. Moreover, while GMMs require training data, this does not impose additional burdens since the necessary data entry is collected in real-time as part of the existing localization procedure, leveraging outputs from the correlator. This integration ensures that the training process aligns seamlessly with standard positioning workflows, eliminating the need for separate data collection and minimizing overhead. This design, once the model is trained, allows anomaly detection and integrity checks to run in parallel with the localization process, without introducing significant latency, ensuring compatibility with real-time systems. Also considering larger-scale 5G deployments, where many gNBs and UEs are involved, the scalability of the approach remains efficient. In typ-

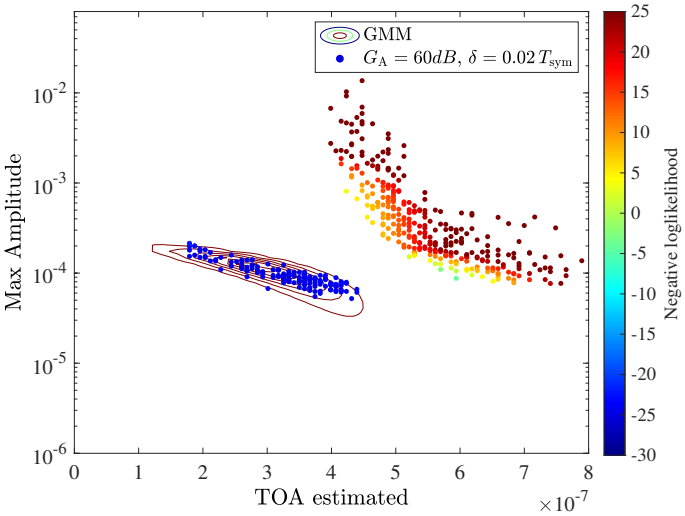

Figure 32: Negative log-likelihood obtained as GMM model in LOS condition with Attack setting: $G_{\mathrm{A}} = 60$ dB and $\delta = 2\%T_{\mathrm{sym}}$. The contour plots represent the GMM obtained without attack. The dots represent measured log-likelihood values.

ical operating scenarios, only a subset of gNBs are connected to the UE at any given time, reducing the computational load and limiting the number of measurements that need to be processed. Furthermore, the trade-off between latency and integrity is carefully managed. Indeed, while the integrity monitoring process may introduce minor delays, these are justified by the critical importance of ensuring reliable positioning. This balance is especially important in safety-critical applications, where accurately detecting spoofing attacks is essential to ensure trust and system functionality.

4.6 Summary and Outlook

In this Chapter, we addressed the critical issue of physical layer threats to 5G positioning systems, which is essential for the reliable operation of safety-critical applications. We presented a comprehensive threat model

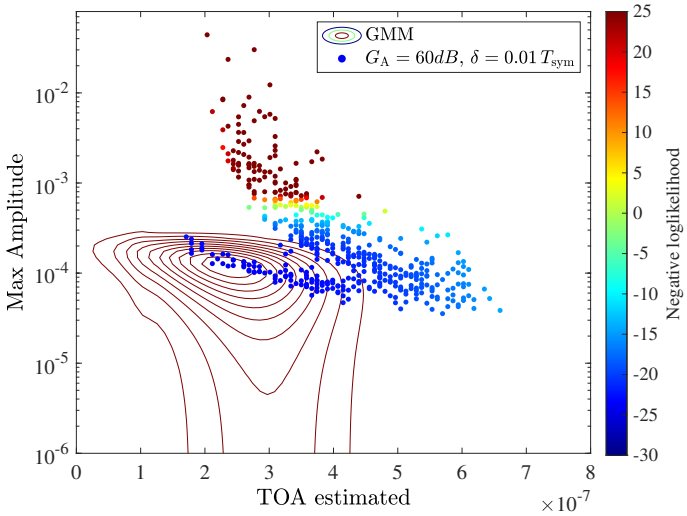

Figure 33: Negative log-likelihood obtained as GMM model in NLOS condition with Attack setting: $G_{\mathrm{A}} = 60$ dB and $\delta = 1\%T_{\mathrm{sym}}$. The contour plots represent the GMM obtained without attack. The dots represent measured log-likelihood values.

Table 9: Results comparison of proposed detection methods under various attacker configurations in both LOS and NLOS scenarios. Thresholds for the max amplitude and GMM-based methods are set at the 95th percentile.

Detection Method	**Channel Configuration**	**False Alarm Rate**	**Attack Configuration and Detection Rate**					
			$G_A = 50$ dB		$G_A = 60$ dB		$G_A = 70$ dB	
			$\delta = 1\%$	$\delta = 2\%$	$\delta = 1\%$	$\delta = 2\%$	$\delta = 1\%$	$\delta = 2\%$
Peaks Order (4.4.2)	LOS	5.4%	14.8%	14.4%	57%	57%	56.8%	57%
	NLOS	10.6%	24%	24.2%	30.6%	29%	31%	31.2%
Max Amp. (4.4.2)	LOS	6.2%	10.4%	10.4%	25.2%	24.6%	53.6%	53.2%
	NLOS	4.2%	10.2%	10.2%	25.6%	25%	53.6%	53.6%
GMM (4.4.3)	LOS	3.6%	15.4%	16%	66%	66.2%	100%	99.6%
	NLOS	11.8%	29.6%	57%	61.2%	81.6%	100%	99.8%

for timing-based measurements and evaluated the impact of such threats under both LOS and NLOS conditions through extensive simulations in a dense indoor deployment scenario compliant with 3GPP specifications. To mitigate these threats, we proposed two detection methods based on time and amplitude analysis, including a GMM-based approach. The latter demonstrated superior performance across a variety of attack config-

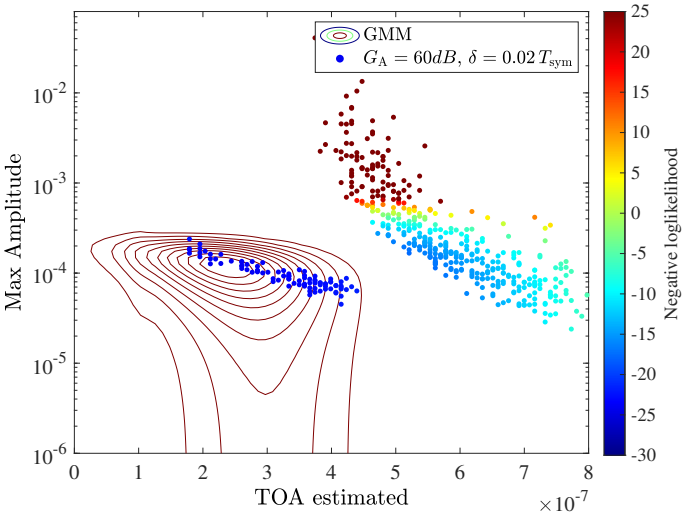

Figure 34: Negative log-likelihood obtained as GMM model in NLOS condition with Attack setting: $G_{\mathrm{A}} = 60$ dB and $\delta = 2\%T_{\mathrm{sym}}$. The contour plots represent the GMM obtained without attack. The dots represent measured log-likelihood values.

urations, significantly reducing integrity risks and enhancing positioning accuracy.

These findings underscore the importance of developing and integrating advanced detection mechanisms to ensure the resilience of 5G and beyond positioning systems against physical layer attacks. Assessing how these factors influence both attack feasibility and detection performance will be essential to validate the generality and robustness of the proposed methods in diverse real-world environments. In the next Chapter, we move from simulation to practical evaluation by presenting an experimental implementation of the *Overshadowing - Replay Attack* (Meaconing) attack described in this Chapter, further highlighting its impact and the challenges associated with real-world detection.

Chapter 5

Translating Theory into Practice: Experimental Analysis of Meaconing Attack

Meaconing is a well-established attack technique targeting positioning systems, where legitimate signals are intercepted, delayed, and retransmitted to manipulate a user's estimated position. This method poses a significant threat as it introduces spatial inaccuracies while maintaining uninterrupted positioning service, remaining effective even when the transmitted data is encrypted. Meaconing primarily exploits systems that rely on time-of-flight calculations, such as Global Navigation Satellite System (GNSS) and radar-based ranging technologies. The impact of meaconing on these systems, as well as potential countermeasures, has been extensively studied over the years [96]–[98]. Additionally, experimental research has demonstrated the feasibility of relay/replay attacks on GNSS signals using easily accessible off-the-shelf hardware, highlighting their practicality in real-world scenarios [7].

While 5th Generation (5G) systems utilize timing-based methods alongside other positioning techniques, meaconing has so far received a some-

what marginal attention as it has been considered not viable in cellular communication systems. As a consequence, recent works on 5G location security assume that adversaries would need to rely on more complex and hard-to-tune selective signal overshadowing techniques (selective spoofing) as mentioned in the previous chapters. In contrast, full-frame meaconing attacks offer a more practical and stealthy alternative. In this scenario, the attacker delays the entire 5G frame, including the Positioning Reference Signal (PRS) and other transmitted signals, and retransmits it with a higher power to exploit the capture effect at the receiver. Unlike selective spoofing, this method does not require knowledge of the PRS initialization parameters, making it simpler to implement. Additionally, it introduces positioning errors without disrupting the ongoing communication process, allowing the attack to remain undetected while compromising the accuracy of the user's position estimate, as illustrated in Figure 35.

