UNICA

UNIVERSITÀ
DEGLI STUDI
DI CAGLIARI

Ph.D. DEGREE IN
ELECTRONIC AND COMPUTER ENGINEERING

Cycle XXXVIII

TITLE OF THE Ph.D. THESIS

Energy-Efficient and Trustworthy GPS-free RSS-based Location-Based Services for Next-Generation IoT

Scientific Disciplinary Sector(s)

ING-INF/03

Ph.D. Student:	Giovanni Pettorru
Supervisor	Virginia Pilloni
Co-Supervisor	Marco Martalò

Final exam. Academic Year 2024/2025
Thesis defence session: February 2026

Contents

Introduction

Scope

Over the past decade, the rapid expansion of the Internet of Things (IoT) has profoundly reshaped the digital landscape, connecting billions of devices capable of sensing, processing, and interacting with their environments. Within this ecosystem, Location-Based Services (LBS) have emerged as a cornerstone technology, enabling context-aware applications in domains as diverse as industrial automation, healthcare, smart cities, and precision agriculture. In these scenarios, the ability to determine the precise location of a device is no longer merely an added feature but a fundamental requirement for operational efficiency and decision-making. Consequently, the scope of this research is specifically centered on enabling robust and trustworthy positioning in resource-constrained IoT environments, focusing on methodologies that operate independently of satellite infrastructures.

Challenges

Despite the ubiquity of IoT, delivering LBS that are at once energy-efficient, accurate, and trustworthy remains an open challenge, particularly in dynamic and resource-constrained environments. Conventional positioning systems, such as the Global Positioning System (GPS), provide high accuracy under open-sky conditions but fall short in IoT deployments due to their high energy demands, unreliable indoor performance, and vulnerability to interference. These limitations have stimulated extensive research on GPS-free localization techniques that exploit existing wireless infrastructures, including WiFi, Bluetooth Low Energy (BLE), and Long-Range (LoRa). Among these, Received Signal Strength (RSS)-based approaches stand out for their sim-

plicity, cost-effectiveness, and compatibility with commodity hardware. However, their reliance on signal intensity makes them inherently fragile: their performance is strongly affected by environmental variability, multipath propagation, and shadowing. Furthermore, the openness of the wireless medium exposes these systems to malicious threats, such as jamming and signal spoofing, which can severely compromise the integrity of the location data.

Motivation

The motivation behind this research stems from the critical gap between the theoretical potential of RSS-based positioning and its practical reliability in hostile or cluttered environments. While low-cost and energy-efficient, current GPS-free solutions often lack the robustness required for mission-critical applications where a wrong position estimate can lead to economic loss or safety risks. There is a pressing need to move beyond simple proximity detection toward a holistic localization framework that not only estimates position but also quantifies the trustworthiness of that estimate, resiliently handling both natural signal degradation and intentional adversarial attacks.

Objectives

The primary objective of this doctoral thesis is to design, implement, and validate a comprehensive framework for energy-efficient and trustworthy GPS-free localization in IoT scenarios. To achieve this, the research pursues the following specific goals:

- To develop hybrid positioning algorithms that mitigate the individual weaknesses of standard range-based and range-free techniques.
- To enhance robust accuracy through multi-interface data fusion, leveraging the diversity of heterogeneous wireless technologies.
- To define a novel metric capable of dynamically assessing the reliability of position estimates based on geometric and environmental factors.

- To design security mechanisms that ensure system availability and integrity even in the presence of jamming or byzantine attacks.
- To demonstrate the practical viability of these solutions through rigorous validation and a real-world case study in a strategic sector.

Main Contributions

In fulfillment of these objectives, the thesis makes the following key scientific and technical contributions:

- **Hybrid GPS-free localization algorithms** that combine range-free fingerprinting and range-based multilateration to improve accuracy and resilience when anchor availability varies.
- **Multi-interface data-fusion methods** that exploit simultaneous RSS measurements from different wireless technologies, increasing robustness to interference and fading.
- **A reliability index** that quantifies the trustworthiness of each location estimate by jointly considering geometry, channel conditions, and malicious activity.
- **Security mechanisms** featuring an enhanced Secure Weighted Least Squares (SWLS)-based algorithm with adaptive thresholding. This mechanism discriminates between heavily jammed anchors and partially affected ones, preserving system availability and accuracy even under strong interference.
- **Experimental validation** of each solution through extensive simulations and, where applicable, field tests, validating the proposed solutions in terms of accuracy and robustness.
- **Application to Smart Agriculture**, showing how the trustworthy LBS framework can create tangible value in a strategic sector where sustainability, tradition, and technological innovation converge, demonstrating the potential impact of advanced IoT-based LBS beyond purely academic contexts.

Thesis Organization

The remainder of this thesis is organized as follows:

- **Chapter 1** reviews the state of the art in GPS-free localization, covering range-based and range-free methods, data-fusion approaches, and security issues.
- **Chapter 2** introduces the reference scenario and the designed architecture, defining the system model, anchor–target interactions, and reliability challenges in adversarial IoT environments.
- **Chapter 3** presents the proposed contributions. It includes hybrid algorithms based on multi-interface data fusion, joint multilateration–fingerprinting techniques, the reliability index for quantifying trust in localization, and security mechanisms to detect and mitigate byzantine and jamming attacks.
- **Chapter 4** describes the methodology adopted for performance evaluation, including simulation and real-world experiments. The results demonstrate the accuracy, robustness, and security of the proposed methods and benchmark them against conventional approaches.
- **Chapter 5** provides a case study in smart agriculture, showcasing the added value of the trustworthy LBS framework in a real-world strategic domain.
- **Chapter 6** concludes the thesis by summarizing the main findings and contributions, and outlines open challenges and future research directions.

This structure follows a logical progression from background and system definition, through methodological contributions and their validation, to a concrete real-world application, ensuring a comprehensive and systematic presentation of the work.

Chapter 1

Background and Related Work

1.1 Location-Based Services in the Internet of Things Era

The IoT has rapidly transformed the way humans interact with their environment and reshaped many aspects of daily life. Its influence spans a wide spectrum of domains, from smart homes and healthcare to industrial automation and transportation, where IoT solutions increasingly serve as critical enablers of efficiency and innovation [1]. To appreciate the scale of this transformation, consider that there are currently an estimated 15 billion connected devices worldwide, a figure expected to rise steadily in the coming years [2]. The growing promise of IoT in specific applications such as home automation, smart agriculture, and Industry 4.0 is largely attributed to the advances in Machine-to-Machine (M2M) communication [3]. This paradigm shift, moving away from the traditional Machine-to-Human (M2H) interactions that characterized the early Internet, allows networks of heterogeneous devices to operate autonomously with minimal human involvement.

In this evolving landscape, where devices increasingly require less human interaction, the significance of context awareness becomes paramount. The term context awareness, which originated more than two decades ago, can be defined in the context of IoT as the ability of devices to collect and use data about their surroundings, enabling them to make more informed and context-relevant decisions [4]. The data collected, referred to as contextual information, encompasses a wide range of categories, including location, timestamp, user behaviors, proximity to other devices, battery level, and various other factors.

Among these, one of the most critical and valuable forms of contextual information is location, which has given rise to a distinct class of services known as LBS [5]. By leveraging the precise position of devices, users, or assets, LBS enables context-aware applications that dynamically adapt to spatial and temporal factors. In the IoT domain, numerous use cases have been explored in the literature: from navigation guidance for warehouse robots [6], to location-based marketing [7], and services for safeguarding elderly people through precise activity and movement tracking in their homes [8].

The impact of LBS, however, extends well beyond these examples. They are increasingly essential across sectors such as smart cities, smart industries, healthcare, agriculture, and transportation. In logistics and mobility, LBS optimizes routes, manages fleets, and tracks vehicles and shipments in real time, improving efficiency, reducing fuel consumption, and enhancing delivery times. In healthcare, they support patient and staff tracking, resource allocation, and faster emergency responses. Retailers use them for inventory management, location-based promotions, and personalized customer experiences. Industrial contexts benefit from asset tracking, warehouse automation, and improved supply chain management. In smart cities, LBS optimizes parking, waste collection, energy monitoring, and traffic management, relying on IoT sensors to enable data-driven services that improve citizens' quality of life while reducing environmental impact [9].

Yet, as the use of LBS grows, so do the associated security and privacy challenges [10]. Location information is inherently sensitive, as it not only reveals the presence and movement of users or assets but also exposes the underlying infrastructure to threats such as spoofing, jamming, and data manipulation. In IoT scenarios, where devices are resource-constrained, often deployed in unprotected environments, and rely on shared wireless channels, the risks are even more pronounced. For these reasons, a secure-by-design approach has become imperative in the development of IoT systems and trustworthy LBS. This thesis is motivated precisely by these challenges: it seeks to investigate how localization methods can be made not only more accurate and energy-efficient, but also resilient against adversarial behaviors.

1.2 Overview of GPS-Free Positioning Methods

The GPS has long been the most widely used technology for positioning and navigation, offering global coverage and reliable accuracy in outdoor environments. Its pervasiveness has made it the reference solution for a wide range of applications, from consumer navigation to logistics and emergency services. However, despite its strengths, GPS presents several drawbacks that limit its suitability in IoT scenarios [11]. Among the most critical issues are its relatively high energy consumption, the need for constant satellite communication, and reduced performance in challenging environments such as indoors, urban canyons, or dense industrial facilities [12, 13]. These limitations are particularly problematic in IoT contexts, where devices are typically resource-constrained and designed to operate under strict energy and sustainability requirements.

To address these challenges, research efforts have increasingly turned toward GPS-free positioning systems, which utilize alternative localization approaches that leverage local wireless signals, environmental characteristics, and sensor data to provide accurate, energy-efficient, and context-aware location information, even in scenarios where satellite-based solutions are impractical or unreliable. In the context of IoT, these techniques are generally classified into three main groups, as reported in Figure 1.1 (page 11): radio range-free methods, radio range-based methods, and hybrid approaches [14]. The following subsections introduce these categories, outlining their underlying principles and discussing their applicability within IoT environments.

1.2.1 Radio Range-Free Techniques

Fingerprinting—Fingerprinting represents the most widely adopted radio range-free localization technique, as evidenced by the extensive body of work available in the literature. As depicted in Figure 1.2 (page 12), the method is typically divided into two phases. During the offline phase, Channel State Information (CSI) and/or RSS measurements are collected at predetermined reference points throughout the environment to construct a fingerprint database. In the subsequent online phase, the target device acquires new RSS measurements while moving within the scenario; these measurements are then matched against the database entries

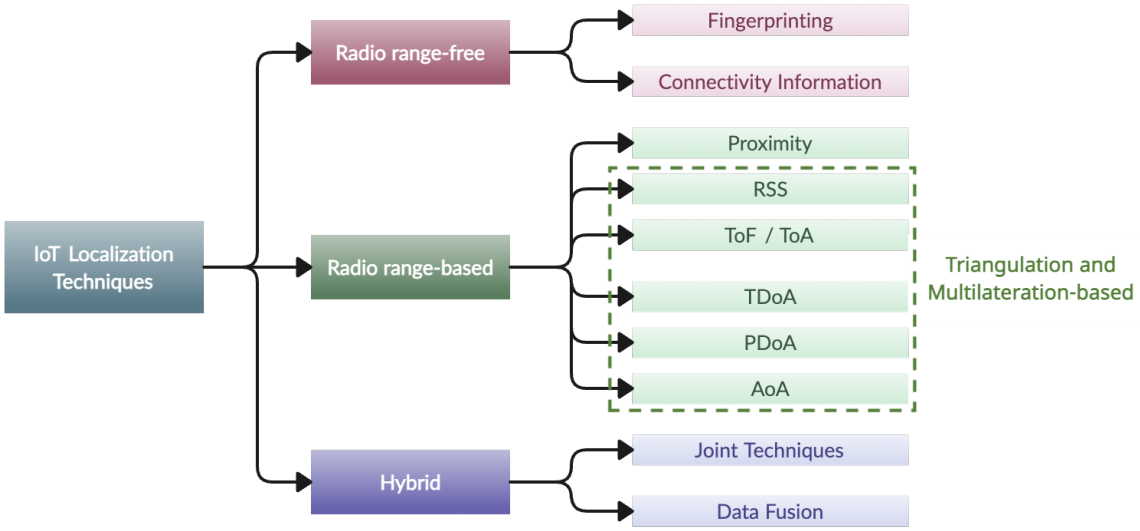


Figure 1.1: Taxonomy of IoT localization techniques [14].

to infer the most probable location of the device [15].

This method eliminates the need for complex position estimation calculations. However, its reliance on the offline phase limits its suitability for dynamic environments, as significant environmental changes necessitate repeating the process. In [16], the authors present a WiFi fingerprinting-based approach for indoor scenarios. Their method addresses offline phase challenges by implementing a dynamic radio map update system, which removes the need for costly and time-consuming manual surveys.