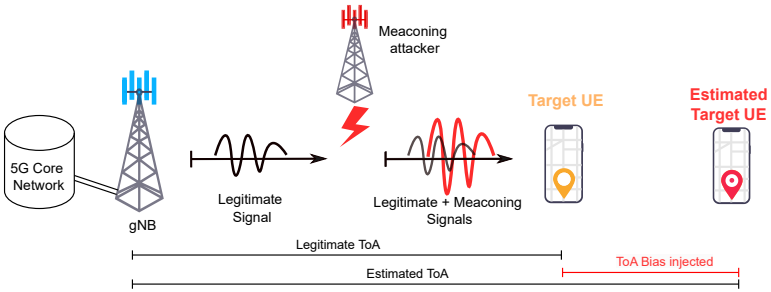

Figure 35: Architecture of meaconing attack and impact on the Time of Arrival (TOA) estimation.

The main concern about meaconing in 5G positioning lies in the nature of the attack itself, which requires the continuous retransmission of delayed and amplified replicas of *entire* 5G frames. However, unlike GNSS systems, where the whole signal is designed for localization purposes, in 5G frames, positioning reference signals constitute only a marginal part. The majority of the frame is instead dedicated to the precise control and reliable delivery of communication data, whose ampli-

fied retransmission is deemed to cause potential communication disruption.

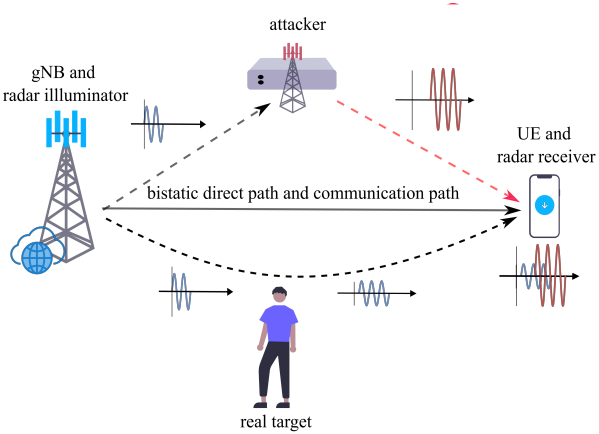

Figure 36: Bistatic 5G New Radio (NR) Integrated Sensing and Communication (ISAC) scenario where the gNodeB (gNB) illuminates the scene and the User Equipment (UE) senses. A blind attacker replays the captured downlink frame with a programmable delay and carrier offset, forging an additional propagation path without demodulating or decoding the signal

ISAC is an emerging paradigm that exploits the same radio resources to simultaneously support data transmission and environmental sensing. At the same time, ISAC inherits from the radar and sensing domain a critical threat surface, where an over-the-air adversary can overshadow or replay the signal to manipulate sensing outcomes [99]. Within this context, we adapt the same meaconing attack on the ISAC framework. Indeed, we investigate an attack scenario in which an adversary blindly delays, applies a frequency offset, and continuously replays the incoming 5G Orthogonal Frequency Division Multiplexing (OFDM) frame at higher power, as shown in Fig. 36.

5.1 System and Threat Model

This section first outlines the structure of 5G communication channels and signals used for both data transmission and positioning, then presents a mathematical model of the meaconing attack and its impact on 5G-based localization services.

5.1.1 System Model: Sensing, Localization and Communication

5G Communication and Localization

In 5G systems, the gNB and UE exchange radio frames containing multiple physical control and data channels [57]. Among the control channels is the Synchronization Signal Block (SSB), which carries the Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS), enabling the UE to synchronize with the gNB's radio frame structure. Among the data channels is the Physical Downlink Shared Channel (PDSCH), which transports user data. Reference signals are embedded within these channels to ensure accurate signal reception and channel estimation. Positioning in 5G leverages dedicated reference signals such as the PRS (downlink) and the Sounding Reference Signal (SRS) (uplink). For downlink positioning, the gNBs periodically transmits in a synchronized way PRSs in predefined radio frame slots during ongoing communication with the target UE. The UE is aware of the PRS configuration and timing information thanks to the Location Management Function (LMF), i.e., the standardized network function overseeing localization. Then, the UE processes the received PRS by relying on a locally generated sequence to measure the TOA. The LMF then uses these measurements to determine the target UE's position.

Integrated Sensing and Communication (ISAC)

The 3rd Generation Partnership Project (3GPP) is currently investigating the standardization of ISAC within 5G/6G systems [24], [25]. Nevertheless, at the time of this work, no specific signals have been defined exclu-

sively for communication and sensing operations. In this study, the 5G OFDM waveform is considered, which, although primarily designed for user communication, can also be leveraged to extract information about surrounding objects and their dynamics by reusing the PRS/SRS originally introduced for positioning in 5G systems. Within this framework, in an ISAC scenario, the gNB illuminates the scene using PRS, while either the gNB (monostatic configuration) or a remote UE (bistatic configuration) performs matched filtering and 2D FFT processing to obtain the Range-Doppler Map (RDM). The RDM constitutes a fundamental performance indicator for sensing operation, as it represents sensed targets in terms of distance and relative velocity.

5.1.2 Threat Model: Meaconing Attack

A meaconing attack involves intercepting a legitimate signal and retransmitting it after introducing a controlled delay and amplification, thereby misleading the receiver about the signal's actual arrival time. In 5G systems, let $s(t)$ represent the signal transmitted by the gNB, which includes both data symbols (communication) and PRS symbols (localization). The attacker first receives the legitimate signal as $r_{\mathrm{A}}(t)$ after propagation from the gNB to the attacker and then retransmits it after a delay δ and by applying an amplification factor G_{A}. The malicious retransmitted signal is

$$s_{\mathrm{A}}(t) = G_{\mathrm{A}} \cdot r_{\mathrm{A}}(t-\delta) \quad \forall t \geq \delta \tag{5.1}$$

The victim UE receives the resulting combined signal, which is the sum of the legitimate signal and the malicious signal after propagation from the attacker to the UE. Assuming a multipath channel, the resulting received signal by the UE can be written as

$$r_{\mathrm{UE}}(t) = \sum_{n=1}^{N_{\mathrm{p}}} \alpha_n s(t-\tau_n) + G_{\mathrm{A}} \sum_{m=1}^{M_{\mathrm{q}}} \gamma_m s(t-\delta-\phi_m) + w(t) \tag{5.2}$$

with the first term depending on the channel from the gNB to the UE, where α_n and τ_n are the complex amplitude and delay for the nth multipath component; the second term depends on the two channels from

the gNB to the attacker and from the attacker to the UE; here, γ_m and ϕ_m are the complex amplitude and delays resulting from the convolution of the two channel responses; the third term is the receiver noise, usually modeled as a white Gaussian noise[1]. Due to the capture effect [74], the UE generally locks onto the strongest signal component for communication and positioning. In a timing-based positioning method, if the attack is successful, i.e., the attacker's delayed signal dominates, the UE estimates the TOA incorrectly, introducing a bias $\Delta = \delta + \phi_1 - \tau_1$, leading to an erroneous position estimate. For instance, a delay of $1\,\mu s$ in TOA estimation results into a ranging error of roughly $300\,m$, significantly degrading localization accuracy.

5.2 Attack Implementation

A full-frame 5G meaconing attack can be executed by using a single Software-Defined Radio (SDR), facing two primary challenges: managing the overhead timing introduced by the attacker's signal processing and mitigating self-interference resulting from simultaneous reception and transmission operations.

Timing

NI Ettus USRP SDR devices are commonly controlled by a host system via the UHD driver and associated APIs [100]. In a conventional setup, the received signal is transferred to the host for processing and then returned to the USRP for re-transmission. This round trip introduces a non-negligible delay on the order of half a millisecond, sufficient to disrupt ongoing 5G communications and related services. However, by leveraging the FPGA-based NI Ettus RF Network on Chip (RFNoC) architecture, the signal reception and re-transmission operations can be directly implemented on the USRP board, thus minimizing the processing

[1]Note that the noise receiver at the attacker side is considered negligible, which is a particularly realistic assumption as an attacker would use a directive antenna to ensure high SNR.

delay. Moreover, we achieve precise control over the introduced delay through the RFNoC Samples per Packet (SPP) parameter.

Self-Interference

Simultaneous reception and transmission inherently suffer from two sources of self-interference: (i) an internal interference due to shared hardware resources between the reception and transmission chains of the SDR; and (ii) the attacker's transmitted signal may inadvertently jam its own receiver if not properly isolated. We employ SDR board such as the NI Ettus X410, which provide distinct, isolated chains on a single device to address the first issue. The second issue is mitigated by employing a directive receiving antenna oriented toward the gNB, which minimizes self-interference by creating a spatial null, or "shadow zone," in the retransmission direction.

5.3 Case-Study based on Signal Generated via MATLAB

Within this preliminary results, we focus on the transmission of the PRS generated through MATLAB, as our primary objective is to investigate and illustrate the impact on TOA estimation during a meaconing attack. In addition, we also evaluated the communication service with a smartphone UE and an Amarisoft Callbox Mini gNB in the next section.

5.3.1 Experimental Testbed

The testbed, illustrated in Figure 37, comprises three Universal Software Radio Peripheral (USRP) SDR devices operating in line-of-sight: two dedicated to legitimate communication and one acting as the attacker.

Legitimate transmission and reception are performed using USRP X310 devices [47] equipped with OmniLOG 70600 omnidirectional antennas [101]. The attacker employs a USRP X410 [102] with a HyperLOG 6080 directive antenna [103] to receive the legitimate signal, thereby

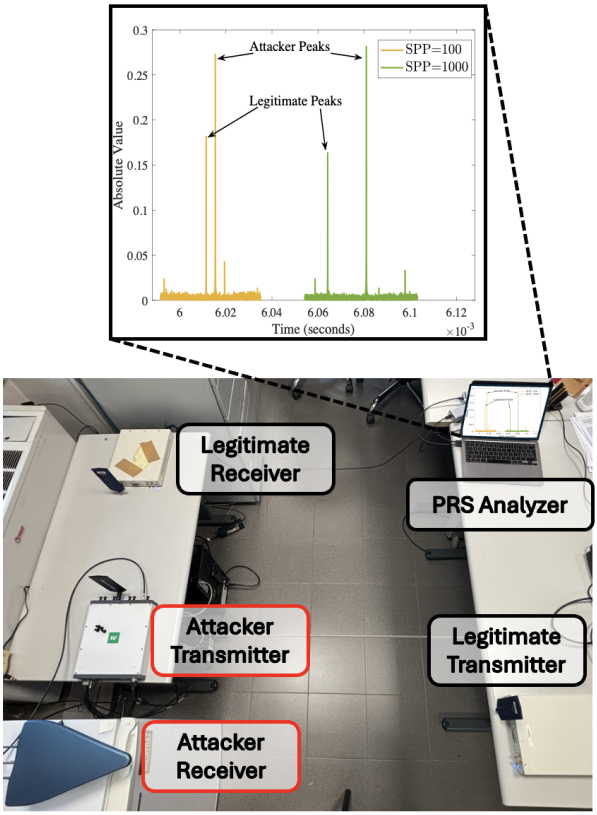

Figure 37: Experimental Setup for 5G Positioning Spoofing Attack: The lower image depicts the testbed environment with Legitimate Tx/Rx, Attacker Tx/Rx, and PRS Analyzer, while the upper plot shows time-domain peaks of Legitimate and Attacker signals, highlighting spoofing effects varying SPP.

avoiding self-interference while transmitting via an OmniLOG 70600 omnidirectional antenna [101]. The PRS is transmitted within the N77 5G NR band with 3.4 GHz carrier frequency, a bandwidth of 60 MHz, and a subcarrier spacing of 30 kHz, corresponding to a symbol time of 33.33 μs. The attacker implementation runs directly within the RF System on Chip (RFSoC) architecture of the USRP X410 board, ensuring minimal delay

during the attack by handling reception and transmission in parallel on the SDR hardware itself, rather than relying on host system processing. The attacker introduces a programmable delay, leveraging the RFSoC SPP parameter.

5.3.2 Results

The upper part of Figure 37 shows the output of the PRS correlation analyzed in MATLAB. A clear distinction can be made between the legitimate and attacker peaks, with the malicious one being higher due to retransmission amplification.

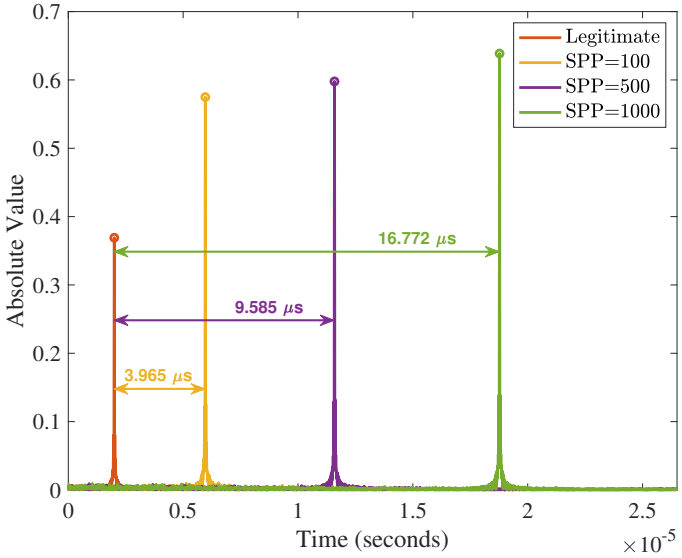

Figure 38: PRS correlation peaks comparing legitimate versus attacker signals across SPP values of 100, 500, and 1000, showing corresponding attacker-induced time delays of $3.965\mu s$, $9.585\mu s$, and $16.772\mu s$ respectively.

Figure 38 further illustrates the increased peak power and the delay introduced by the attacker in the TOA estimation, observed by different attacker parameter SPP set to 100, 500, and 1000. This delay, observed as

the time difference between the legitimate and malicious peaks, grows as the attacker increases the relative delay. The impact of the attack becomes more significant with higher delay values, leading to an increase in the normalized absolute value of the correlation peak, as the overlap between the legitimate and attacker PRS signals diminishes. The minimum delay in this configuration occurs when SPP is set to 100, corresponding to a bias injection of approximately $3.965\ \mu$s in the timing measurement. This delay translates to an erroneous increase of around 1188 m in the estimated distance between the gNB and the UE. For instance, as shown in [17], a bias of approximately 100 meters in the TOA estimation can result in a localization error of about 12 meters at the 90th percentile. Such a bias severely compromises the final position estimation, emphasizing the need for robust countermeasures. While our demonstration targets TOA manipulation specifically, the underlying principles extend to other positioning methods. This meaconing technique can readily compromise Time Difference of Arrival (TDOA) and Round Trip Time (RTT) measurements, and with directional antennas, can similarly affect angle-based positioning. The attack highlights a fundamental vulnerability: wireless positioning systems remain susceptible to physical-layer manipulation regardless of cryptographic protections.

5.4 Case-Study based on Full 5G System

In this section, we describe the configuration of the testbed deployed for the experimental case study, as illustrated in Figure 39. We then present the results and analyze the meaconing attack's impact on both communication and localization services.

5.4.1 Experimental Testbed

The experimental testbed used to demonstrate the meaconing attack on full-frame 5G transmissions comprises the following components:

- **5G Core Network:** A commercial Athonet[2] 5G CN handles signal-

[2]https://buy.hpe.com/it/it/software/networking-software/private-network-

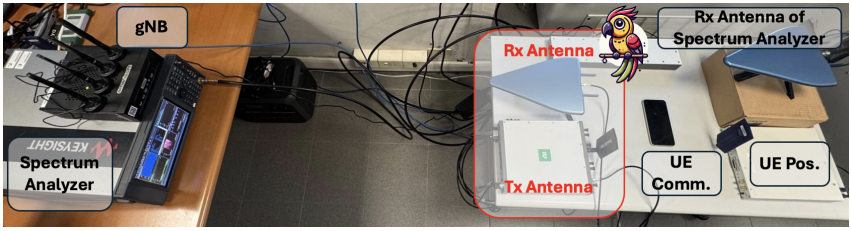

Figure 39: Experimental testbed setup for the full-frame 5G meaconing attack, comprising the 5G Core Network (CN), gNB, UEs (Samsung smartphone and USRP X310), the "parrot" attacker's device SDR (Ettus X410), and a Keysight spectrum analyzer.

ing, authentication, and other control-plane functions.

- **gNB:** The gNB is realized using an Amarisoft Call Box Mini [46], providing the 5G NR access interface for both communication and positioning services.

- **UEs:** Two distinct receivers are employed to evaluate communication and localization services, separately. A Commercial Off The Shelf (COTS) Samsung A54 5G smartphone tests the communication service, ensuring that data sessions are intact under attack. For the localization service, a USRP X310 [47] equipped with an OmniLOG 70600 [101] omnidirectional antenna and controlled via MATLAB is utilized to process PRS signals and analyze ranging timing-based measurements.

- **Attacker:** The *"parrot"* device leverages a NI Ettus X410 [102] SDR. A directive HyperLOG 6080 [103] antenna is pointed toward the gNB for precise signal reception, while an OmniLOG 70600 omnidirectional antenna replays the captured signal. This configuration enables controlled meaconing of full-frame 5G signals.

- **Spectrum Analyzer:** A Keysight MXA N9021B [104] spectrum analyzer validates the presence and influence of the attacker on the

software/aruba-networking-private-5g-software/athonet-mobile-core/p/1014769364

resulting 5G NR signal. Indeed, by examining the received signal power per Resource Element (RE) before and after the meaconing event, it confirms the attack's impact on the 5G system.

5.4.2 Results

To assess the feasibility and impact of the meaconing attack under realistic 5G conditions, we analyze both duplexing schemes: Frequency Division Duplex (FDD) and Time Division Duplex (TDD) as shown in Table 10.

Table 10: Radio Frequency configuration of the two scenarios analyzed during the meaconing attack.

Multiplexing Schemes	NR Band	BW [MHz]	SCS [kHz]	Symbol Time [μs]
TDD	78	20	30	33.33
FDD	7	20	15	66.67

Evaluating the meaconing attack across these configurations, FDD with comparatively relaxed timing constraints and TDD with more stringent timing, provides a comprehensive view of its robustness and effectiveness under varying operational scenarios. The TDD setup, in particular, presents a challenging environment that closely mirrors real-world demands on 5G systems, thereby offering a rigorous test of the attack's viability.

Attack Validation

We employ two distinct methods to verify the correct execution of the meaconing attack.

- **Smartphone-based Approach:** A COTS smartphone running the *NetworkSignalGuru* (v4.6.21) application [105] is used to measure key radio metrics like Reference Signal Received Power (RSRP) and signal-to-interference-plus-noise ratio (SINR). From application screenshot [105], [106] we observed that, under the attack, the

RSRP increased by approximately 13 dBm, the SINR decreased by 6 dB, while the Reference Signal Received Quality (RSRQ) remained relatively stable, as shown in the Figure 40.