This localization technique increasingly relies on Machine Learning (ML) to achieve accurate position estimation. Models such as Random Forest (RF), k-Nearest Neighbors (kNN), Long Short-Term Memory (LSTM), and Convolutional Neural Networks (CNN) are widely applied, each offering distinct advantages. Building on these methods, [17] employs Particle Swarm Optimization (PSO) for fingerprinting, achieving higher accuracy than RF. In the same vein, [18] proposes EdgeLoc, a WiFi system that leverages Capsule Neural Networks (CapsNet) and an edge–IoT framework to mitigate hardware variability and multipath effects, enabling reliable real-time localization. Heterogeneous infrastructures are addressed in [19], where the DELTA ML model integrates Raspberry Pi, Arduino, ZigBee, BLE, and 5G into a multi-layer radiomap, refining both two-dimensional (2D) and three-dimensional (3D) positioning through recursive

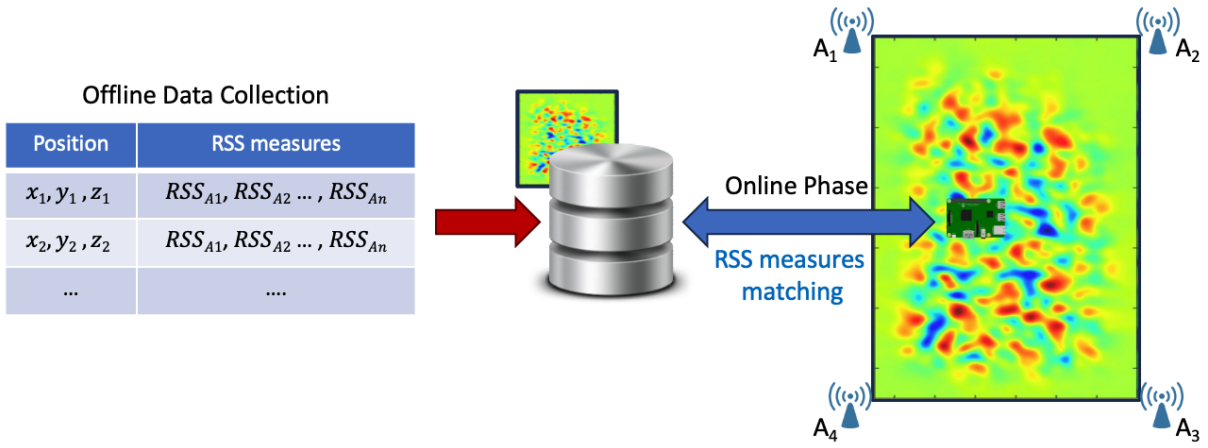


Figure 1.2: Fingerprinting-based localization.

predictions. Finally, [20, 21] demonstrate the effectiveness of Deep Learning (DL) approaches, including Artificial Neural Networks (ANN), LSTM, and CNN, consistently outperforming traditional algorithms across open datasets and real-world deployments.

Connectivity Information—Range-free localization algorithms based on connectivity information are attractive for IoT due to their low complexity and cost-effectiveness. However, they provide coarse granularity, since position estimates depend on hop counts rather than physical distance. Unlike fingerprinting, where granularity depends on the density of the radio map, connectivity-based methods generally achieve lower accuracy [22]. A widely adopted approach is Distance Vector-Hop (DV-Hop), which propagates location information by incrementing hop counts from anchor nodes. Each node records the minimum hop count to anchors, which then estimates the average hop distance and broadcasts it. Target nodes use these values to refine their position estimates [23]. A representative topology is shown in Figure 1.3 (page 13).

Recent research has focused on improving DV-Hop performance. In [24], error correction metrics are integrated to reduce distance estimation errors. Energy efficiency is addressed in [25] through a three-step method combining improved MAC discovery, node categorization, and error correction. In [26], DV-Hop is enhanced with PSO, yielding higher accuracy than the baseline. Similarly, [27] integrates DV-Hop with Chicken Swarm Optimization (CSO), further improving efficiency and accuracy over PSO-based solutions. Finally, [28] proposes a centralized algorithm optimizing accuracy via connectivity constraints, and a distributed, low-complexity variant based on two-hop neighborhoods.

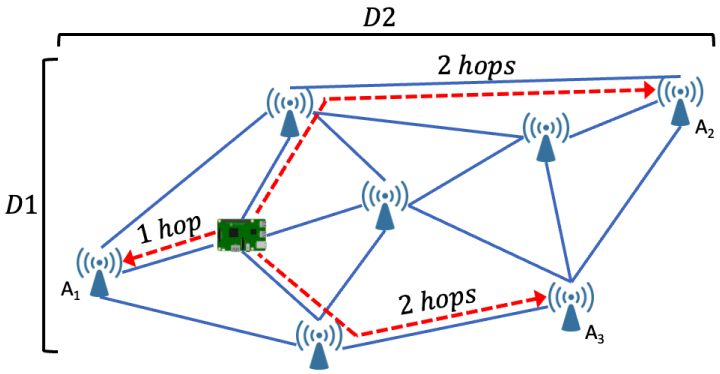


Figure 1.3: DV-Hop localization topology.

1.2.2 Radio Range-Based Techniques

Proximity—This approach determines whether two devices are within a predefined range or directly connected, rather than computing exact distances. The target's location is typically inferred from the coordinates of the closest anchor node, as depicted in Figure 1.4 (page 14). Due to its conceptual simplicity and low demands on energy and computation, proximity-based localization is widely adopted in the literature [29], making it well-suited to IoT deployments where fine-grained positioning is not critical.

Several studies have explored different technologies to implement this approach. In [30], BLE beacons are assessed for indoor localization by comparing popular devices and evaluating their power consumption and proximity accuracy. The same technology is applied in [31] to enhance visitor experience in a museum environment. Sigfox-based solutions are presented in [32], starting with a simple method that estimates position from the strongest base station and evolving to cluster-based algorithms that improve accuracy. Finally, [33] evaluates a proximity-based algorithm over a public Narrowband IoT (NB-IoT) network in a large-scale urban setting, benchmarking its accuracy against other radio range-based and range-free methods.

Received Signal Strength (RSS)—A widely used IoT localization method is RSS-based multilateration. As shown in Figure 1.5 (page 14), the target collects RSS measurements from nearby anchors, converts them into distance estimates, and applies multilateration, typically via Least Squares (LS) optimization, to determine its position. This approach is cost-effective and prac-

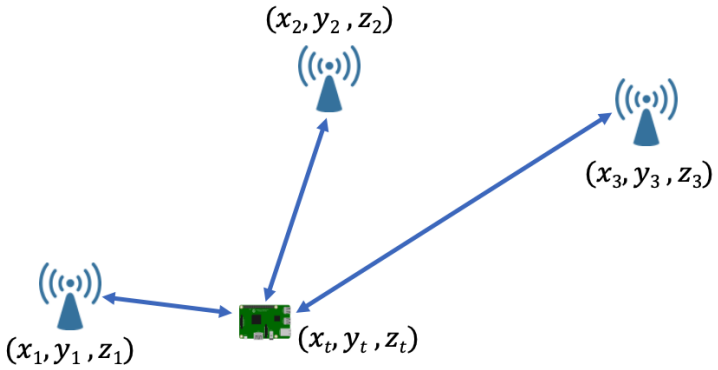


Figure 1.4: Proximity-based localization.

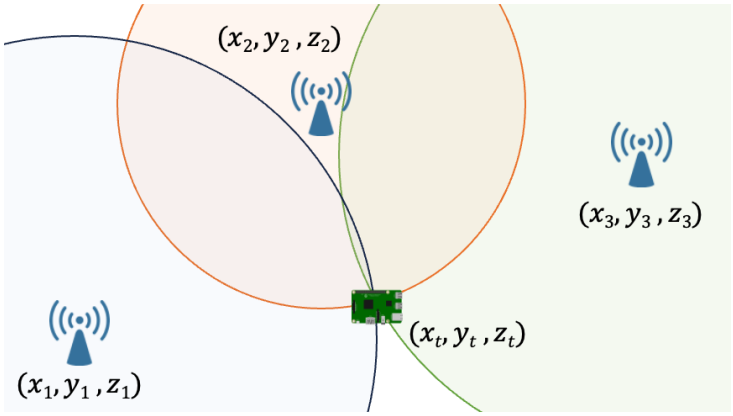


Figure 1.5: Multilateration-based localization principle using signal measurements to estimate distances between the target and anchors.

tical, exploiting built-in radio transceivers, requiring no dedicated ranging hardware, and integrating seamlessly with existing networks. Its low computational and energy demands make it ideal for large-scale or battery-powered deployments while maintaining sufficient accuracy for many IoT services [34].

These advantages have driven extensive research on range-based methods, leading to numerous enhancements and technology-specific implementations. In [35], Dempster–Shafer theory, non-Gaussian probability density functions, and realistic RSS modeling are combined to handle measurement imperfections and anchor unreliability, achieving excellent performance in residential and laboratory IoT environments. Focusing on indoor contexts, [36] proposes a multilateration algorithm using Non-linear Least Squares (NLS) that outperforms existing solutions in accuracy. Complementing these, [37] compares WiFi and Long-Term Evolution (LTE) for

RSS-based localization, selecting the technology according to indoor or outdoor deployment. The potential of LoRa for RSS-based positioning is demonstrated in [38, 39], which validates its accuracy and robustness in both indoor and outdoor scenarios. Finally, [40] explores more challenging environments, applying RSS-based techniques to underwater and underground wireless sensor networks and highlighting the need to address directionality issues in such settings.

Time of Flight (ToF) and Time of Arrival (ToA)—These methods estimate target–anchor distances from signal propagation time and then apply multilateration, as illustrated in Figure 1.5 (page 14). Despite their technical appeal, they are limited by sensitivity to clock-synchronization errors and by signal deflection from obstacles, which complicates indoor deployment [41].

Several studies have sought to overcome these constraints. In [42], a ToF algorithm combines joint clock synchronization, LS estimation of emission and arrival times, and Maximum Likelihood Estimation (MLE) with a Gaussian noise model, outperforming conventional approaches. To further mitigate synchronization issues, [43] presents a BLE system for continuous time alignment, achieving microsecond-level accuracy and proving effective for ToF-based positioning. Similarly, [44] introduces an embedded optimization scheme using nonlinear LS and two-way ToA measurements on an Ultra-WideBand (UWB) network, attaining sub-decimeter accuracy for high-precision applications.

Time Difference of Arrival (TDoA)—Considering the limitations of ToA and ToF, recent studies have investigated alternative techniques with comparable principles, among which TDoA has gained particular attention. This approach reduces implementation complexity by requiring clock synchronization only among anchor nodes [45]. The target's position is then inferred by deriving distances from the differences in signal arrival times at multiple anchors and applying multilateration, as illustrated in Figure 1.5 (page 14).

Another major limitation inherited from ToA and ToF is vulnerability to Non-Line-of-Sight (NLOS) propagation, which distorts true distance estimation. In [46], this issue is mitigated by two formulations: one jointly estimates source position and NLOS error to tighten error bounds, while the other introduces a balancing parameter and a modified measurement model to handle the triangle-inequality violations common in robust LS. Similarly, [47] employs Semi-Definite Programming (SDP) to further reduce NLOS-induced errors.

Beyond NLOS, TDoA systems also face multipath interference in indoor environments. To

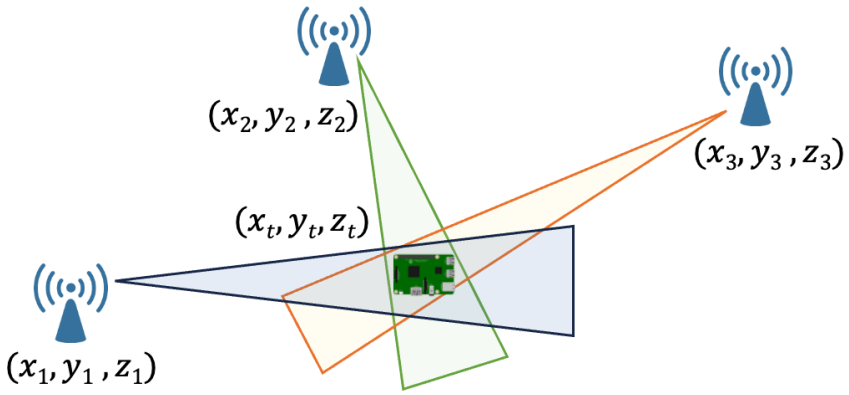


Figure 1.6: AoA-based localization.

address this, [48] proposes broadband signal generation on low-power narrowband transceivers, validated with Software-Defined Radio (SDR) measurements, achieving excellent performance within the 2.4 GHz ISM band. Anchor geometry can also compromise accuracy when anchors are placed too closely or symmetrically. The work in [49] tackles this by selecting and fusing subsets of anchors, an approach later extended in [50] for mobile target tracking. Finally, TDoA has proven effective with low-power, low-cost technologies such as LoRa: [51] demonstrates reliable indoor/outdoor localization for vulnerable people (e.g., search and rescue), while [52] validates five LoRa-based TDoA algorithms through simulations and field trials.

Angle of Arrival (AoA)—In AoA localization, the target position is determined as the centroid of the intersection area formed by the sight triangles between the target and anchor nodes (Figure 1.6, page 16). This geometry-based method can achieve high accuracy, but its practical deployment in IoT is constrained by the need for specialized hardware such as antenna arrays and advanced signal processing [53]. Moreover, AoA typically requires an unobstructed Line-of-Sight (LOS) and is sensitive to environmental factors, which can further limit its robustness in real-world scenarios.

Despite these constraints, several studies advance this promising approach. In [54], a two-step iterative algorithm combines AoA estimation with multilateration, achieving superior results on a BLE network. Similarly, [55] applies a CNN to BLE signals to mitigate noise, multipath effects, and path loss. To improve reliability in WiFi–based AoA, [56] proposes a confidence-aware system that assigns decision weights according to measurement certainty. UWB solu-

tions include AnguLoc [57], which addresses duplex ambiguity and clock skew to enhance accuracy and reduce packet exchanges, and the framework in [58], which integrates NLS, Kalman filtering, and Gaussian filtering to counter interference in 5G and IoT networks. Finally, [59] tackles hardware integration, proposing a Multiple-Input Multiple-Output (MIMO) antenna design that lowers the complexity of embedding AoA methods into compact IoT devices.

1.2.3 Hybrid Approaches

Recent research shows growing interest in hybrid approaches for IoT localization because of their ability to overcome the limitations of individual techniques [14]. By intelligently combining different positioning strategies, for example, integrating proximity-based detection with multilateration, or by fusing heterogeneous data sources such as WiFi, Bluetooth, and other radio technologies, these methods exploit the complementary strengths of each component. Such cross-layer and multi-technology integration enables localization systems to achieve higher accuracy, greater adaptability to diverse environments, and improved resilience against interference and environmental dynamics, ultimately providing more reliable and energy-efficient IoT location services.