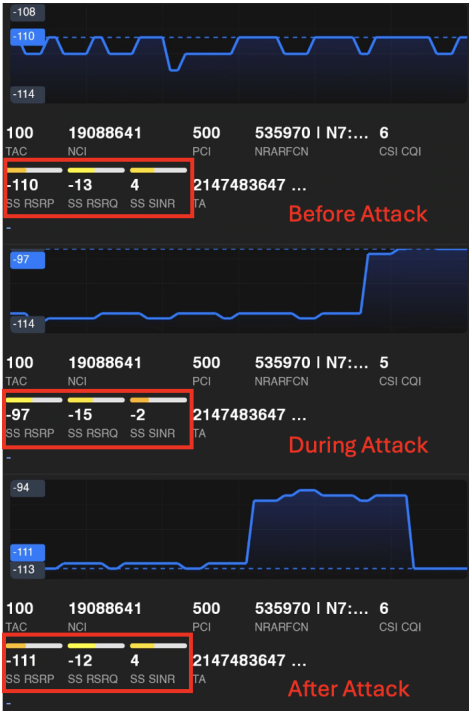

Figure 40: Measured power levels of reference signals (RSRP, RSRQ, and SINR) using the smartphone application before (top), during (middle), and after (bottom) the meaconing attack.

In addition, in the upper plot of Figure 41 shows a histogram of the measured RSRP with and without the attack in both TDD and FDD scenarios. Under attack, the RSRP increases by approximately 10 dB in both scenarios, confirming that the attacker's signal significantly affects the received power levels at the UE by overshadowing the legitimate communication.

- **Spectrum Analyzer-based Approach:** For a more formal and pre-

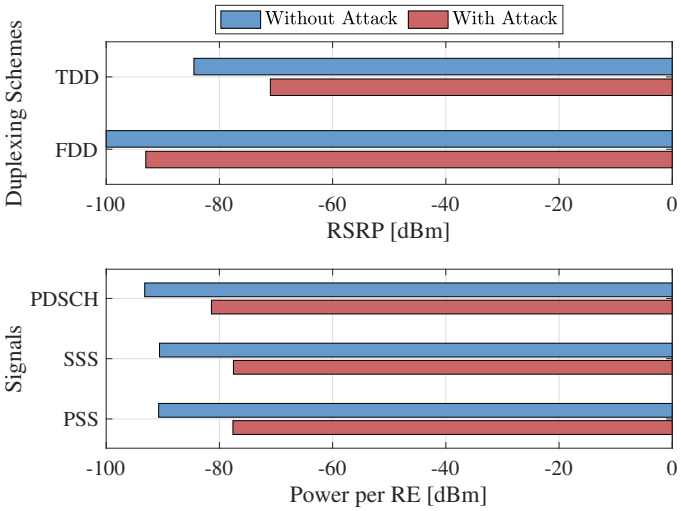

Figure 41: Attack Power Analysis: (Top) RSRP measurements using spectrum analyzer in both TDD and FDD duplexing schemes, with and without the meaconing attack. (Bottom) Power per RE for various 5G signals under the FDD scheme, demonstrating increased power levels during the attack.

cise verification, we use a Keysight MXA N9021B spectrum analyzer [104] capable of decoding the 5G frame and measuring the power per RE for different signals as show in table 11. In the lower plot of Figure 41, we observe the same trend: the power per RE is higher when the attack is active. This result corroborates the findings from the smartphone measurements, confirming that the meaconing attack indeed increases the signal power level received by the UE under both FDD and TDD schemes.

Impact on Communication Service

Having established the presence of the attacker, we now examine its influence on the ongoing communication service. First, the meaconing attack does not completely interrupt the communication between the gNB and the UE, avoiding Denial of Service (DoS), thus maintaining a degree

of stealthiness. This behavior is evident in Figure 42, where the downlink bitrate decreases during the attack (highlighted in red) without dropping to zero. Second, although communication is not halted, the amount of transmitted data diminishes because the victim UE perceives increased interference. As confirmed by the measured SINR, which declines from about 13 dB to 8.5 dB during the attack, the UE experiences lower signal quality. This degradation prompts a downgrade in modulation order: as shown in Figure 42, the modulation scheme shifts from 16QAM to QPSK during the attack, then returns to 16QAM afterward. This direct correlation between reduced SINR, lowered modulation order, and decreased bitrate exemplifies the negative impact of the meaconing attack on communication performance.

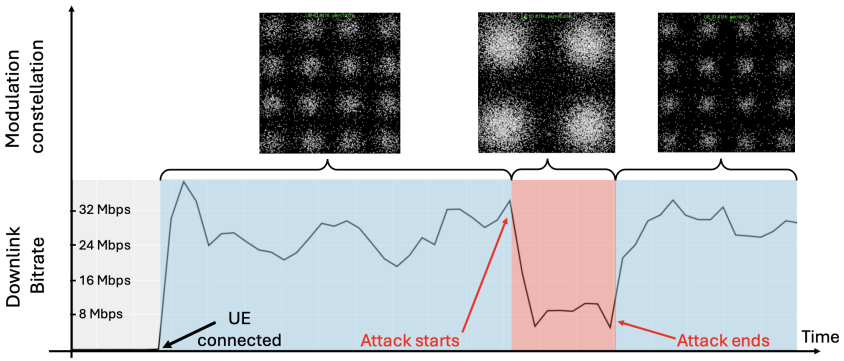

Figure 42: Temporal evolution of downlink bitrate (Bottom) and uplink modulation constellation (Top) with (red zone) and without (blue zone) the meaconing attack.

Table 11: Power per RE for different signals with and without the meaconing attack, measured using the spectrum analyzer.

	Power per RE [dBm]			
Signal	PSS	SSS	PBCH-DMRS	PBCH
with attack	-78,88	-78,72	-78,93	-78,96
without attack	-87,93	-87,9	-88,05	-87,98

Impact on Localization Service

Finally, we assess the meaconing attack's impact on 5G localization. The primary metric is the correlation of the received PRS with a locally generated reference sequence. By monitoring these correlation peaks, is possible to estimate TOA and leverage multiple synchronized gNBs to infer the UE position.

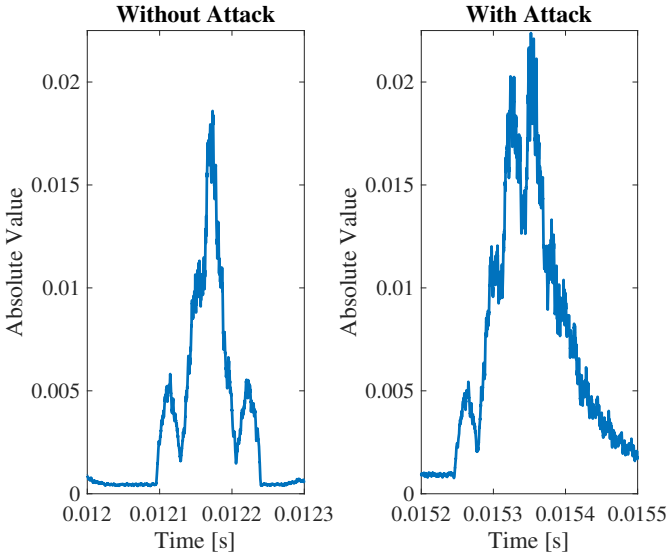

Figure 43: Correlation peaks of the PRS signal: (Left) Single peak without the meaconing attack, and (Right) dual peaks with the attack, indicating the presence of an additional delayed and amplified signal from the attacker.

Figure 43 demonstrates how the attack introduces additional peaks in the PRS correlation. A simple moving average filter, with a window size equal to 100 samples, is applied to the correlation output values for better visualization clarity. Only one legitimate, dominant peak is visible without attack (left plot), while a second significant peak appears under attack conditions (right plot). The second peak is delayed and amplified with respect to the legitimate. This secondary peak directly stems from the attacker's retransmission, which introduces an artificial mali-

cious delay. In our attack scenario, adjusting the RFNoC-related SPP parameter to 2000 results in a delay of about $30\,\mu$s, making the two peaks easily distinguishable. Reducing the SPP to 100 decreases the delay to approximately $4\,\mu$s, representing a more realistic and challenging attack scenario. Even such a smaller delay translates into a substantial ranging error (on the order of 1200 m), severely compromising the accuracy of the UE's position estimate.

5.5 Case-Study based on ISAC Scenario

This kind of attack can be replicated also in the ISAC framework since as described the communication between the gNB and the UE is not interrupted. Hence, the same attack can disrupt the sensing performance without performing a DoS on the communication of the ISAC.

5.5.1 Experimental Testbed

The testbed used to exploit the impact of the attack on ISAC scenario is the same as the previous section (shown in Figure 39), with the only difference that the UE is used for sensing operation with respect to positioning. As previously described in the case study, the relay-based attack is implemented using a radio loopback mechanism on our SDR platform. The attacker captures the legitimate OFDM signal, applies a programmable delay, and retransmits it with increased power, functionally equivalent to a single-tap finite impulse response (FIR) filter. The delay is precisely controlled through the SPP parameter in the FPGA-based RFSoC architecture, which we set to 100, corresponding to about $3.9\,\mu$s delay. This short delay in the uplink scenario ensures that the injected path's peak remains within the limited Channel Impulse Response (CIR) window of the Amarisoft gNB. By boosting the retransmitted signal's power, the attacker can inject false targets or mask genuine ones, while maintaining operational communication.

5.5.2 Results

We now evaluate the impact of the attack on ISAC in two different ways. In the former one, in downlink scenario, by looking the RDM obtained by the correlation of the PRS. In the latter one. in uplink scenario, we look on the CIR of the SRS transmitted by the smartphone and received and analyzed by the Amarisoft.