Joint Techniques—Several studies highlight the benefits of combining complementary techniques to improve localization accuracy and scalability. In [60], Round-Trip Time (RTT) is fused with WiFi RSS to enhance both precision and system scalability. Hybrid RSS–AoA methods are explored in [61], which achieves robust 3D positioning while mitigating nonconvexity and computational complexity, and in [62], which targets harsh outdoor IoT environments with a scalable algorithm. Other works integrate time-based approaches: [63] combines ToF and TDoA to couple the accuracy of ToF with the energy efficiency of TDoA, while [64] fuses TDoA and Phase Difference of Arrival (PDoA) with PSO to significantly boost localization performance over standard TDoA-only methods.

Data Fusion—Shifting the focus to hybrid algorithms that combine different transmission technologies, a clear trend emerges: the prevalent adoption of WiFi, owing to its wide integration in most IoT infrastructures. In [65], the fusion of a WiFi architecture, characterized by shaded coverage regions, with BLE beacons significantly improved indoor localization accuracy.

To leverage complementary strengths, [66,67] propose hybrid schemes that integrate a WiFi backbone with strategically placed UWB beacons, achieving highly accurate positioning while mitigating the limitations of each technology. Concluding this line of research, [68] presents a multi-protocol system unifying WiFi, Bluetooth, ZigBee, and UWB, which was validated in realistic operational environments and demonstrated superior performance across all evaluation metrics.

1.3 Trustworthiness and Security in Localization Systems

A wide range of attacks can compromise IoT localization systems by targeting different stages of their operation. Such attacks may disrupt the localization system, undermining its availability, or manipulate measurements to produce false positions, threatening authenticity. The following analysis examines the main threat models associated with each localization technique and presents the most effective countermeasures proposed in the literature [14].

1.3.1 Availability

Attacks targeting availability are designed to prevent the system from determining the position of the target. Among these, Denial-of-Service (DoS) attacks are particularly significant, with jamming representing the most frequently documented case in the literature [69]. Jamming consists of deliberately saturating or obstructing the communication channel so that legitimate nodes are unable to exchange data. None of the localization techniques discussed in this work is completely resistant to this type of attack [70].

Consider, for instance, RSS-based localization. In this approach, the estimation of target–anchor distances depends on RSS measurements and on calculations derived from the signal propagation model [71]. When a jamming attack occurs, the Signal-to-Noise Ratio (SNR) at the receiver drops sharply. As a result, the target, unaware of the interference, overestimates its distance from the anchors, which can cause significant localization errors or, in the worst case, make position estimation unfeasible [72].

A substantial body of research has addressed the problem of jamming in the broader con-

text of IoT and Wireless Sensor Networks (WSNs), proposing numerous detection and mitigation strategies [73–77]. Narrowing the focus to IoT localization systems, [78] introduces AS-DILOC, a consensus-based iterative distributed algorithm equipped with an abandonment mechanism to cope with packet loss in communication links during DoS attacks, thereby ensuring accurate sensor localization regardless of the attacker's behavior.

1.3.2 Authenticity

Among the major security risks faced by IoT localization systems, authenticity stands out as critical. Attacks often target these systems by compromising anchors or infiltrating the network under a trusted identity, then corrupting distance estimates through falsified reference positions or by altering transmission parameters such as signal power [79]. Attacks of this nature can be classified into four main categories based on their execution method: spoofing, sybil, byzantine, and wormhole attacks [14].

Spoofing—In a spoofing attack, a malicious node impersonates a legitimate anchor, often by duplicating its MAC address, thereby disrupting the localization process in multiple ways. Several studies propose countermeasures, including prototyping platforms designed to evaluate secure indoor localization and to analyze spoofing behavior, demonstrating their effectiveness for assessing defense strategies [80]. Other works, focusing on fingerprint-based localization, introduce detection schemes capable of identifying falsified fingerprints both during database updates and online inference, achieving high localization accuracy while neutralizing spoofing attempts [81].

Sybil—The sybil attack is a particularly severe threat to IoT localization systems that rely on connectivity information. By creating multiple false identities, an attacker can distort the perceived network topology and compromise localization accuracy [82]. To counter this, several defenses have been proposed. For example, [83] presents a secure variant of DV–Hop that detects and mitigates sybil nodes while maintaining estimation accuracy. Likewise, [84] introduces a method for RSS-based localization that combines approximate point-in-triangulation checks with differential privacy techniques to protect node identity and increase robustness against such attacks.

Byzantine—Among the various threats to IoT localization, byzantine attacks rank among the most frequently addressed in the literature due to their disruptive potential. A byzantine attack occurs when an adversary gains control of one or more network nodes and deliberately disrupts the localization process by supplying false data or altering transmission parameters, thereby degrading position accuracy [85].

Several countermeasures have been proposed. In [86], four techniques, Weighted Least Squares (WLS), Secure Weighted Least Squares (SWLS), and two L1-based methods (LN-1 and LN-1E), are evaluated for detecting and mitigating both uncoordinated and coordinated malicious nodes. Another WLS-based approach in [87] targets adversaries that manipulate anchor transmission power. Probabilistic strategies include [88], which frames the attack as a maximum a posteriori problem and uses an iterative algorithm to approximate the posterior while jointly estimating position and velocity and identifying compromised nodes, and [89], which proposes a two-step feature selector integrating an access-point trust model with Manifold Learning to improve resilience against byzantine behavior.

Wormhole—In a wormhole attack, an adversary deploys two colluding nodes and links them with a dedicated low-latency channel. This hidden connection misleads neighboring nodes into believing they are only one hop away from distant nodes, corrupting the perceived network topology [90]. Such attacks can severely disrupt DV–Hop-based localization, prompting extensive research on detection and mitigation.

In [91], a secure DV–Hop algorithm delegates data transmission to neighbor nodes and applies a trust-based strategy, significantly improving detection rates, reducing localization errors, and lowering energy consumption. Building on centralized localization, [92] integrates malicious-node identification via a single-class Support Vector Machine and a recovery phase to develop a Secure Optimized Localization algorithm effective against wormhole attacks. Similarly, [93] strengthens resilience by leveraging Farkas' lemma to identify and counter wormhole behavior with higher accuracy than several existing approaches.

Multi-Threat Solutions—Some studies propose integrated defenses capable of countering multiple types of attacks described above.

In [94], a blockchain-based secure localization algorithm protects both the declared anchor positions and the authenticity of exchanged data, effectively mitigating diverse attack vectors.

Table 1.1: Comparison of localization techniques.

Technique	Accuracy	Implementation Cost	Complexity and Energy Consumption	Coverage and Scalability
Fingerprinting	Medium/High	Medium/High	Low/Medium	High
Connection Information	Low	Medium/High	Medium	High
Proximity	Low	Low	Low	Low/Medium
Multilateration-based	Medium/High	High	High	Medium/High

Along the same line, [95] presents a blockchain-enabled fingerprinting scheme that maintains a tamper-proof, real-time database of electromagnetic fingerprints and demonstrates strong resilience to spoofing and sybil attacks through simulation.

Within fingerprint-based localization, [96] introduces a semi-supervised learning technique that continuously adapts to environmental changes, providing robustness against several attack types. A similar rationale is applied in [97], where a hybrid machine-learning model detects routing-based threats such as wormhole and sybil attacks by optimizing distance, location, and data communication features. Finally, [98] explores the same classes of threats, proposing detection algorithms built on the concept of the highest-rank common ancestor and validating their effectiveness experimentally.

1.4 Comparative Analysis and Identified Research Gaps

From a comparative perspective, each GPS-free localization technique discussed in the previous section exhibits a specific balance of strengths and limitations, highlighted in Table 1.1.

Fingerprinting achieves a favorable trade-off between accuracy, complexity, and energy efficiency, which explains its popularity, though its deployment cost grows with coverage. Connectivity-based approaches offer similar cost and scalability profiles but suffer from lower positioning accuracy.

Within the radio range-based family, multilateration based on RSS, AoA, ToF, and ToA de-

livers high accuracy and scalability but at the price of higher implementation cost and energy consumption, whereas proximity methods remain attractive only when coarse positioning suffices. These findings are consistent with the statistical evidence that the majority of published works favor range-based techniques, which combine relatively straightforward implementation with strong accuracy and adaptability to diverse environments.

An increasingly important trend is the adoption of hybrid approaches that blend different algorithms and fuse heterogeneous radio technologies such as WiFi, Bluetooth, UWB, and LoRa. By leveraging complementary strengths, hybrids improve accuracy beyond that of single techniques and, crucially, enhance robustness and reliability. This makes them particularly promising for small to large-scale IoT deployments where energy efficiency and adaptability are critical.

Security and trustworthiness considerations further sharpen this picture. The radar diagram in Figure 1.7 (page 23) summarizes the main security threats to IoT localization. Each vertex represents a specific attack type, and the closer a data point lies to a vertex, the greater the vulnerability reported in the literature. Byzantine attacks, in which compromised anchors inject false data, are the most critical and well-documented risk for range-based methods. By contrast, jamming-based DoS attacks, though less explored in GPS-free positioning studies, are widely recognized as potentially highly disruptive, threatening the availability of IoT localization services. Connectivity-driven schemes are additionally vulnerable to wormhole and sybil attacks, while fingerprinting faces a combination of spoofing and database manipulation risks.

Although the literature proposes various countermeasures, most focus narrowly on accuracy improvements or single-attack detection, leaving the broader challenges of resilience and continuous reliability evaluation, which are key requirements for real-world IoT services, only partially addressed. Closing this gap is critical because trustworthy positioning is fundamental for safe, LBS-driven operations in smart agriculture, smart cities, industrial automation, and other IoT-enabled infrastructures.

This challenge forms the core motivation of the present doctoral research. Throughout my work, particular emphasis has been placed on hybrid GPS-free localization and on mechanisms to strengthen not only accuracy but, above all, trustworthiness in adversarial environments. The work explores methods to detect and characterize vulnerabilities, introduces metrics to

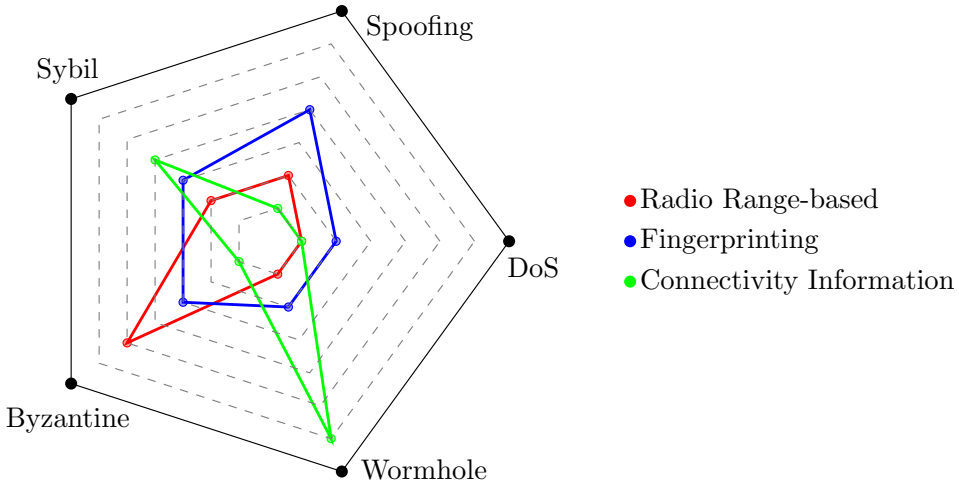


Figure 1.7: Impact of major attacks across different localization techniques.

quantify their impact, and develops strategies to mitigate and counteract potential attacks, ultimately applying these technologies and techniques in real-world scenarios. All these advances converge into a unified architecture for trustworthy and energy-efficient IoT localization, which will be presented and analyzed in the following chapters.

Chapter 2

System Model

Building on the background and challenges outlined in the previous chapters, this part of the thesis introduces the core scientific and technical contributions of the research. It defines the reference scenario and the proposed architecture, an integrated framework designed to deliver sustainable and trustworthy GPS-free localization for IoT LBS.

This chapter details the proposed hybrid range-based and range-free algorithms, the reliability index for continuous quality assessment, and the security mechanisms to detect and mitigate malicious activities. Together, these elements form the methodological backbone of the thesis, enabling accurate, energy-efficient, and resilient IoT positioning even in dynamic or adversarial environments.

2.1 Reference Scenario and Proposed Architecture

The reference scenario, shown in the physical layer of Figure 2.1 (page 25), consists of N wireless devices acting as anchors with known fixed positions and a target whose location must be estimated. It represents dynamic indoor or outdoor environments, such as smart buildings or parking areas, where moving obstacles and structural changes can significantly affect signal propagation and, consequently, localization accuracy.

Each i-th anchor deployed in the environment (i = $\{1,2,\ldots,N_{\mathrm{a}}\}$), is located at fixed coordinates $\boldsymbol{a}_i = [a_i^x, a_i^y]^T$, while the target is assumed stationary at $\boldsymbol{t} = [t^x, t^y]^T$, with T denoting transposition. Although the current analysis is confined to a two-dimensional plane, the

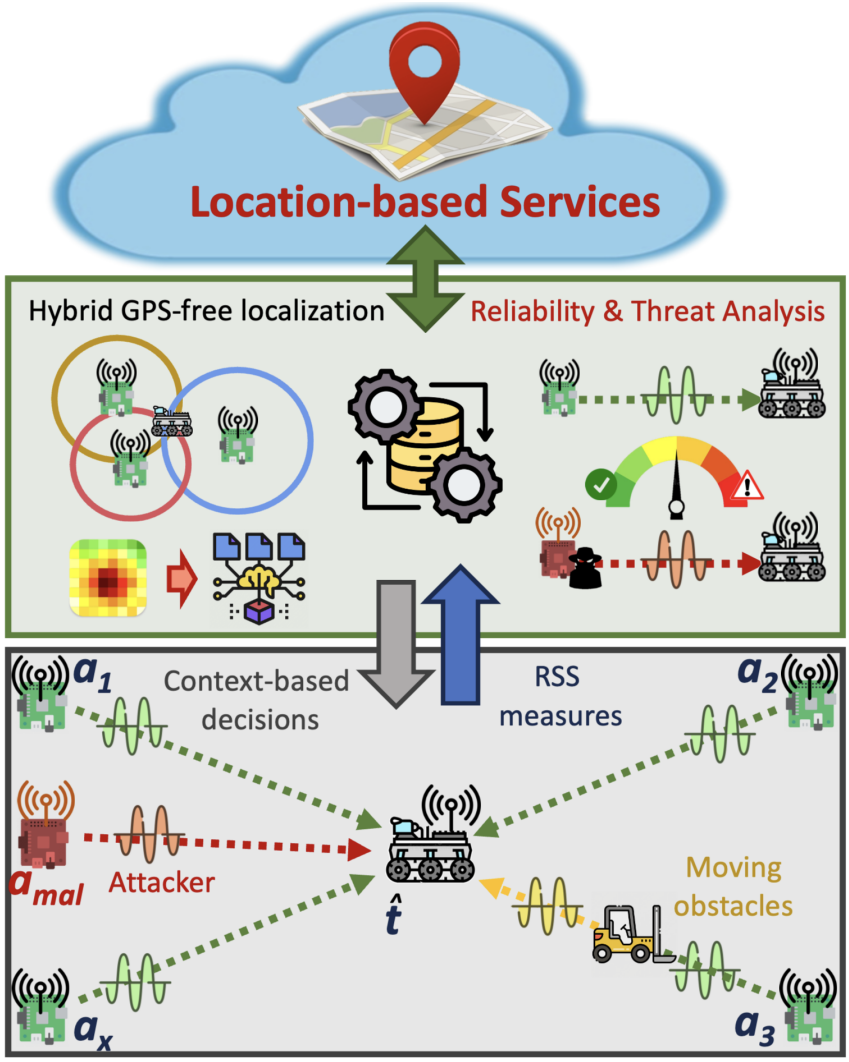


Figure 2.1: Reference scenario and conceptual integration into the POSIDONIA architecture.

methodology can be readily extended to 3D.

The Euclidean distance between the target and anchor i is expressed as

$$d_i = \sqrt{(a_i^x - t^x)^2 + (a_i^y - t^y)^2} \tag{2.1}$$

During operation, anchors transmit packets to the target, which derives RSS measurements used for localization. Depending on the configuration, computations are performed either directly on the device (device-based localization) or offloaded to the Fog/Edge layer (device-assisted localization). The estimated position is then supplied to higher-level LBS.

Because many IoT environments already deploy WiFi or Bluetooth connectivity, leverag-

ing this infrastructure is more cost-effective than installing additional hardware. Access Points (APs) and connected devices can thus serve as anchors, while the target needs only a standard wireless interface to collect RSS data.

However, the dynamic and potentially adversarial nature of this scenario introduces significant challenges. Moving obstacles or malicious nodes can degrade signal quality and threaten the accuracy and trustworthiness of range-based techniques such as multilateration and fingerprinting.

To address these issues, the next chapters propose hybrid GPS-free localization strategies that fuse measurements from different wireless interfaces or combine complementary methods (e.g., fingerprinting and multilateration). This approach aims to enhance localization efficiency and resilience, laying the foundation for reliable and accurate LBS in real-world IoT environments.

This scenario forms the foundation of the proposed POSition Information with Digital twin Offloading in trustworthy Next-generation Internet Applications (POSIDONIA) architecture. Building on it, POSIDONIA is designed not only to deliver reliable, energy-efficient, and secure GPS-free localization for LBS but also to continuously assess the trustworthiness of its outputs. Beyond pure positioning, the architecture incorporates parallel processes across the Fog, Edge, and Cloud (FEC) continuum. On one side, it evaluates the geometric conditions between anchors and the target, together with dynamic variations of the wireless channel, to derive a reliability index that quantifies the confidence level of each estimated position. On the other, it integrates mechanisms for detecting and mitigating malicious activities that could compromise data integrity or disrupt the localization process. Through this dual strategy, POSIDONIA ensures that the positioning information delivered to LBS is accurate, energy-efficient, and resilient against both environmental uncertainties and adversarial threats.

2.2 Range-Based Localization

This section introduces the range-based component of the proposed localization framework, which estimates the target position by first inferring its distances to surrounding anchors and then solving a multilateration problem. The first subsection details how RSS measurements are

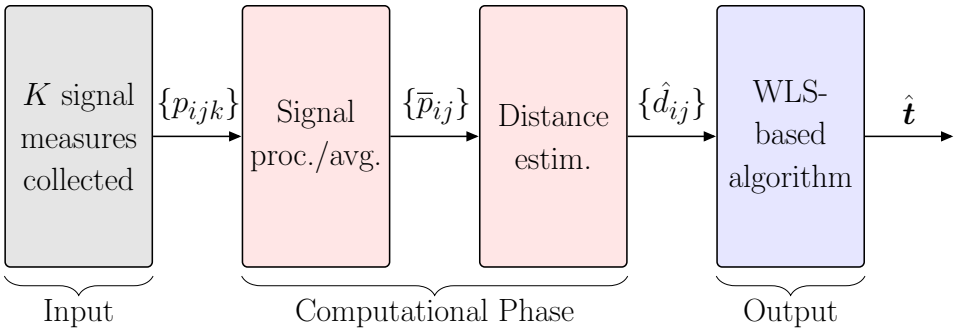


Figure 2.2: General scheme of the distance-based localization method.

collected and processed, using noise averaging to improve measurement reliability, while the second focuses on the multilateration procedure, highlighting the WLS algorithm that underpins the range-based hybrid localization strategies developed in this thesis.

2.2.1 RSS-Based Target-Anchors Distances Estimation

To enable localization, the anchors deployed in the scenario, as illustrated in Section 2.1, periodically transmit signals that are collected by the target to estimate its distance from each anchor. During every localization act, the target acquires a set of RSS samples from each wireless interface j ($j = 1, \ldots, \mu_i$) of every anchor i, as shown in the first block of Figure 2.2 (page 27).

Each of the K RSS measurements, denoted p_{ijk} for sample k ($k = 1, \ldots, K$), follows the standard path-loss model [99]:

$$p_{ijk} = p_0 - 10n \log_{10} d_i + \varepsilon_{ijk} \tag{2.2}$$

where p_0 is the received power at a reference distance of 1 m, n is the path-loss exponent (typically 2–4 [100]), and $\varepsilon_{ijk} \sim \mathcal{N}(0, \sigma_j^2)$ is an additive noise term representing propagation effects such as shadowing or reflections. These noise terms are assumed to be independent and identically distributed across anchors and samples, with variance dependent on the specific wireless technology.

In the second block of Figure 2.2 (page 27), the K samples are averaged to mitigate noise, yielding the mean RSS

$$\overline{p}_{ij} = \frac{1}{K}\sum_{k=1}^{K} p_{ijk} = p_0 - 10n\log_{10} d_i + \varepsilon_{ij} \tag{2.3}$$

where $\varepsilon_{ij} \sim \mathcal{N}(0, \sigma_j^2/K)$ [101]. Averaging thus reduces the impact of random fluctuations and improves measurement reliability [102].

Finally, the third block performs maximum-likelihood distance estimation for each interface j of anchor i, assuming that the residual noise ε_{ij} is sufficiently small [101]. The estimated distance $\hat{d}_{ij}$ is therefore computed as

$$\hat{d}_{ij} \simeq 10^{\frac{\overline{p}_{ij} - p_0}{10n}} \tag{2.4}$$

Once the distances $\hat{d}_{ij}$ from all anchors have been obtained, the target position $\boldsymbol{t}$ is calculated using a multilateration-based algorithm [103], which combines the estimated distances to infer the most likely location of the device.

2.2.2 Multi-Interface Multilateration-Based Localization

Multilateration is a fundamental technique for estimating the position of a target from its measured distances to multiple anchors. By solving a system of geometric equations that relate anchor coordinates and target–anchor distances, multilateration determines the most probable target location and is widely adopted in IoT localization for its balance of accuracy and computational efficiency [103].

Among multilateration algorithms, the LS method is one of the most established, estimating the target position by minimizing the sum of squared residuals between measured and calculated distances. Building on this principle, the WLS algorithm [86] introduces a key refinement by assigning reliability weights to each measurement. These weights reflect factors such as obstacles, target–anchor distance, and wireless channel conditions, enabling more accurate and robust estimates than methods that treat all data equally. While the standard WLS formulation assumes single-interface devices, this work extends it to multi-interface anchors, allowing the fusion of multiple RSS measurements further to enhance accuracy and reliability in dynamic IoT environments.

Suppose that anchor i provides RSS measurements on $M_i \leq \mu_i$ interfaces, meaning that not all installed interfaces necessarily deliver data. In particular, $M_i = 0$ represents an anchor with no usable measurements. The total number of active interfaces is therefore

$$L = \sum_{i=1}^{N} M_i \leq \sum_{i=1}^{N} \mu_i \tag{2.5}$$

Following the mathematical formulation detailed in [86], the WLS algorithm solves a system of equations of the form $\boldsymbol{A\rho} = \boldsymbol{b}$, where the unknown vector is

$$\boldsymbol{\rho} = \begin{bmatrix} \boldsymbol{t} \\ ||\boldsymbol{t}||^2 \end{bmatrix} \tag{2.6}$$

with $\boldsymbol{t}$ the 2D target position and $||\boldsymbol{t}||^2$ its squared Euclidean norm, which stands for the distance of the vector with respect to the origin.

The multi-interface WLS solution introduced in this work uses a matrix $\boldsymbol{A}$ and vector $\boldsymbol{b}$ that are built from the anchors' coordinates and the estimated target–anchor distances. For each row ℓ of $\boldsymbol{A}$ and corresponding element of $\boldsymbol{b}$,

$$\boldsymbol{A}_\ell = \begin{bmatrix} -2\boldsymbol{a}_i^T & 1 \end{bmatrix} \qquad b_\ell = \begin{bmatrix} \hat{d}_{ij}^2 - ||\boldsymbol{a}_i||^2 \end{bmatrix} \tag{2.7}$$

where the row index ℓ is given by

$$\ell = \begin{cases} j & \text{for } i = 1 \\ \sum_{m=1}^{i-1} M_m + j & \text{for } i > 1 \end{cases} \tag{2.8}$$

A diagonal weight matrix $\boldsymbol{W}$ of size $L \times L$ assigns a weight w_ℓ to each RSS measurement, reflecting its reliability. Derived as the inverse variance of the squared distance estimate (Var$(\hat{d}^2)^{-1}$) under the assumption of Log-Normal signal propagation, w_ℓ is computed as

$$w_\ell = \left\{ \hat{d}_{ij}^4 \exp\left(\frac{\sigma_{RSS_j}^2}{4.715n^2}\right) \left[\exp\left(\frac{\sigma_{RSS_j}^2}{4.715n^2}\right) - 1\right] \right\}^{-1} \tag{2.9}$$

Having these elements available, the final WLS estimate of $\boldsymbol{\rho}$ is therefore

$$\hat{\boldsymbol{\rho}} = \left(\boldsymbol{A}^T\boldsymbol{W}\boldsymbol{A}\right)^{-1}\boldsymbol{A}^T\boldsymbol{W}\boldsymbol{b}, \tag{2.10}$$

from which the target position is obtained as

$$\hat{\boldsymbol{t}} = [\hat{\rho}_1, \hat{\rho}_2]^T \tag{2.11}$$

2.3 RSS-Based Range-Free Fingerprinting

RSS-based fingerprinting localization is typically organized into two fundamental phases: offline training and online inference, as discussed in Section 1.2.1.

During the offline phase, a detailed radio map is constructed by collecting RSS measurements from multiple anchors at a dense grid of Reference Points (RPs) across the area of interest. The selection of these RPs typically follows a uniform grid topology, with a spatial resolution determined by the dimensions of the environment and the required positioning granularity. The density of these RPs strongly influences the achievable accuracy; a higher density captures fine-grained signal fluctuations caused by multipath fading and shadowing, thereby improving the distinguishability of adjacent locations. However, increasing RP density yields diminishing returns and significantly increases the labor cost. Consequently, the chosen grid spacing represents a trade-off between the desired localization error bound and the time required to survey the site. The collected fingerprints then serve as the training set for ML models such as kNN, RF, or CNN.

Once the models are trained, the process moves to the online phase. Here, the target node acquires new RSS samples and feeds them to the trained models, which compare the incoming measurements against the stored radio map to infer the most probable location. This separation of training and inference not only enables real-time operation during deployment but also facilitates periodic updates of the radio map and the ML models to cope with environmental changes such as moving obstacles or evolving network layouts.

2.4 Threat Models

Reliable IoT localization must be accurate and trustworthy, even in adversarial conditions. However, GPS-free wireless positioning systems are vulnerable to security threats that can corrupt

measurements, degrade accuracy, or disable the service. Among these, jamming and byzantine attacks are particularly disruptive, as they directly target RSS-based localization.

Jamming Attacks—By intentionally obstructing or interfering with data transmission and reception, jamming disrupts communication channels and prevents nodes from functioning correctly. Given the reliance of RSS-based localization on precise signal strength measurements, such interference can severely distort the received signal, leading to inaccurate distance estimates and, ultimately, to large positioning errors or complete failure of the localization process.

To simulate this type of attack, the jammer's interference signal power (J^p) is modeled as a ratio α of the average transmission power of the anchors (in linear form). While the parameter α establishes the nominal intensity of the attack, a Uniform distribution is adopted to model the stochastic fluctuations of the jamming signal amplitude. This approach captures the unpredictability of the interference by allowing the instantaneous power to vary randomly within a bounded range around the baseline level defined by α, rather than assuming a static value.

Following the jamming model described in [72], the power of the interfering jammer at anchor i is given by

$$I_i = J^p - 10n \log_{10} \delta_i \tag{2.12}$$

Here, the parameter n denotes the path loss exponent defined earlier, and δ_i is the distance between the jammer and the i-th anchor. Anchors operate on different communication channels, which may change over time. To address this, the jammer is modeled to target specific communication channels, selectively interfering with anchors operating on those frequencies. This interaction alters the power measured by the target as described in Equation (2.3), resulting in inaccurate target-anchor distance estimations and negatively affecting position estimation. Additionally, the amplitude of the interference signal is modeled to vary over time, introducing further variability and increasing the complexity of the localization process.