Downlink Scenario

Considering the downlink scenario in absence of an attack the resulting RDM at the receiver is shown in Figure 44. In the absence of the attack, the strongest correlation peak corresponding to the direct path between the gNB and the UE. Indeed, it is located at the origin with zero Doppler due to the static nature of the setup.

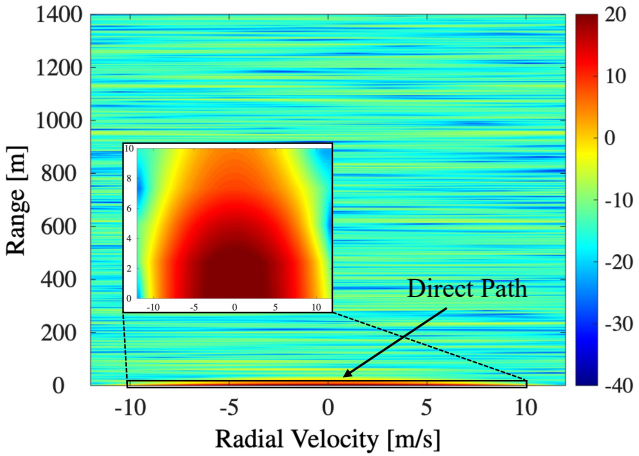

Figure 44: RDMs at the receiver without an attack. The legitimate direct path appears centered at zero range and zero Doppler, as expected in a static scenario and highlighted in the plot zoom.

We progressively increase the attacker's output power while keeping the delay fixed from 48 dB to 60 dB. The received power ratio between replay and legitimate signals, determines two observed distinct outcomes:

1. **Ghost-Target Injection:** If the attacker's signal reaches the receiver with lower power than the legitimate transmission, the PRS correlation peak of the genuine signal remains dominant and is correctly interpreted as the direct path. A second, weaker peak, delayed by

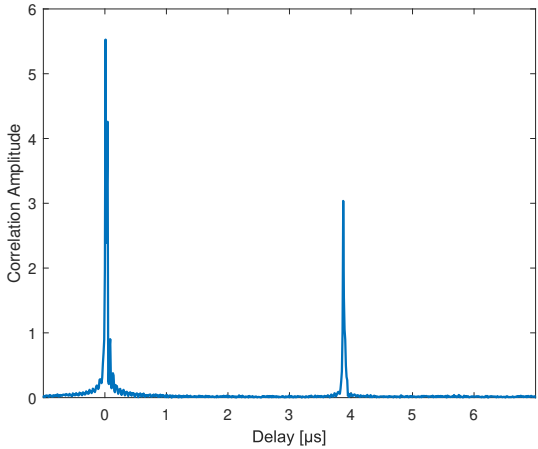

Figure 45: PRS correlation when the attacker transmits with a gain of 48 dB. The legitimate peak is aligned at zero delay, while the attacker's weaker peak is delayed by 3.9μs.

3.9μs, appears as a result of the forged signal. Figure 45 illustrates this case, where the attacker uses a transmit gain of 48 dB. The legitimate peak is aligned at zero delay and has higher amplitude, while the delayed peak corresponds to the attacker's signal. The resulting RDM, shown in Figure 46, reveals a fake target at a bistatic range of approximately 1150 m, consistent with the introduced delay of around 3.9μs. Moreover, due to the 100 Hz frequency offset applied during retransmission, the forged target appears with an artificial Doppler shift equivalent to a radial velocity of about 5 m/s, creating the illusion of motion.

2. **RDM misalignment:** When the attacker signal has higher power than the legitimate one, the delayed peak becomes the strongest

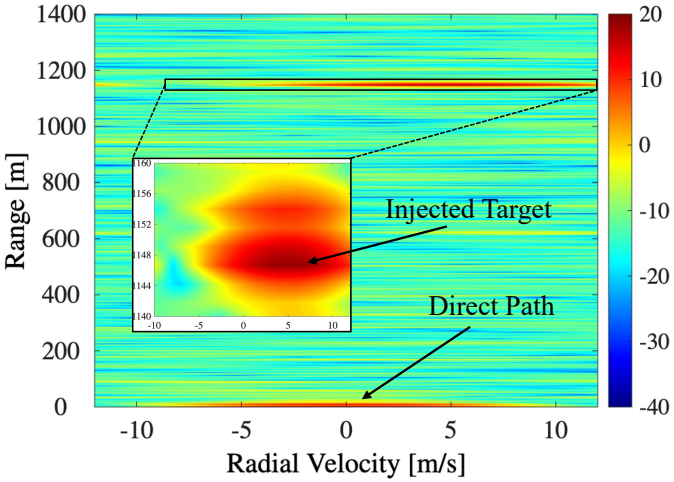

Figure 46: RDM under ghost-target injection. The replayed frame introduces a systematic velocity bias of $5m/s$, moving the true direct path and injecting a false echo.

in the PRS correlation and is mistakenly interpreted as the direct path, causing it to be wrongly aligned at zero delay. The Figure 47 shows the PRS correlation when the attacker transmits with a gain of 60 dB. As a result, the RDM is re-aligned to this delayed signal. This misalignment causes any real targets located at shorter ranges than the fake one to be masked or discarded, as their returns fall outside the expected range window relative to the (forged) direct path. Conversely, real targets located at greater ranges than the fake one are shifted in the RDM and appear closer than their actual positions. The re-alignment of the RDM also impacts the estimation of target velocities. When the attacker's signal is mistaken for the direct path, any frequency shift it introduces may be misinterpreted as the receiver's Carrier Frequency Offset (CFO) relative to the transmitter. Consequently, the Doppler processing is anchored to the attacker's frequency, which is now assumed to represent zero Doppler. This shift in reference leads to incorrect Doppler estimates for legitimate targets, whose velocities are measured relative to the

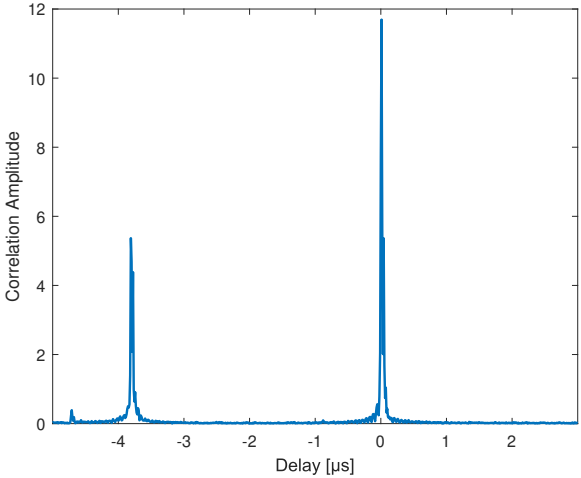

Figure 47: PRS correlation at 60 dB attacker gain. The replayed peak is now the strongest and is misidentified as the direct path, thereby obscuring any earlier legitimate targets.

attacker's signal rather than the true transmitter.

Uplink Scenario

We further extend the attack to the uplink, targeting the SRS in a TDD configuration. The attacker captures the legitimate SRS with a directional antenna and retransmits a delayed version using an omnidirectional antenna, incrementally raising the TX gain. The attack's impact on uplink sensing is evaluated by analyzing the CIR and Signal-to-Noise Ratio (SNR) of the SRS at the gNB.

As shown in Figure 48, the legitimate direct path appears as the central peak, while the attacker successfully injects a delayed peak corresponding to the malicious path with a gain of 44 dB. At this point, the SNR of the SRS is 10.9 dB.

As the attacker's gain increases to 48 dB (Figure 49), the SNR drops significantly to -7.1 dB, and the legitimate peak is no longer centered.

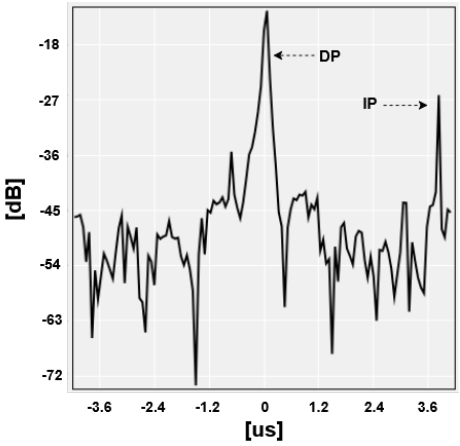

Figure 48: SRS CIR at the gNB with low attacker gain. The CIR window shows both the legitimate direct path (DP) peak and the delayed malicious injected path (IP) peak.

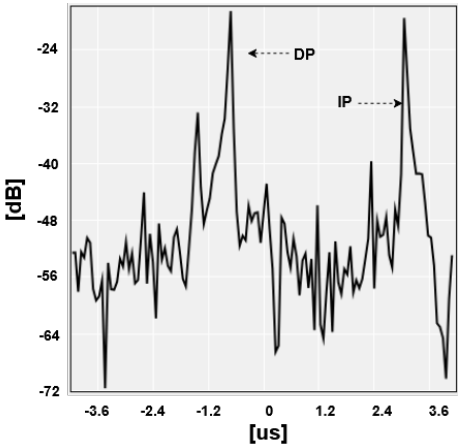

Figure 49: SRS CIR at the gNB. The CIR window shows both the legitimate direct path (DP) peak and the delayed malicious injected path (IP) peak.