This study considers two distinct jammer behaviors: constructive-destructive interference, in which the jammer either increases or decreases the power level of communication between the target and the anchors without fully disrupting it, and Denial-of-Service (DoS) interference, in which the jammer renders one or more anchors completely unavailable for the localization process. Figure 2.3 (page 32) illustrates these jamming behaviours by plotting the average RSS

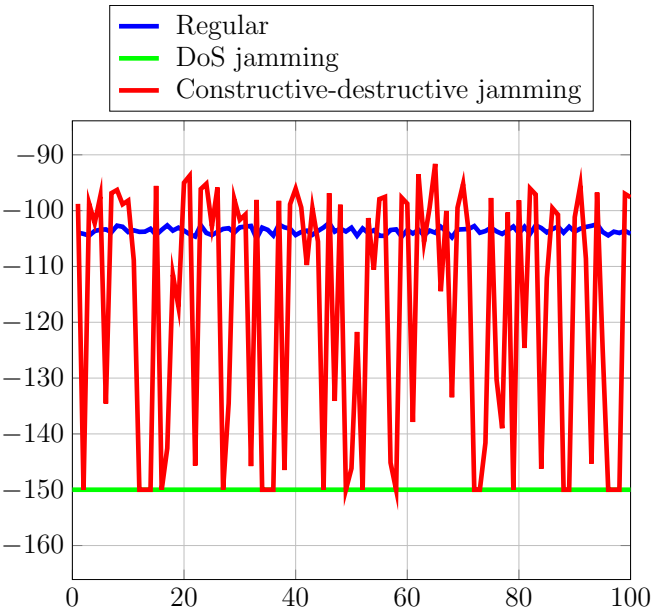


Figure 2.3: $\overline{p}_i$ for the three key scenarios for a given anchor: regular anchor not under attack, under DoS jamming, and under constructive and destructive jamming interference.

observed by the target over measurement bursts for three representative conditions: the anchor operating normally, the anchor under DoS jamming where the measured RSS collapses to the receiver sensitivity level ($\sim -150\,\mathrm{dBm}$), and the anchor affected by constructive/destructive interference jamming. The figure shows how DoS jamming effectively silences the link by driving signal power to the sensitivity floor, while interference-type jamming produces large, rapidly varying RSS deviations. Both mechanisms reduce the usable signal power at the target, either by making the signal fall below the reception threshold or by corrupting its waveform, thereby disrupting localization while remaining difficult to detect by simple monitoring systems.

Byzantine Attacks—As introduced in Section 2.2.1, the standard path-loss model in Equation 2.2 is used to estimate anchor–target distances, which then feed multilateration-based localization algorithms. A malicious node can exploit this dependency by manipulating the RSS, thereby causing systematic overestimation or underestimation of these distances and ultimately leading to significant position-estimation errors. In a byzantine attack, the transmitted power of a compromised anchor is deliberately perturbed by adding a random noise term, so that

$$P_{tx} = P_{benev} + \delta \tag{2.13}$$

Where P_{benev} corresponds to the transmitted power under normal conditions when no malicious manipulation occurs. The term $\delta \sim \mathcal{U}(-\sigma_\varepsilon, \sigma_\varepsilon)$ represents the noise injected by the malicious node [86]. This manipulation effectively alters the RSS values that the target node receives, leading to either an overestimation or underestimation of the distance between the anchor and the target.

Chapter 3

Proposed Solutions: Hybrid Localization and Reliability Assessment

3.1 Data Fusion–Based Hybrid Approach

The multi-interface WLS described in Section 2.2.2 forms the foundation for hybrid localization approaches that fuse data from multiple wireless technologies. Such data fusion mitigates interference effects, enhancing accuracy while increasing system robustness and resilience [104]. Two strategies are considered: Redundant Anchors Positioning System (RAPS), which exploits all available measurements in the WLS formulation of Equation (2.10), and Multi-Interface Adaptive Positioning System (MAPS), which opportunistically selects the best technology per anchor before applying WLS [105].

The overall workflow of these methods is illustrated in Figure 3.1 (page 35) and detailed below.

3.1.1 Redundant Anchors Positioning System (RAPS)

The RAPS method is rooted in the concept of redundancy, proving to be conceptually simple but very effective. In an attempt to improve the robustness and accuracy of the system, RAPS virtually combines the number of available anchors of the two technologies, considering them as stand-alone entities. Specifically, Equation (2.7) is constructed with L as in Equation (2.5),

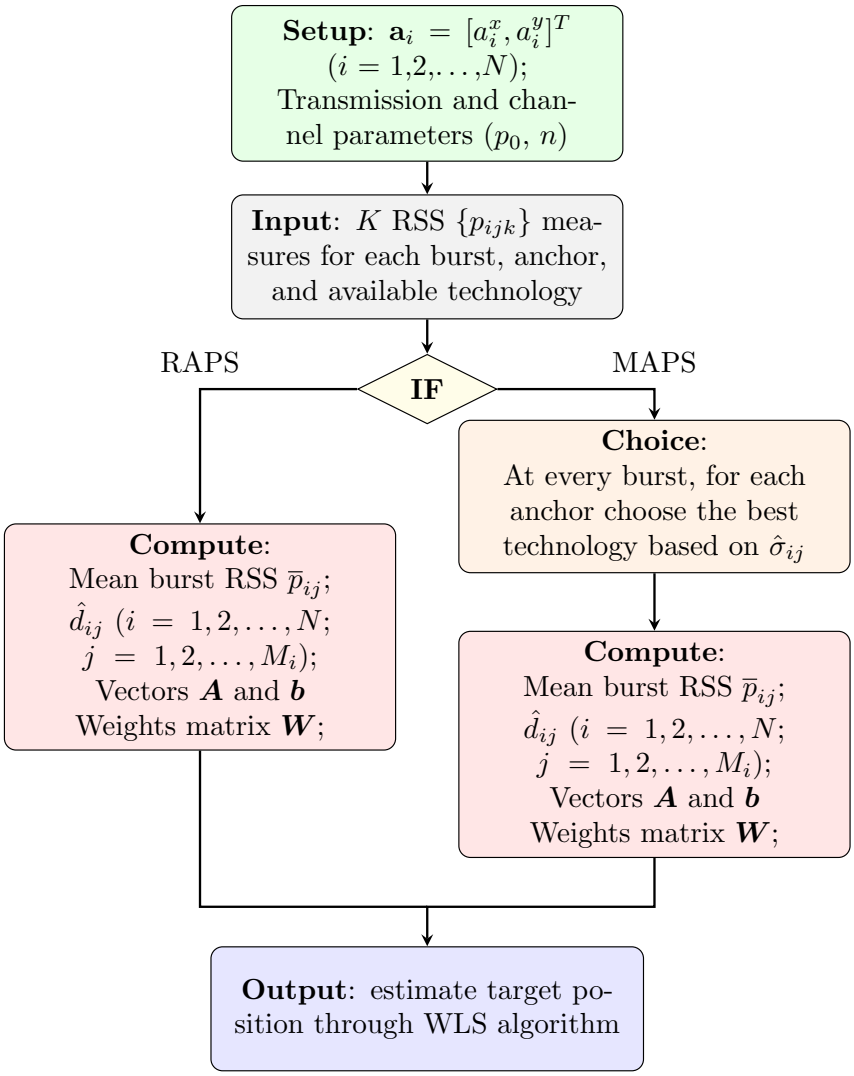


Figure 3.1: Flowchart of the RAPS and MAPS algorithms.

introducing M_i equations for estimating the distance corresponding to each anchor. This approach mitigates the impact of interference that may occur on one of the technologies.

As an illustrative example, suppose that the localization algorithm is based on 10 anchors, each equipped with 2 wireless interfaces, e.g., WiFi and BLT. RAPS solves the multi-interface WLS with a system of 20 equations. This extends the established localization schemes, where single-interface devices are used; in this case, the mathematical derivations would lead to a system with 10 equations associated with the same anchors' positions.

The RAPS redundancy becomes especially valuable in scenarios where the knowledge of channel conditions and the behavior of different technologies at different times is incomplete.

3.1.2 Multi-Interface Adaptive Positioning System (MAPS)

As in RAPS, the MAPS method tries to mitigate the potential impact of interference on different wireless technologies in distinct time intervals. Unlike RAPS, which directly uses the multi-interface WLS described in Section 2.2.2, this method dynamically selects one of the available technologies on each anchor based on its reliability, to be input to a standard single-interface WLS. This leads to a different computational complexity, as will be detailed in Section 3.1.3.

As shown in Figure 3.1 (page 35), in a preliminary stage, MAPS computes the standard deviation of the burst of data received on the available M_i wireless interfaces for anchor i as

$$\hat{\sigma}_{ij} = \sqrt{\frac{1}{K-1}\sum_{k=1}^{K-1}(p_{ijk} - \overline{p}_{ij})^2} \tag{3.1}$$

The best technology for anchor i estimates the distance to the anchor with the minimum error possible. Therefore, MAPS selects the technology that provides the minimum estimated standard deviation. In fact, this statistical measure provides information on RSS signal fluctuation over the burst time interval, thus offering relative knowledge on the impact of noise. The set of estimated standard deviations is defined as

$$\mathbf{\Sigma}_i = [\hat{\sigma}_{i1}, \ldots, \hat{\sigma}_{iM_i}]^T \tag{3.2}$$

and the minimum is extracted, i.e., $\hat{\sigma}_{ir} = \min\{\mathbf{\Sigma}_i\}$. Therefore, technology r is chosen for anchor i.

At this point, the WLS system in Equation (2.7) is formulated using the selected information from the N anchors as described above. Using the same illustrative example in RAPS, if 10 anchors are equipped with 2 wireless interfaces, MAPS solves the single-interface WLS with a system of 10 equations. However, each equation associated with a specific anchor may come from data of a different wireless interface, e.g., half of the equations are associated with WiFi data and half with BLT.

This modification makes WLS-based position estimation more computationally efficient than RAPS, as will be detailed in Section 3.1.3.

3.1.3 Discussion on Computational Complexity

Both RAPS and MAPS build on the WLS framework but differ in the dimensions of the matrices and vectors in Equation (2.7). In addition, MAPS introduces a preliminary step to select the optimal technology for each anchor.

For a system with Q equations and V variables, building the system requires $\mathcal{O}(Q)$ operations. Solving it with the WLS algorithm entails a computational cost of $\mathcal{O}(VQ^2 + V^2Q)$ [106], which therefore represents the dominant overall complexity.

In RAPS, the system comprises $Q = L = \sum_i M_i$ equations as in Equation (2.5), with $V = 3$, resulting in a computational complexity of $\mathcal{O}(3L^2 + 9L)$. In MAPS, the system instead involves $Q = N \leq L$ equations and requires an additional technology–selection step. This selection has a cost of $\mathcal{O}(N)$, which is negligible compared to the WLS solution itself, whose complexity is $\mathcal{O}(3N^2 + 9N)$.

The overall complexity of the two algorithms is therefore

$$\mathcal{C} = \begin{cases} \mathcal{O}(3L^2 + 9L) & \text{for RAPS} \\ \mathcal{O}(3N^2 + 9N) & \text{for MAPS} \end{cases} \tag{3.3}$$

Figure 3.2 (page 38) illustrates the complexity $\mathcal{C}$ as N varies from 3 to 10 for both RAPS and MAPS. All anchors are assumed to have the same number M of wireless interfaces, each providing data. As expected, MAPS is unaffected by M since its complexity depends only on N; notably, the MAPS curve coincides with that of RAPS when $M = 1$. In contrast, the complexity of RAPS grows with M, while preserving the same overall trend.

3.2 Joint Techniques–Based Hybrid Approach

The literature presents a range of IoT localization strategies, each with its own distinct strengths and limitations. Fingerprint-based localization is widely adopted due to its scalability and high accuracy [107], but it relies heavily on an offline training phase and is sensitive to environmental dynamics. Changes in the propagation environment, such as moving obstacles or fluctuating channel conditions, cause variations in the RSS, which can degrade positioning accuracy and make frequent retraining costly.

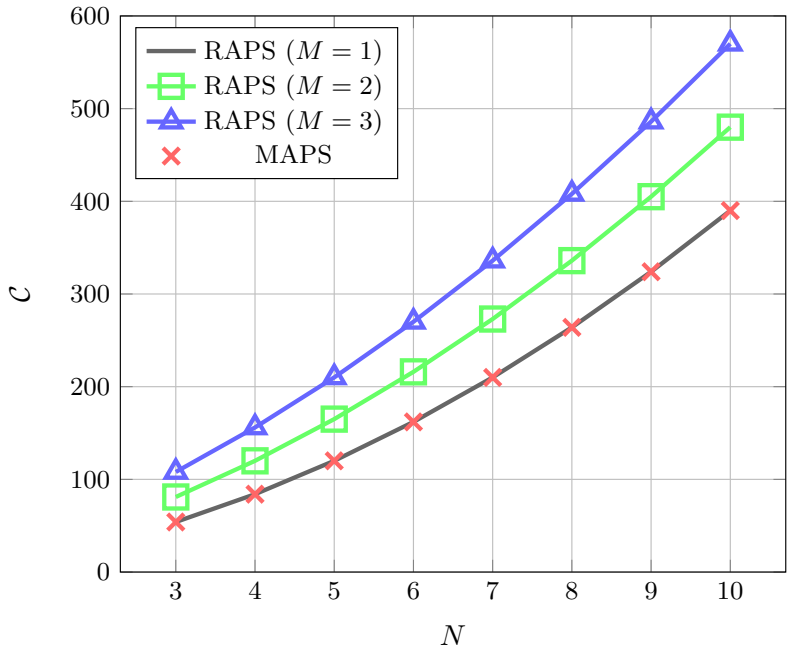


Figure 3.2: Computational complexity as a function of M and N for RAPS and MAPS algorithms.