Finally, in Figure 50, with a gain of 52 dB, the attacker's peak becomes dominant, and the gNB resynchronizes on it. The SNR in this case

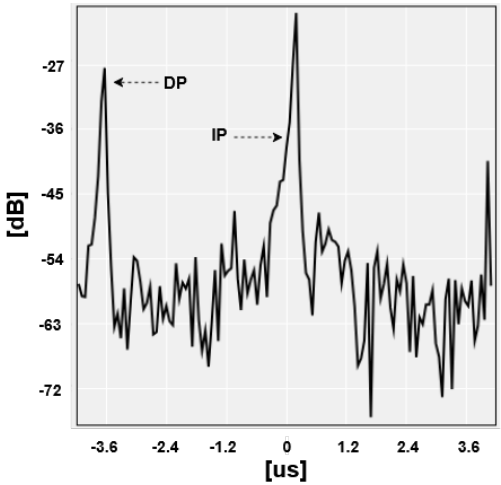

Figure 50: SRS CIR at the gNB with high attacker gain. The CIR window shows both the legitimate direct path (DP) peak and the delayed malicious injected path (IP) peak.

slightly recovers to 0.4 dB. The time offset between the peaks matches the configured delay, i.e. approx. $4\,\mu$s delay, confirming the attack's precision and its potential to compromise both communication and sensing integrity in integrated systems.

5.6 Discussion

This work represents an important step forward in understanding the practical implications of meaconing attacks in 5G systems; however, it should be regarded as a starting point for a broader investigation into the resilience of 5G positioning systems.

First, as already mentioned in the previous chapters, robust countermeasures must be developed to detect and defend against meaconing attacks, also leveraging metrics derived from communication signals. For example, a simple change detection method using a metric like SINR would be sufficient to identify a baseline attack.

However, it is crucial to note that defensive strategies should also account for the possibility that attacks may become *significantly more sophisticated* than the simple delayed and amplified retransmissions demonstrated in this work. Such attacks may employ programmable delays and gains to fine-tune the retransmission of signals, and they may even manipulate channel characteristics to make frame superposition less detectable, potentially making the attack harder to identify and mitigate.

Chapter 6

Conclusion

This thesis addresses the resilience of 5G positioning along three complementary contributions: an optimization framework, physical-layer security, and experimental validation.

The first contribution investigates the localization process not merely as a challenge of accuracy or latency, but as a multi-objective optimization problem that also considers resilience and resource efficiency. In particular, resilience and security take on an increasingly central role, given the critical applications that rely on secure and reliable positioning services. Building on this, the contributions of this work continue focusing on positioning security. We include a detailed overview of potential threats that can be carried out in 5G networks and analyze both insider and third-party attacks, distinguishing between high-level threats and those at the physical layer, where the attack surface is broader and the potential impact is more severe. Among these, particular attention is devoted to physical-layer spoofing attacks that target timing measurements. Such attacks cause a significant degradation of positioning performance, exceeding the limits defined by the required performance service levels. To support this analysis, we propose a threat model and develop two complementary detection strategies: the first exploits intrinsic signal properties, and the second leverages machine-learning techniques, in particular Gaussian Mixture Model, with the latter method

providing further gains in robustness. Although research on the security of 5G positioning is gradually gaining attention in the literature, experimental implementations of attacks and corresponding countermeasures remain inadequate. To the best of our knowledge, this thesis presents the first demonstration of a meaconing attack implemented on a replay attack on a fully 5G frame using a dedicated testbed composed of end-to-end 5G system. The results show that timing measurements can be effectively tampered with, while ongoing communication remains operational, although with a significant degradation in quality. This outcome demonstrates that such an attack can be conducted in a stealthy manner, without resulting in a denial-of-service. These findings emphasize the urgent need for robust and integrated detection methods to safeguard the resilience of 5G positioning systems. Looking ahead, the threats analyzed in this work have implications beyond 5G positioning, particularly in the emerging Integrated Sensing and Communication paradigm as preliminary results demonstrate. Indeed, recent studies have demonstrated the feasibility of similar attacks within the Integrated Sensing and Communication framework, leading to incorrect estimations of the number of targets, as well as erroneous range and Doppler measurements in both monostatic and bistatic radar scenarios. These attacks can leave the communication service unaffected, thereby maintaining stealth while compromising sensing performance.

In conclusion, this thesis confirms that resilience and security are not secondary features, but fundamental requirements for critical applications. Positioning systems, on which these applications rely, must ensure reliability even under challenging conditions and potential intentional attacks, highlighting that robustness and trustworthiness are essential for their proper functioning and safe deployment in real-world scenarios.

Bibliography

[1] S. Dwivedi, R. Shreevastav, F. Munier, *et al.*, "Positioning in 5G Networks", *IEEE Communications Magazine*, vol. 59, no. 11, pp. 38–44, 2021. DOI: 10.1109/MCOM.011.2100091.

[2] P. Hammarberg, J. Vinogradova, G. Fodor, R. Shreevastav, S. Dwivedi, and F. Gunnarsson, "Architecture, Protocols, and Algorithms for Location-Aware Services in Beyond 5G Networks", *IEEE Commun. Standards Mag.*, vol. 6, no. 4, pp. 88–95, Dec. 2022.

[3] S. Bartoletti and N. Blefari-Melazzi, *Positioning and Location-based Analytics in 5G and Beyond*, first. United Kingdom: Wiley-IEEE Press, 2024.

[4] X. Li, M. Ge, X. Dai, *et al.*, "Accuracy and reliability of multi-GNSS real-time precise positioning: GPS, GLONASS, BeiDou, and Galileo", *Journal of Geodesy*, vol. 89, Mar. 2015. DOI: 10.1007/s00190-015-0802-8.

[5] A. Zaidi and M. Suddle, "Global Navigation Satellite Systems: A Survey", in *2006 International Conference on Advances in Space Technologies*, 2006, pp. 84–87. DOI: 10.1109/ICAST.2006.313803.

[6] ETSI, "Satellite Earth Stations and Systems (SES); GNSS based location systems; Part 3: Performance requirements", European Telecommunications Standards Institute (ETSI), Technical Report (TR) 103.246-3, Oct. 2020, 1.3.1.

[7] M. Lenhart, M. Spanghero, and P. Papadimitratos, "Relay/replay attacks on GNSS signals", in *14th ACM Conf. on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '21, 2021.

[8] 3GPP, "5G System (5GS) Location Services (LCS); Stage 2", 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 23.273, Dec. 2023, 18.4.0.

[9] J. Li, K. K. Nagalapur, E. Stare, *et al.*, "5G New Radio for public safety mission critical communications", *IEEE Commun. Standards Mag.*, vol. 6, no. 4, pp. 48–55, Dec. 2022.

[10] S. Bartoletti, H. Wymeersch, T. Mach, *et al.*, "Positioning and Sensing for Vehicular Safety Applications in 5G and Beyond", *IEEE Communications Magazine*, vol. 59, no. 11, pp. 15–21, Nov. 2021.

[11] N. Decarli, A. Guerra, C. Giovannetti, F. Guidi, and B. M. Masini, "V2X Sidelink Localization of Connected Automated Vehicles", *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 1, pp. 120–133, 2024. DOI: 10.1109/JSAC.2023.3322853.

[12] M. Singh, M. Roeschlin, A. Ranganathan, and S. Capkun, "V-Range: Enabling Secure Ranging in 5G Wireless Networks", in *NDSS*, 2022.

[13] K. Gao, H. Wang, H. Lv, and P. Gao, "Your Locations May Be Lies: Selective-PRS-Spoofing Attacks and Defence on 5G NR Positioning Systems", in *IEEE INFOCOM 2023-IEEE Conference on Computer Communications*, IEEE, 2023, pp. 1–10.

[14] K. Gao, H. Wang, and H. Lv, "Surgical Strike on 5G Positioning: Selective-PRS-Spoofing Attacks and Its Defence", *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 10, pp. 2922–2937, 2024. DOI: 10.1109/JSAC.2024.3414592.

[15] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim, and Y. Kim, "Hiding in plain signal: Physical signal overshadowing attack on LTE", in *USENIX Security Sympo. (USENIX Security 19)*, Santa Clara, CA, Aug. 2019, pp. 55–72.

[16] Y. Li, S. Liu, Z. Yan, and R. H. Deng, "Secure 5G Positioning With Truth Discovery, Attack Detection, and Tracing", *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22 220–22 229, Nov. 2022.

[17] G. Focarelli, S. Zanini, I. Palamà, G. Bianchi, and S. Bartoletti, "Positioning Security in 5G and Beyond: Model and Detection of Physical Layer Threats", *IEEE Transactions on Wireless Communications*, vol. 25, pp. 1048–1061, 2026. DOI: 10.1109/TWC.2025.3588718.

[18] A. K. Dutta and M. Singh, "Invited Paper: Challenges and Opportunities in Enabling Secure 5G Positioning", in *2023 15th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, 2023, pp. 498–504. DOI: 10.1109/COMSNETS56262.2023.10041419.

[19] E. S. Lohan, A. Alén-Savikko, L. Chen, *et al.*, "5G positioning: Security and privacy aspects", *A Comprehensive Guide to 5G Security*, pp. 281–320, 2018.

[20] 3GPP, "Architectural Enhancements to support Ranging based services and Sidelink Positioning", 3rd Generation Partnership Project (3GPP), Technical specification (TS) 23.586, Sep. 2025, 18.7.0.

[21] M. Polese, L. Bonati, S. D'oro, S. Basagni, and T. Melodia, "Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges", *IEEE Communications Surveys & Tutorials*, 2023.