To enhance robustness, one of the solutions proposed is combining RSS-based fingerprinting with multilateration, leveraging available anchor measurements to compensate for environmental dynamics and potential system attacks [108]. However, multilateration's computational complexity grows with the number of anchors (Equation 2.7). To balance accuracy and efficiency, the WLS component is restricted to a subset of $N = 4$ anchors, satisfying the minimum requirement of $N \geq 3$ for 2D multilateration.

Building on the reference scenario of Figure 2.1 (page 25), suppose that a subset of anchors $N_{\text{null}} \subset N$ becomes unavailable due to blockage or interference, possibly caused by jamming or byzantine, as discussed in later sections, thereby preventing reliable communication with the target. The ML fingerprinting model is pre-trained and remains fixed during operation.

The logical flow of the proposed algorithm is shown in Figure 3.3 (page 39). During each localization act, the target acquires K RSS samples from every active anchor, computes their mean, and uses these averages as input to estimate its position. Simultaneously, the system determines the number of unavailable anchors N_{null}. If all anchors are available ($N_{\text{null}} = 0$), the system executes standard ML-based fingerprinting, and the hybrid estimate $\hat{\boldsymbol{t}}$ coincides with the fingerprinting output $\hat{\boldsymbol{t}}_{ML}$.

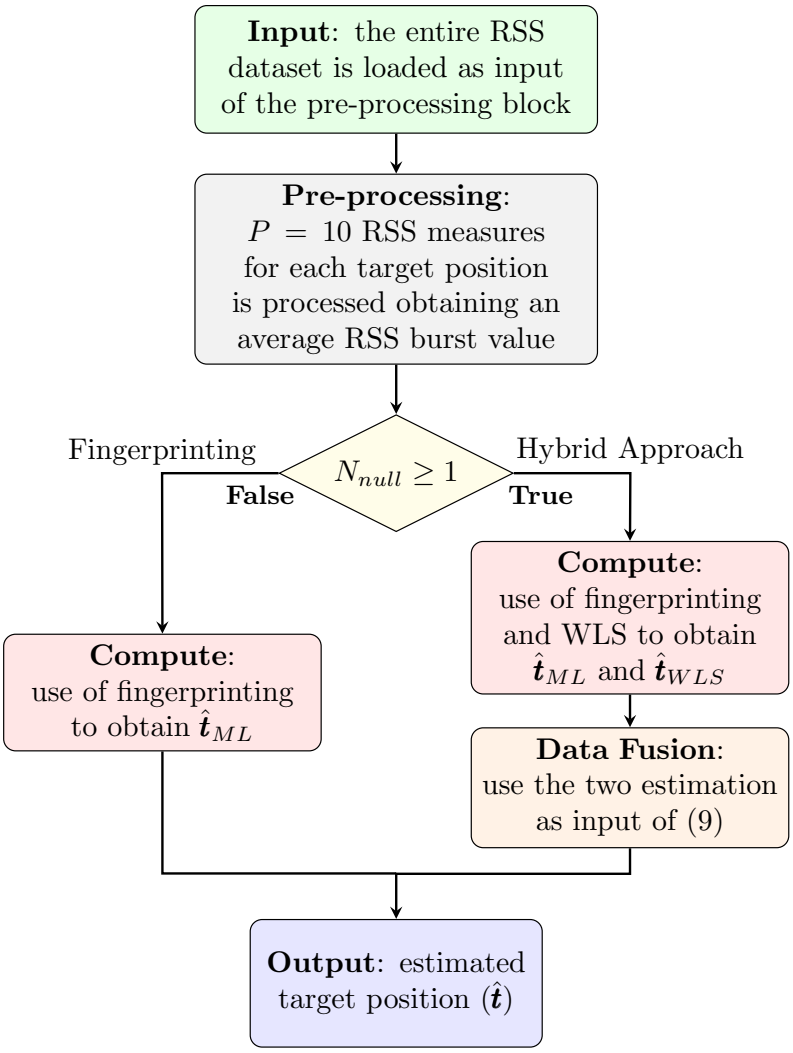


Figure 3.3: Flowchart of the proposed hybrid algorithm.

If one or more anchors are unavailable ($N_{\text{null}} > 0$), two parallel estimations are performed: a multilateration-based estimate $\hat{\boldsymbol{t}}_{WLS}$ using the WLS algorithm, and an ML-based fingerprinting estimate $\hat{\boldsymbol{t}}_{ML}$. These are then fused through a weighted combination that accounts for the reduced anchor availability:

$$\hat{\boldsymbol{t}} = \frac{\hat{\boldsymbol{t}}_{WLS}(1+\omega) + \hat{\boldsymbol{t}}_{ML}(1-\omega)}{2} \tag{3.4}$$

where ω is a weighting factor proportional to N_{null}. Empirically, setting $\omega = 0.2 \times N_{\text{null}}$ provides a good balance between the two estimates. This hybrid design adapts to dynamic environments by retaining fingerprinting efficiency under full coverage, while integrating multilateration during anchor outages to preserve accuracy and reliability.

3.3 Localization Reliability Index

In localization and navigation, reliability expresses the confidence in the accuracy of a position estimate at a given time and location [109]. This confidence depends on several factors, including the geometric configuration of anchors and target, the quality of received signals, environmental dynamics, and possible malicious activity. To address this, this work [110] defines a composite reliability index as:

$$\Upsilon_{tot} = \alpha\, \Upsilon_T + (1-\alpha)\, \Upsilon_{MU} \tag{3.5}$$

where $\Upsilon_T \in [0,1]$ represents the scenario-based component and $\Upsilon_{MU} \in [0,1]$ the threat-based component of the index, while the weight $\alpha \in [0,1]$ balances their contributions in the weighted average.

Scenario-based component—Υ_T quantifies the impact of anchor geometry and radio propagation conditions on the overall localization reliability. In the WLS algorithm, the weight matrix $\boldsymbol{W}$ defined in Equation (2.10) adjusts the influence of each anchor according to its proximity to the target, assigning higher weights to closer anchors. A detailed analysis showed that the trace of this matrix, $\mathrm{tr}(\boldsymbol{W}) = \sum_{i=1}^{N} w_i$, is the most effective indicator for representing this component of the reliability index. It is worth noting that, while Υ_T aims to reflect geometry and propagation effects, the weights w_i may also vary with the intensity of potential attacks rather than simply with the number of malicious anchors.

The results show that the weight matrix $\boldsymbol{W}$ is highly sensitive to variations in σ, with $\mathrm{tr}(\boldsymbol{W})$ decreasing sharply as σ_ω increases, as illustrated in Figure 3.4 (page 41). This monotonic, non-increasing trend with growing attack intensity confirms that $\mathrm{tr}(\boldsymbol{W})$ is a meaningful and reliable indicator of localization confidence.

To ensure Υ_T remains within the range $[0,1]$, the matrix trace is normalized as:

$$\Upsilon_T = \frac{\mathsf{tr}(\boldsymbol{W}) - \max\{\mathsf{tr}(\boldsymbol{W}(\sigma_\omega^{\min}))\}}{\max\{\mathsf{tr}(\boldsymbol{W}(\sigma_\omega^{\min}))\} - \min\{\mathsf{tr}(\boldsymbol{W}(\sigma_\omega^{\max}))\}} \tag{3.6}$$

where:

- $\max\{\mathsf{tr}(\boldsymbol{W}(\sigma_\omega^{\min}))\}$ is the maximum trace of $\boldsymbol{W}$ computed for the smallest value of σ_ω;
- $\min\{\mathsf{tr}(\boldsymbol{W}(\sigma_\omega^{\max}))\}$: the minimum trace of $\boldsymbol{W}$ computed for the largest value of σ_ω.

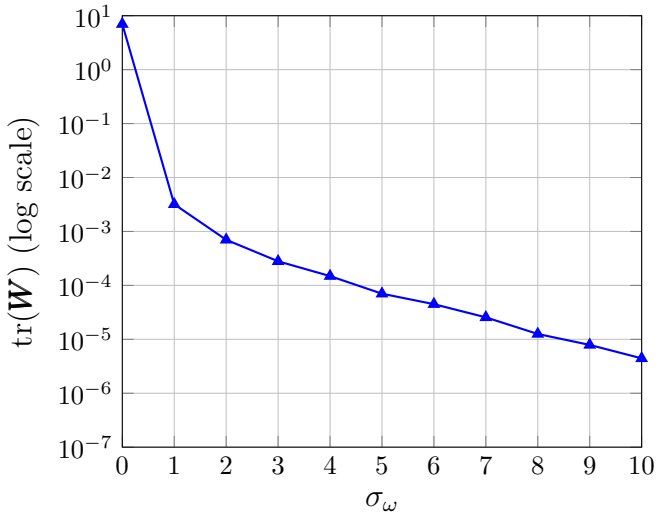


Figure 3.4: Log periodic curve $\mathrm{tr}(\boldsymbol{W})$ as a function of σ_ω.

Threat-related component—Υ_{MU} quantifies the impact of malicious anchors on the localization process, particularly those acting as byzantine attackers. As demonstrated in [86] and discussed in Section 2.4, the standard deviation of the RSS measurements between the i-th anchor and the target, σ_i, is strongly correlated with the presence of malicious behavior. To quantify this effect, the overall average of the standard deviation values across the entire system is considered:

$$\bar{\sigma} = \frac{1}{N} \sum_{i=1}^{N_A} \sigma_i \tag{3.7}$$

To quantify the influence of malicious anchors on Υ_{MU}, the measured $\bar{\sigma}$ is compared with the theoretical average $\bar{\sigma}_{th}$, expressed as a weighted combination of the standard deviation contributed by malicious anchors σ_{mal} and by honest anchors σ_{hon}:

$$\bar{\sigma}_{th} = \beta\, \sigma_{mal} + (1 - \beta)\, \sigma_{hon} \tag{3.8}$$

where $\beta = N_{MU}/N_A$ is the ratio of malicious anchors to the total number of anchors, and

$$\sigma_{mal} = \sqrt{\sigma^2 + \sigma_\omega^2} \qquad \sigma_{hon} = \sigma.$$

Figure 3.5 (page 43) illustrates the theoretical behavior of $\bar{\sigma}_{th}$ for different levels of malicious interference, considering a scenario with a maximum ratio $\beta = 3/7$. The approach can be

readily generalized to configurations with more anchors and, consequently, a higher fraction of malicious nodes. A heuristic analysis of these curves for varying β and σ_ω shows that the threat-related component is jointly influenced by the proportion of malicious nodes β and the normalized attack intensity $\check{\sigma}_\omega$, defined as

$$\check{\sigma}_\omega = \sigma_\omega / \sigma_\omega^{max}$$

where the normalization is performed with respect to the maximum attack intensity $\sigma_\omega^{\max}$, so that both $\check{\sigma}_\omega$ and β lie in the range $[0, 1]$.

Accordingly, the threat-related component Υ_{MU} is defined as

$$\Upsilon_{MU} = 1 - \frac{\check{\sigma}_\omega + \beta}{2} \tag{3.9}$$

In other words, stronger attacks or a larger proportion of malicious nodes lead to a lower value of the threat-related component of the reliability index. Since neither of these quantities can be directly measured, they must be estimated.

As noted earlier, a high standard deviation of the RSS measurements between an anchor and the target (σ_i) is a strong indicator of malicious behavior [86]. Accordingly, the i-th anchor is classified as malicious when σ_i exceeds the nominal value σ by more than a predefined threshold ζ:

$$\sigma_i > \zeta\sigma.$$

where $1(\cdot)$ denotes the indicator function, which equals 1 when the condition is satisfied and 0 otherwise.

Accordingly, the estimated attack intensity $\hat{\sigma}_\omega$ can be obtained by comparing the computed standard deviation in Equation (3.7) with the theoretical average in Equation (3.8). After simple algebraic rearrangement, $\hat{\sigma}_\omega$ is given by:

$$\hat{\sigma}_\omega^2 = \left[\frac{1}{\beta}\hat{\sigma} - \left(\frac{1}{\beta} - 1\right)\sigma\right]^2 - \sigma^2 \tag{3.10}$$

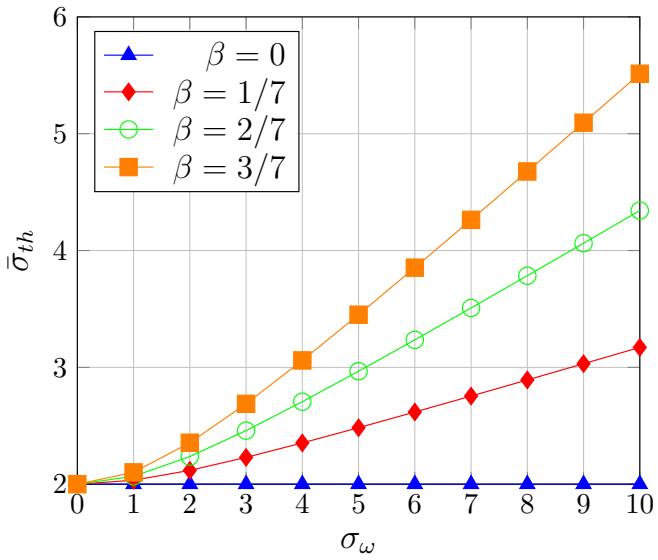


Figure 3.5: Theoretical average standard deviation $\bar{\sigma}_{th}$ as a function of σ_ω for different β.

3.4 Jamming Detection and Mitigation Approach

Jamming attacks, modeled as described in Section 2.4, can severely compromise RSS-based multilateration by either corrupting the received power through constructive/destructive interference or by rendering anchors entirely unavailable through DoS. To preserve localization accuracy under such conditions, this work introduces a detection-and-mitigation strategy specifically tailored for RSS-based WLS positioning.