[22] 3GPP, "NG Radio Access Network (NG-RAN); Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN", 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.305, Sep. 2023, 17.6.0.

[23] S. Bartoletti, S. Mazuelas, A. Conti, and M. Z. Win, "Efficient Localization via Soft Information With Generic Sensing Measurements", *IEEE Transactions on Wireless Communications*, vol. 24, no. 7, pp. 5400–5414, 2025. DOI: 10.1109/TWC.2025.3540081.

[24] 3GPP, "Service requirements for Integrated Sensing and Communication", 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 22.137, Mar. 2024, 19.1.0.

[25] 3GPP, "Study on Integrated Sensing and Communication", 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 22.837, Jun. 2024, 19.4.0.

[26] Wei, Zhiqing and Qu, Hanyang and Wang, Yuan and Yuan, Xin and Wu, Huici and Du, Ying and Han, Kaifeng and Zhang, Ning and Feng, Zhiyong, "Integrated sensing and communication signals toward 5G-A and 6G: A survey", *IEEE Internet of Things Journal*, vol. 10, no. 13, pp. 11 068–11 092, 2023.

[27] S. Zanini, L. Petrucci, I. Palamà, G. Bianchi, and S. Bartoletti, "Towards End-to-end Implementation of 5G Positioning with Off-the-shelf Devices", in *2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall)*, 2024, pp. 1–6. DOI: 10.1109/VTC2024-Fall63153.2024.10757829.

[28] L. Petrucci, S. Zanini, I. Palamà, N. B. Melazzi, and S. Bartoletti, "Localization in 5G and Beyond: A Multi-Objective Approach for Accuracy, Latency, and Resilience", *IEEE Transactions on Mobile Computing*, vol. 24, no. 12, pp. 12 771–12 783, 2025. DOI: 10.1109/TMC.2025.3588712.

[29] S. Zanini, S. Bartoletti, G. Focarelli, I. Palama, and G. Bianchi, "Location Security in 5G and Beyond: Potential Threats and Countermeasures", *IEEE Communications Magazine*, pp. 1–7, 2026. DOI: 10.1109/MCOM.001.2500274.

[30] G. Focarelli, S. Zanini, G. Bianchi, and S. Bartoletti, "Physical Layer Threats to 5G Positioning: Impact on TOA-Based Methods", in *2024 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2024, pp. 926–931. DOI: 10.1109/ICCWorkshops59551.2024.10615737.

[31] S. Zanini, G. Focarelli, I. Palamà, A. Rivitti, G. Bianchi, and S. Bartoletti, "Experimental Viability of Full-Frame 5G Meaconing Attacks", in *2025 IEEE Wireless Communications and Networking Conference (WCNC)*, 2025, pp. 1–3. DOI: 10.1109/WCNC61545.2025.10978169.

[32] G. Focarelli, S. Zanini, I. Palamà, A. Rivitti, S. Bartoletti, and G. Bianchi, "WIP: Parrots in the Air: Experimental Validation of Full-Frame Meaconing in 5G Systems", in *2025 IEEE 26th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2025, pp. 118–121. DOI: 10.1109/WoWMoM65615.2025.00028.

[33] I. Palamà, G. Focarelli, S. Zanini, G. Bianchi, and S. Bartoletti, "Blind Deception in ISAC via Full-Frame OFDM Replay", in *Proceedings of the ACM Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization*, 2025, pp. 25–32.

[34] O. Alliance, "O-RAN.WG1.Use-Cases-Analysis-Report-R003-v13.00 Technical Report O-RAN Work Group 1 (Use Cases and Overall Architecture) Use Cases Analysis Report", O-RAN Alliance, R003, Feb. 2024, v13.00.

[35] O.-R. Alliance, "O-RAN Work Group 1 (Use Cases and Overall Architecture) Use Cases Detailed Specification", O-RAN Alliance, R003, Feb. 2024, v13.00.

[36] 3GPP, " LTE Positioning Protocol (LPP)", 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 37.355, Sep. 2023, 17.6.0.

[37] 3GPP, "NG-RAN; NR Positioning Protocol A (NRPPa)", 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.455, Jun. 2023, 17.5.0.

[38] 3GPP, "Study on positioning use cases", 3rd Generation Partnership Project (3GPP), Technical report (TR) 22.872, Sep. 2018, 16.1.0.

[39] 3GPP, "Service requirements for the 5G system", 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 22.261, Sep. 2023, 19.4.0.

[40] 3GPP, "5G System; Location Management Services; Stage 3", 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 29.572, Jan. 2024, 18.4.0.

[41] 3GPP, "5G System; Access and Mobility Management Services; Stage 3", 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 29.518, Jan. 2024, 18.4.0.

[42] "Open5gs". (), [Online]. Available: https://open5gs.org (visited on 04/10/2024).

[43] "Free5GC". (), [Online]. Available: https://free5gc.org (visited on 04/10/2024).

[44] "OpenAirInterface Software Alliance." (), [Online]. Available: https://openairinterface.org (visited on 04/10/2024).

[45] "srsRAN Project". (), [Online]. Available: https://www.srsran.com (visited on 04/10/2024).

[46] "Amarisoft, LTE Software eNodeB and NR Software gNB; version 2024-04-10". (), [Online]. Available: https://tech-academy.amarisoft.com/lteenb.doc (visited on 04/10/2024).

[47] Ettus Research, National Instruments. "USRP X310". (), [Online]. Available: https://www.ettus.com/all-products/usrp-x310/ (visited on 04/10/2024).

[48] B. Coll-Perales, M. C. Lucas-Estañ, T. Shimizu, *et al.*, "End-to-End V2X Latency Modeling and Analysis in 5G Networks", *IEEE Transactions on Vehicular Technology*, vol. 72, no. 4, pp. 5094–5109, 2023. DOI: 10.1109/TVT.2022.3224614.

[49] 3GPP, "5G; NR; NR and NG-RAN Overall description; Stage-2", 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.300, Sep. 2025, 17.6.0.

[50] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, "A fast and elitist multiobjective genetic algorithm: NSGA-II", *IEEE Transactions on Evolutionary Computation*, vol. 6, no. 2, pp. 182–197, 2002. DOI: 10.1109/4235.996017.

[51] Q. Zhang and H. Li, "MOEA/D: A Multiobjective Evolutionary Algorithm Based on Decomposition", *IEEE Transactions on Evolutionary Computation*, vol. 11, no. 6, pp. 712–731, 2007. DOI: 10.1109/TEVC.2007.892759.

[52] M. M. Rahman, A. Siddika Arshi, M. M. Hasan, S. Farzana Mishu, H. Shahriar, and F. Wu, "Security Risk and Attacks in AI: A Survey of Security and Privacy", in *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2023, pp. 1834–1839. DOI: 10.1109/COMPSAC57700.2023.00284.

[53] 3GPP, "Study on NR positioning enhancements", 3rd Generation Partnership Project (3GPP), Technical Report (TR) 38.857, Mar. 2021, 17.0.0.

[54] R. Fletcher and C. M. Reeves, "Function minimization by conjugate gradients", *The computer journal*, vol. 7, no. 2, pp. 149–154, 1964.

[55] C. Zhu, R. H. Byrd, P. Lu, and J. Nocedal, "Algorithm 778: L-BFGS-B: Fortran subroutines for large-scale bound-constrained optimization", *ACM Trans. Math. Softw.*, vol. 23, no. 4, pp. 550–560, Dec. 1997, ISSN: 0098-3500. DOI: 10.1145/279232.279236. [Online]. Available: https://doi.org/10.1145/279232.279236.

[56] C. W. Royer, M. O'Neill, and S. J. Wright, "A Newton-CG algorithm with complexity guarantees for smooth unconstrained optimization", *Mathematical Programming*, vol. 180, pp. 451–488, 2020.

[57] 3GPP, "NR; Physical channels and modulation", 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.211, Sep. 2023, 18.0.0.

[58] G. Van Rossum and F. L. Drake, *Python 3 Reference Manual*. Scotts Valley, CA: CreateSpace, 2009, ISBN: 1441412697.

[59] 3GPP, "Study on channel model for frequencies from 0.5 to 100 GHz", 3rd Generation Partnership Project (3GPP), Technical report (TR) 38.901, Apr. 2024, 18.0.0.

[60] P. Virtanen, R. Gommers, T. E. Oliphant, *et al.*, "SciPy 1.0: Fundamental Algorithms for Scientific Computing in Python", *Nature Methods*, vol. 17, pp. 261–272, 2020. DOI: 10.1038/s41592-019-0686-2.

[61] "LMF". (), [Online]. Available: https://github.com/LucaPetrucci/LMF (visited on 04/22/2024).

[62] P. Ngatchou, A. Zarei, and A. El-Sharkawi, "Pareto multi objective optimization", in *Proceedings of the 13th International Conference on, Intelligent Systems Application to Power Systems*, 2005, pp. 84–91.

[63] M. A. Ramirez, S.-K. Kim, H. A. Hamadi, *et al.*, "Poisoning attacks and defenses on artificial intelligence: A survey", *arXiv preprint arXiv:2202.10276*, 2022.

[64] I. Guvenc and C.-C. Chong, "A Survey on TOA Based Wireless Localization and NLOS Mitigation Techniques", *IEEE Communications Surveys & Tutorials*, vol. 11, no. 3, pp. 107–124, 2009. DOI: 10.1109/SURV.2009.090308.

[65] A. Conti, F. Morselli, Z. Liu, *et al.*, "Location Awareness in Beyond 5G Networks", *IEEE Communications Magazine*, vol. 59, no. 11, pp. 22–27, 2021. DOI: 10.1109/MCOM.221.2100359.