The first step is to identify anchors affected by jamming. The detector exploits the statistical dispersion of the RSS samples collected from each anchor — a simple yet effective criterion whose intuition is visualized in Figure 2.3 (page 32). Let σ_i denote the standard deviation of the i-th anchor's RSS burst (see Equation (3.7)). Anchors subject to jamming typically exhibit anomalously large variability compared to nominal channel conditions, which makes σ_i a practical indicator of interference.

A classical approach is the SWLS method [86], which classifies anchor i as under attack, whether by constructive/destructive jamming or by a byzantine adversary, whenever

$$\sigma_i > \zeta \cdot \sigma \tag{3.11}$$

where σ is the expected standard deviation under normal conditions and ζ is a sensitiv-

ity threshold. Once jammed anchors are detected, their measurements are excluded from the multilateration process. The remaining anchors, assumed trustworthy, are then processed with the SWLS algorithm [86], a robust variant of WLS that maintains the same mathematical formulation of Equation (2.10) but operates on the pruned set of equations. By filtering out unreliable data, SWLS significantly limits the propagation of corrupted RSS values into the position estimate. A limitation of SWLS, however, emerges in sparse deployments or under strong jamming: by discarding suspicious anchors, it may reduce the number of valid measurements to the point where the WLS solver becomes inaccurate or even infeasible, since at least three anchors are required to ensure a consistent 2D localization.

To improve robustness in highly dynamic IoT environments, this work adopts an adaptive refinement of Equation (3.11). Instead of comparing σ_i only to a fixed multiple of σ, the threshold is set relative to the statistical distribution of all anchors' standard deviations:

$$\sigma_i > \mu_\sigma + \zeta \cdot \sigma_\sigma \tag{3.12}$$

Here, μ_σ and σ_σ denote the mean and standard deviation of the set $\{\sigma_i\}$ across all anchors, respectively. This adaptive rule, with ζ empirically determined as discussed in Section 4.4, highlights outliers by jointly considering the overall noise level and its variability among anchors. Building on this statistical detection, the proposed method integrates SWLS-based mitigation to preserve localization accuracy even under strong and dynamic jamming conditions. In doing so, it overcomes a key limitation of standard SWLS, where the exclusion of several anchors can leave too few measurements for accurate or even feasible WLS, by ensuring that a sufficient set of reliable anchors remains available for consistent 2D localization.

Chapter 4

Simulation and Experimental Results

This chapter presents a comprehensive validation of the methods proposed in this thesis. For each contribution, the simulation setup and corresponding results are first detailed to evaluate performance under controlled and reproducible conditions. Where applicable, the experimental setup and field–test outcomes are subsequently reported to assess real-world feasibility and confirm the findings obtained through simulation. This structure ensures that every proposed solution is rigorously examined from implementation to quantitative evaluation, enabling a thorough and systematic analysis of its accuracy, robustness, and security.

Across all analyses, localization accuracy is consistently quantified by the Root Mean Square Error (RMSE), expressed in meters, which measures the dispersion of position estimates with respect to the true location. Formally, it is defined as

$$\Theta = \sqrt{\frac{1}{B}\sum_{b=1}^{B}\left\|\boldsymbol{t} - \hat{\boldsymbol{t}}_b\right\|^2} \tag{4.1}$$

where B is the number of collected bursts (i.e., trials) and $\hat{\boldsymbol{t}}_b$ is the estimated position at the b-th burst. This common metric provides a consistent basis for comparing the accuracy of all proposed algorithms under both simulated and experimental conditions.

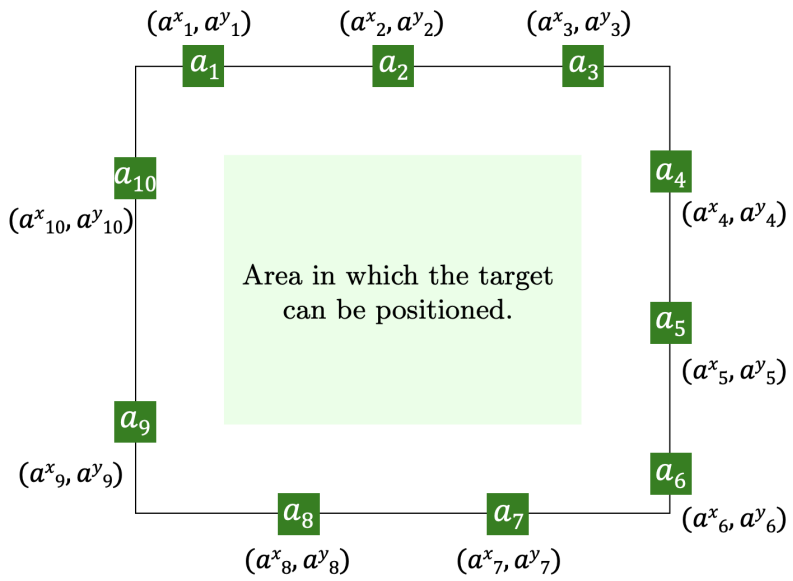


Figure 4.1: Illustrative scenario considered in a given random trial.

4.1 Validation of the Data Fusion–Based Hybrid Approach

4.1.1 Simulation Setup

Python was selected as the primary programming language for the simulation campaigns, ensuring straightforward code reuse in subsequent field experiments. To guarantee consistency between simulated tests and real-world validations, a geometrically simple environment was modeled, allowing direct replication in the physical deployment. As depicted in Figure 4.1 (page 46), the simulated area is a $50 \times 60\text{m}^2$ rectangle with $N = 10$ anchors, a quantity selected to ensure sufficient redundancy and geometric stability against potential node failures or attacks. To robustly validate performance across diverse topologies, anchor locations are randomized in each trial rather than fixed. This configuration offers a representative trade-off between coverage and computational complexity [111], although the proposed methodology is general and can be adapted to different values of N.

The target is allowed to move within an inner subsection of 30×40 m^2, a design choice that mitigates potential issues related to anchor proximity. Each anchor is assumed to be equipped with $M = 2$ wireless interfaces, representing two distinct technologies, hereafter denoted as T_1 and T_2.

Each localization instance, referred to as a trial B, consists of randomly placing the anchors along the scenario perimeter while keeping the target at a fixed position. Preliminary tests with varying B showed that increasing the count beyond 10^4 produces negligible improvements in the statistical reliability of the results. Based on this analysis, B is set to 10^4, which is sufficient to capture the variability introduced by measurement noise and different anchor–target configurations, thereby ensuring a robust and statistically sound evaluation of the proposed algorithms.

The measured RSS was simulated based on the actual distance between the anchors and the target, incorporating additive noise according to Equation (2.2). The transmission and channel parameters ($p_0 = -40$ dBm and $n = 4$) were derived from empirical measurements collected in outdoor and indoor parking facilities [104]. The selected parameters reflect the severe signal attenuation caused by typical obstacles in these environments, such as vehicles occupying parking slots, pedestrians, and structural pillars, thereby ensuring a faithful reproduction of a realistic, complex IoT environment. Measurements from each anchor have been gathered in bursts of $K = 10$ consecutive samples, as the default value. However, the impact of K (to 50 packets) is also investigated in the remainder of this Section. In terms of channel noise associated with shadowing and mirroring, the noise standard deviations have been set to $\sigma_{\mathrm{R},1} = 2$ for T_1 and $\sigma_{\mathrm{R},2} = (1 + \alpha)\sigma_{\mathrm{R},1}$ for T_2, with α ranging from 0 to 1 in steps of 0.25; Additionally, for robustness tests, a fading component σ_f ranging from 1 to 5 dB in steps of 1 dB is included;

The parameters used for the simulations are summarized in Table 4.1.

4.1.2 Simulation Results

The simulation results in this section validate the hybrid localization approaches introduced in Section 3.1, assessing their positioning accuracy and robustness under the channel conditions described in Section 4.1.1. Rather than comparing absolute RMSE values of different RSS-based techniques, the focus is on the relative behavior of the proposed hybrid algorithms (MAPS and RAPS) as simulation parameters and channel conditions vary, benchmarked against the conventional WLS operating in single-technology mode as commonly adopted in the literature.

It is important to note that MAPS and RAPS are designed for general range-based position-

Table 4.1: Simulation parameters.

Parameter	Value
Anchors' area	50×60 m^2
Target area	30×40 m^2
B	10^4
N	10
K	$[10, 50]$
α	$[0, 1]$
p_0	-40 dBm
n	4
$\sigma_{\mathrm{R},1}$	2 dB
$\sigma_{\mathrm{R},2}$	$(1+\alpha)\sigma_{\mathrm{R},1}$
σ^F	$[0, 5]$ dB

ing. Indeed, parallel validation using ToF approaches yielded results in line with those presented here, confirming the general applicability of the solutions [105]. However, to maintain consistency with other solutions analyzed in this paper, this section details only the RSS-based simulation results.

Accuracy Performance—First, the accuracy of the two hybrid algorithms is evaluated. As illustrated in Figure 4.2 (page 49), for a scenario in which the two technologies (T_1 and T_2) exhibit identical standard deviations ($\sigma_{\mathrm{R},1} = \sigma_{\mathrm{R},2}$, i.e., $\alpha = 0$), the single-technology method provides accuracy comparable to that of the hybrid MAPS algorithm. In contrast, the hybrid RAPS algorithm, which concurrently exploits measurements from both technologies, attains superior accuracy under the same conditions.

However, as α increases, indicating a growing disparity between T_1 and T_2, both hybrid algorithms exhibit performance that progressively falls between that of the two single-technology approaches. This trend reflects the limiting effect of the less reliable technology. In particular, the RAPS method is more strongly influenced by the degradation of T_2: while the RMSE of T_2 roughly doubles as α grows from 0 to 1, the RMSE of RAPS rises by about 64%.

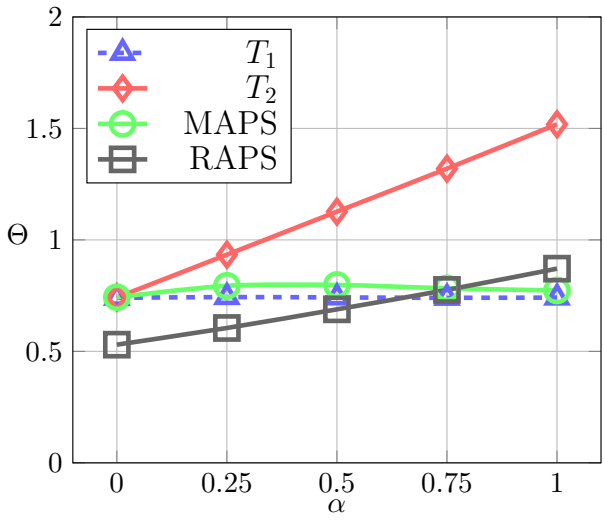


Figure 4.2: Simulated localization accuracy in terms of Θ as α varies, affecting the transmitting channel.

Conversely, MAPS increasingly favors the better-performing technology T_1 as the performance gap widens. When T_2 suffers degradation, MAPS tends to select T_1 for most anchors, thereby reducing the impact of T_2 on the final estimate. Even when accounting for statistical fluctuations within each burst interval, the RMSE of MAPS remains largely stable, confirming the robustness of this selective strategy in filtering out weaker technologies.

Subsequently, with α fixed at 0.25, the impact of increasing the burst size K from 10 to 50 is examined. The upper limit of $K = 50$ is motivated by practical constraints of real-time experimental deployment: with a sampling interval of 100 ms, acquiring 50 packets per burst requires 5 s, a duration that may be impractical for many IoT applications.

As shown in Figure 4.3 (page 50), increasing the burst size K enhances the value of Θ, as larger bursts better average out Gaussian noise due to shadowing and reflections. However, the gain progressively saturates beyond a certain K, while further increases also incur longer acquisition delays for each burst.

Robustness Performance—In addition to accuracy, it is crucial to evaluate the robustness of the proposed hybrid approaches under non-ideal propagation conditions. Real-world wireless channels are affected not only by Gaussian noise but also by phenomena such as multipath fading and temporal fluctuations. To capture these effects, the robustness tests extend the

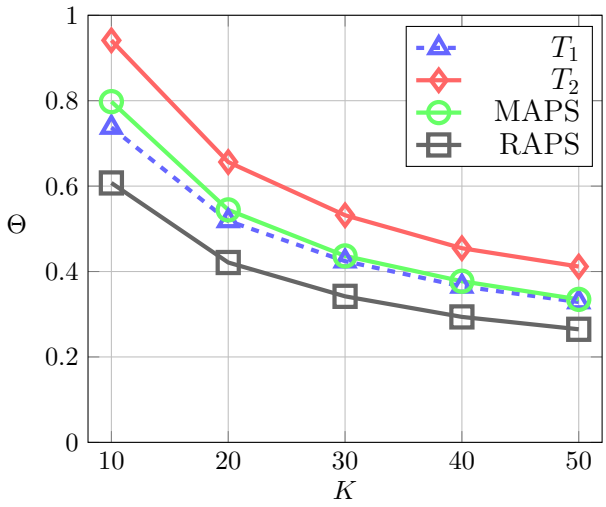


Figure 4.3: Simulated localization accuracy in terms of Θ as K varies, while keeping α constant.

channel model in (2.2) by introducing a Rayleigh fading component into the received power:

$$p'_{ijk} = p_{ijk} + \beta_{ijk} \tag{4.2}$$

where $\beta_{ijk} = \sigma^F \sqrt{-2 \ln u_{ijk}}$, being u_{ijk} independent and identically uniformly distributed numbers in the interval $[0, 1]$. The σ^f parameter characterizes the fading intensity [112].

This model is particularly significant in environments where signals are subject to reflections, diffraction, and scattering, which are typical of dynamic and heterogeneous scenarios, such as those in the IoT case under consideration [100].

For these robustness simulations, and based on the previous accuracy analysis, the noise parameters were set to $\sigma_{\mathrm{R},1} = 2$ dB and $\sigma_{\mathrm{R},2} = 4$ dB, with a burst size of $K = 10$.

As shown in Figure 4.4 (page 51), the RMSE of all schemes increases with the fading intensity σ^F, confirming that stronger multipath effects degrade localization performance.