[66] H. L. V. Trees, *Detection, Estimation, and Modulation Theory*, first. New York, NY 10158-0012: John Wiley & Sons, Inc., 1968.

[67] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Upper Saddle River, NJ: Prentice-Hall, 1993.

[68] D. Dardari, C.-C. Chong, and M. Win, "Threshold-Based Time-of-Arrival Estimators in UWB Dense Multipath Channels", *IEEE Transactions on Communications*, vol. 56, no. 8, pp. 1366–1378, 2008. DOI: 10.1109/TCOMM.2008.050551.

[69] D. Dardari, A. Conti, U. Ferner, A. Giorgetti, and M. Z. Win, "Ranging With Ultrawide Bandwidth Signals in Multipath Environments", *Proceedings of the IEEE*, vol. 97, no. 2, pp. 404–426, 2009. DOI: 10.1109/JPROC.2008.2008846.

[70] L. Bai, C. Sun, A. G. Dempster, H. Zhao, J. W. Cheong, and W. Feng, "GNSS-5G Hybrid Positioning Based on Multi-Rate Measurements Fusion and Proactive Measurement Uncertainty Prediction", *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–15, 2022. DOI: 10.1109/TIM.2022.3154821.

[71] Y. Arjoune and S. Faruque, "Smart jamming attacks in 5G new radio: A review", in *Annual Computing and Commun. Workshop and Conf. (CCWC)*, Las Vegas, NV, USA, Jan. 2020, pp. 1010–1015.

[72] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, P. M. Kintner, *et al.*, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer", in *Proc. Int. Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS)*, Savanna, GA, USA, Sep. 2008, pp. 2314–2325.

[73] V. Hamici-Aubert, J. Saint-Martin, R. E. Navas, G. Z. Papadopoulos, G. Doyen, and X. Lagrange, "Leveraging Overshadowing for Time-Delay Attacks in 4G/5G Cellular Networks: An Empirical Assessment", in *The 19th International Conference on Availability, Reliability and Security (ARES 2024)*, 2024.

[74] K. Whitehouse, A. Woo, F. Jiang, J. Polastre, and D. Culler, "Exploiting the capture effect for collision detection and recovery", in *IEEE Workshop on Embedded Networked Sensors (EmNetS-II)*, IEEE, 2005.

[75] M. Meghdadi, S. Ozdemir, and I. Güler, "A survey of wormhole-based attacks and their countermeasures in wireless sensor networks", *IETE technical review*, vol. 28, no. 2, pp. 89–102, Sep. 2014.

[76] N. Zhu, J. Marais, D. Bétaille, and M. Berbineau, "GNSS Position Integrity in Urban Environments: A Review of Literature", *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 9, pp. 2762–2778, 2018. DOI: 10.1109/TITS.2017.2766768.

[77] L. Ding, G. Seco-Granados, H. Kim, *et al.*, "Bayesian integrity monitoring for cellular positioning—a simplified case study", in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*, IEEE, 2023, pp. 1050–1056.

[78] 3GPP, "NR; Physical layer procedures for data", 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.214, Sep. 2023, 18.0.0.

[79] B. Hu, H. Tian, W. Ni, S. Fan, W. Ni, and E. Hossain, "Multipath Identification, User Localization, and Environment Mapping in Radio SLAM", *IEEE Transactions on Communications*, vol. 72, no. 10, pp. 6457–6473, 2024. DOI: 10.1109/TCOMM.2024.3393977.

[80] I. Guvenc, C.-C. Chong, and F. Watanabe, "NLOS Identification and Mitigation for UWB Localization Systems", in *2007 IEEE Wireless Communications and Networking Conference*, 2007, pp. 1571–1576. DOI: 10.1109/WCNC.2007.296.

[81] I. Güvenç, C.-C. Chong, F. Watanabe, and H. Inamura, "NLOS identification and weighted least-squares localization for UWB systems using multipath channel statistics", *EURASIP J. Adv. Signal Process*, vol. 2008, Jan. 2008, ISSN: 1110-8657. DOI: 10.1155/2008/271984. [Online]. Available: https://doi.org/10.1155/2008/271984.

[82] B. C. Tedeschini, G. Kwon, M. Nicoli, and M. Z. Win, "Real-Time Bayesian Neural Networks for 6G Cooperative Positioning and Tracking", *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 9, pp. 2322–2338, 2024.

[83] B. C. Tedeschini, M. Nicoli, and M. Z. Win, "On the Latent Space of mmWave MIMO Channels for NLOS Identification in 5G-Advanced Systems", *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 6, pp. 1655–1669, 2023.

[84] D. A. Reynolds *et al.*, "Gaussian mixture models", *Encyclopedia of biometrics*, vol. 741, no. 659-663, 2009.

[85] Z. Feng, C. K. Seow, and Q. Cao, "GNSS Anti-spoofing Detection based on Gaussian Mixture Model Machine Learning", in *2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC)*, IEEE, 2022, pp. 3334–3339.

[86] B. Chettri and B. L. Sturm, "A deeper look at Gaussian mixture model based anti-spoofing systems", in *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, IEEE, 2018, pp. 5159–5163.

[87] X. Qiu, T. Jiang, S. Wu, and M. Hayes, "Physical layer authentication enhancement using a Gaussian mixture model", *IEEE Access*, vol. 6, pp. 53 583–53 592, 2018.

[88] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength", in *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, IEEE, 2008, pp. 1768–1776.

[89] A. P. Dempster, N. M. Laird, and D. B. Rubin, "Maximum likelihood from incomplete data via the EM algorithm", *Journal of the royal statistical society: series B (methodological)*, vol. 39, no. 1, pp. 1–22, 1977.

[90] A. Xhafa, J. A. del Peral-Rosado, J. A. López-Salcedo, and G. Seco-Granados, "Evaluation of 5G Positioning Performance Based on UTDoA, AoA and Base-Station Selective Exclusion", *Sensors*, vol. 22, no. 1, 2022, ISSN: 1424-8220. DOI: 10.3390/s22010101. [Online]. Available: https://www.mdpi.com/1424-8220/22/1/101.

[91] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "Gps vulnerability to spoofing threats and a review of antispoofing techniques", *International Journal of Navigation and Observation*, vol. 2012, no. 1, p. 127 072, 2012. DOI: https://doi.org/10.1155/2012/127072. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1155/2012/127072. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1155/2012/127072.

[92] F. Rothmaier and J. A. Del Peral Rosado, "A Parametric Study on Autonomous Integrity Monitoring using non-GNSS Signals", in *2023 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, 2023, pp. 1154–1161. DOI: 10.1109/PLANS53410.2023.10139988.

[93] J. Khalife, M. Maaref, and Z. M. Kassas, "Opportunistic Autonomous Integrity Monitoring for Enhanced UAV Safety", *IEEE Aerospace and Electronic Systems Magazine*, vol. 38, no. 5, pp. 34–44, 2023. DOI: 10.1109/MAES.2022.3178664.

[94] M. Jia, J. Khalife, and Z. M. Kassas, "Performance Analysis of Opportunistic ARAIM for Navigation With GNSS Signals Fused With Terrestrial Signals of Opportunity", *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 10, pp. 10 587–10 602, 2023. DOI: 10.1109/TITS.2023.3277393.

[95] F. Munier, Z. Xiong, R. Shreevastav, *et al.*, "Positioning of RedCap Devices in 5G Networks", *IEEE Commun. Mag.*, vol. 62, no. 8, pp. 110–116, 2024.

[96] M. Coulon, A. Chabory, A. Garcia-Pena, *et al.*, "Characterization of Meaconing and its Impact on GNSS Receivers", in *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, 2020, pp. 3713–3737.

[97] R. Blum, D. Dötterböck, and T. Pany, "Investigation of the vulnerability of mobile networks against spoofing attacks on their GNSS timing-receiver and developing a meaconing protection", in *Proceedings of the 2019 International Technical Meeting of The Institute of Navigation*, 2019, pp. 345–362.

[98] E. Axell, M. Alexandersson, and T. Lindgren, "Results on GNSS meaconing detection with multiple COTS receivers", in *2015 Int. Conf. on Localization and GNSS (ICL-GNSS)*, 2015.

[99] L. Pucci, E. Paolini, and A. Giorgetti, "System-level analysis of joint sensing and communication based on 5G new radio", *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 7, pp. 2043–2055, 2022.

[100] E. Research, *Usrp hardware driver (uhd™) software*, `https://github.com/EttusResearch/uhd`.

[101] Aaronia AG, *OmniLOG® 70600*, `https://aaronia.com/en/shop/antennas-sensors/biconical-antenna/omnidirectional-antenna-6ghz`,

[102] Ettus Research, National Instruments, *Usrp x410*, `https://www.ettus.com/all-products/usrp-x410/`.

[103] Aaronia AG, *HyperLOG® 6080*, `https://aaronia.com/en/shop/log-per-antenne-hyperlog6080`,

[104] Keysight, *Spectrum Analyzer MXA N9021B*, `https://www.keysight.com/us/en/product/N9021B/n9021b-mxa-signal-analyzer-multi-touch-10-hz-50-ghz.html`,

[105] QTRUN Technologies, *Network signal guru*, 2024. [Online]. Available: `https://play.google.com/store/apps/details?id=com.qtrun.QuickTest`.

[106] Parizene, *Netmonitor: 5G, Cell & WiFi*, 2024. [Online]. Available: `https://play.google.com/store/apps/details?id=com.parizene.netmonitor`.