Notably, the trends observed in the absence of fading remain valid under these harsher conditions, a finding that will be further examined in real-world experiments and highlights the importance of mitigating this class of noise.

Subsequently, with the fading intensity fixed at $\sigma^F = 2$ dB, additional tests were performed by varying the burst size K from 10 to 50, with the upper bound again chosen to balance accuracy and the sampling time required for each acquisition.

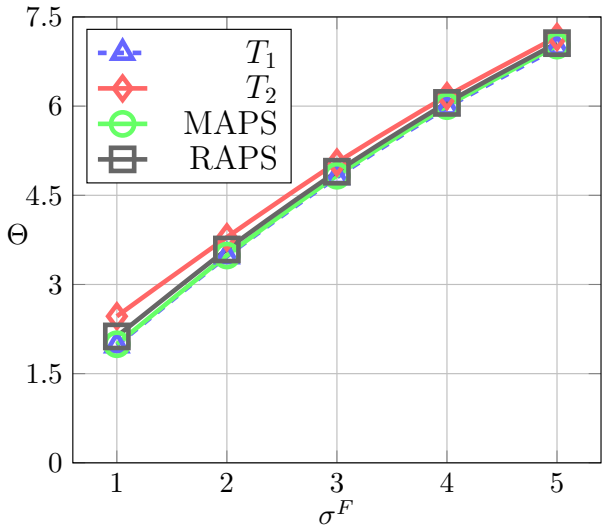


Figure 4.4: Simulated localization robustness results in terms of Θ as σ^F varies, affecting the transmitting channel.

As shown in Figure 4.5 (page 52), larger burst sizes yield improved localization accuracy; however, unlike the results in Figure 4.3 (page 50), the RMSE exhibits only marginal reductions as K increases. This indicates that, under fading conditions, the detrimental impact of multipath noise dominates, limiting the benefits of averaging a larger number of samples for target–anchor distance estimation.

4.1.3 Proof of Concept and Experimental Setup

To complement the simulation study, a real-world experimental campaign was conducted to validate MAPS and RAPS under realistic operating conditions. The objective is to confirm that the accuracy trends and robustness improvements observed in simulations are preserved in practice when using standard IoT wireless technologies.

The Proof of Concept (PoC) targets two widely deployed IoT interfaces, WiFi and BLE. To minimize implementation complexity and communication overhead, the system leverages native discovery mechanisms, including WiFi Probe Requests and BLE Inquiry packets, without introducing additional signaling. These messages, normally exchanged to detect nearby devices, provide the RSS measurements required for localization, enabling seamless integration with existing traffic.

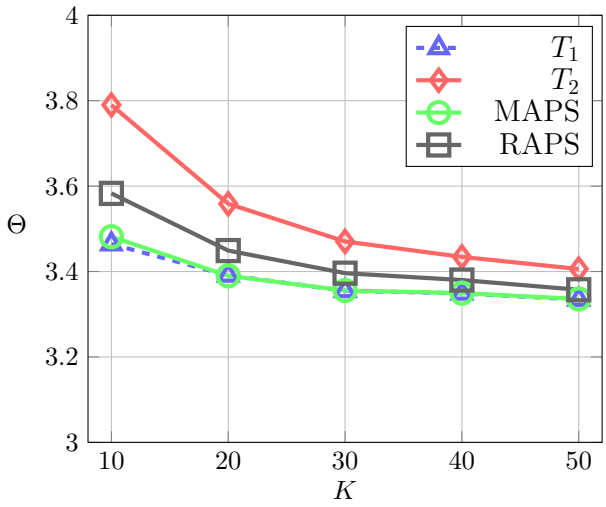


Figure 4.5: Simulated RSS-based localization robustness results in terms of Θ as K varies, while keeping σ^F constant.

The experimental platform consists of Raspberry Pi boards. The target is a Raspberry Pi 4 Model B equipped with its internal BLE interface and an external Realtek RTL8812BU USB WiFi adapter, providing sufficient computational capability for measurement and position estimation. Each anchor is implemented on a cost-effective Raspberry Pi Zero W with integrated WiFi and BLE, tasked only with transmitting discovery packets at a constant rate. All devices are mounted on tripods at a height of 1.5 m, identified as optimal through preliminary tests to minimize ground reflections and ensure stable reception. During data acquisition, the target remains stationary while collecting RSS samples from every anchor for 15 minutes per run.

Custom Python scripts manage data collection. On the target, the PyShark library captures WiFi probe requests [113], while Bluepy is used for BLE [114]. Packets are filtered by MAC address to retain only anchor-originating data. On each anchor, a lightweight script continuously scans for nearby networks and devices, thereby generating the required discovery packets.

Experiments were carried out in the parking area of the Faculty of Engineering, University of Cagliari, using three main scenarios (Figure 4.6) (page 54):

- *Scenario A*: an outdoor 21×30 m^2 rectangle with six anchors in LOS and the target fixed at $[0, 0]^T$;
- *Scenario B*: an extended 32×30 m^2 outdoor area with seven anchors—five in LOS and

two in NLOS—and the target fixed at $[4.6, 0]^T$;

- *Scenario C*: an indoor configuration replicating Scenario A with minor adjustments to account for pillars and parked vehicles;

- *Scenario* 0: a preliminary setup used to characterize propagation patterns, where the target remains stationary while a single anchor moves along a straight path from 5 m to 25 m away.

These modular scenarios are representative of larger deployments and are suitable for extending the framework to more complex environments while preserving the observed performance trends [115]. The datasets collected in these experiments are openly available [116].

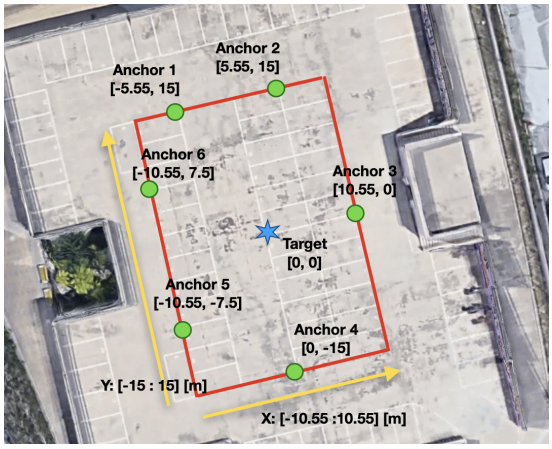
4.1.4 Experimental Results

This section evaluates the performance of the hybrid approaches presented in Section 3.1, with particular attention to localization accuracy and resilience to environmental noise. Their effectiveness is benchmarked against a conventional single-technology solution, using the experimental methodology detailed in Section 4.1.3.

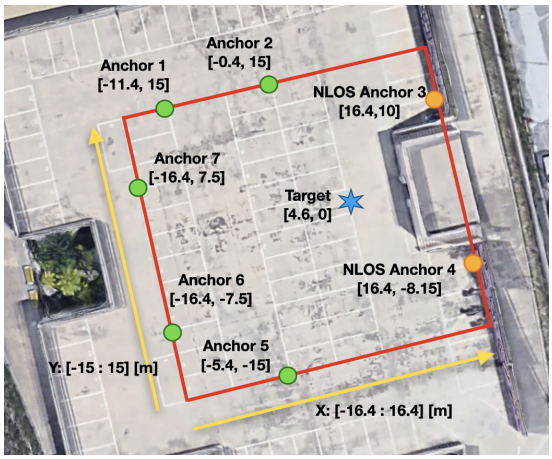
To ensure consistency with the simulation study, measurements were collected in bursts of $K = 10$ consecutive samples within a representative experimental scenario. Using the propagation data obtained from Scenario 0, the parameters of Equation (2.4) were set to $p_0 = -40$ dBm and $n = 4$. Consistent with the simulation settings, the WLS weight matrix was generated with $\sigma_j = 2$ dB for both interfaces. Although these parameter values primarily capture the effects of shadowing, the experimental environment also induces fading phenomena. As a result, the reported findings inherently account for the robustness of the hybrid approaches under realistic channel conditions.

Preliminary Statistical Analysis—As a first step, a statistical analysis of the collected RSS data was performed to gain a comprehensive understanding of its behavior across different technologies, in this case, WiFi and BLE. The analysis was carried out by separately examining each anchor and each scenario. In particular, Figure 4.7 (page 55) shows, for Scenario A[1], the

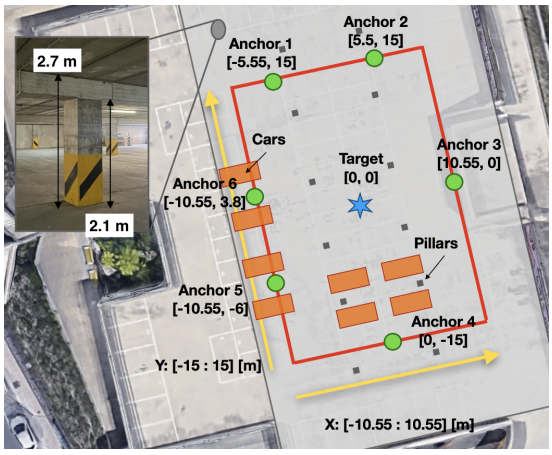
[1]Similar considerations apply to the other scenarios.



(a)



(b)



(c)

Figure 4.6: Experimental scenarios: (a) Scenario A, (b) Scenario B, and (c) Scenario C.

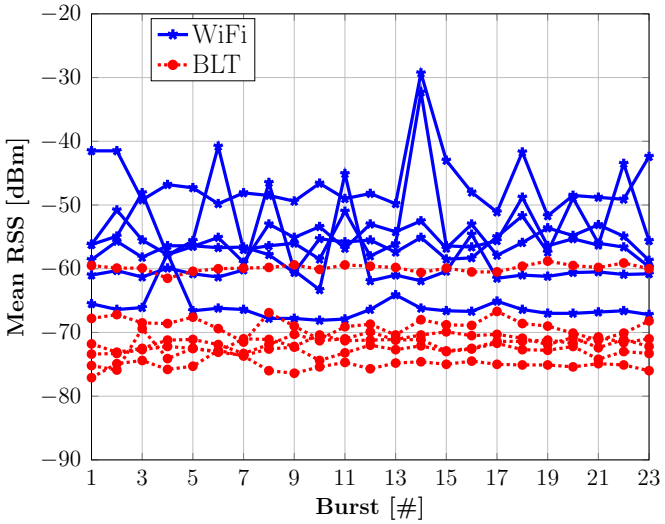


Figure 4.7: Mean RSS, as a function of time, in Scenario A for both WiFi and BLT technologies.

mean RSS as a function of time for both WiFi and BLE. In the plot, each curve tracks the temporal RSS variation for a specific anchor, with distinct color coding used to differentiate between the WiFi and BLE technologies. The results highlight that WiFi provides, on average, a higher received power than BLE, which is expected given the higher transmission power specified by the WiFi standard. However, due to stronger interference in the considered environment (e.g., concurrent WiFi connections within the university), BLE exhibits more stable measurements with lower temporal fluctuations, resulting in a more consistent RSS profile.

To gain a comprehensive understanding of the RSS data, a statistical analysis was performed by examining each anchor and scenario individually. Figure 4.8 (page 56) reports, for every scenario and anchor, the average standard deviation of the RSS measurements computed over time.

It is worth noting that, under fixed conditions, BLT consistently exhibits greater stability than WiFi across all the analyzed scenarios, confirming the trend already observed in Figure 4.7 (page 55).

Localization Performance—The localization performance of the proposed hybrid approaches, compared with conventional single-technology methods, is shown in Figure 4.9 (page 57) and quantified in terms of RMSE as defined in Equation (4.1). Specifically, the figure presents point clouds of the estimated positions for each method, while the corresponding RMSE values are summarized in Table 4.2.

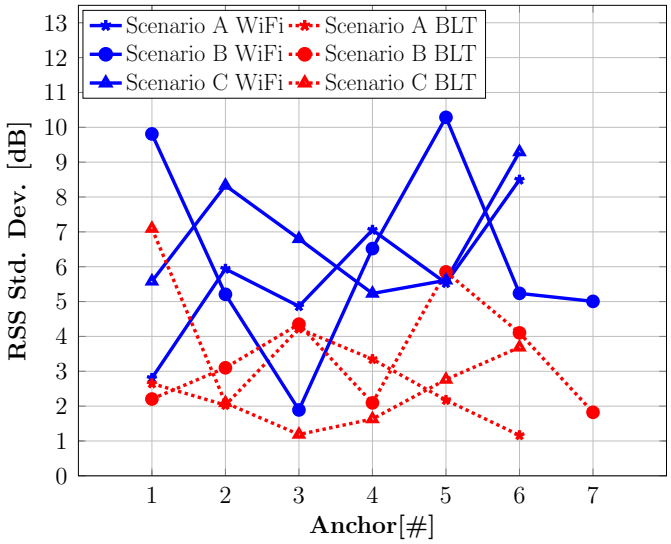


Figure 4.8: Average standard deviation (over time) of the RSS measurement for each scenario and anchor.

Table 4.2: Localization performance of the considered algorithms, expressed as Θ in meters.

Scenario	WiFi Θ	BLT Θ	MAPS Θ	RAPS Θ
A	2.10	1.42	1.95	1.89
B	5.13	7.32	5.33	5.52
C	2.36	2.54	2.49	2.39

The experimental findings closely align with the simulation outcomes reported in Section 4.1.2, confirming that the proposed hybrid approaches preserve both accuracy and robustness in real-world conditions. Across all scenarios, the hybrids consistently yield RMSE values lying between those of the individual technologies, reflecting the same trends observed in simulation, especially when the performance gap between the two technologies is significant. For example, while WiFi outperforms BLE in Scenario B, the opposite occurs in Scenarios A and C. These results demonstrate that, on average, the hybrid methods offer greater overall effectiveness and resilience, which is particularly advantageous when the better-performing technology cannot be predetermined. Furthermore, when considering only the hybrid solutions, their accuracy remains essentially stable across all tested scenarios.

To ensure consistency between the simulated and experimental analyses, the influence of

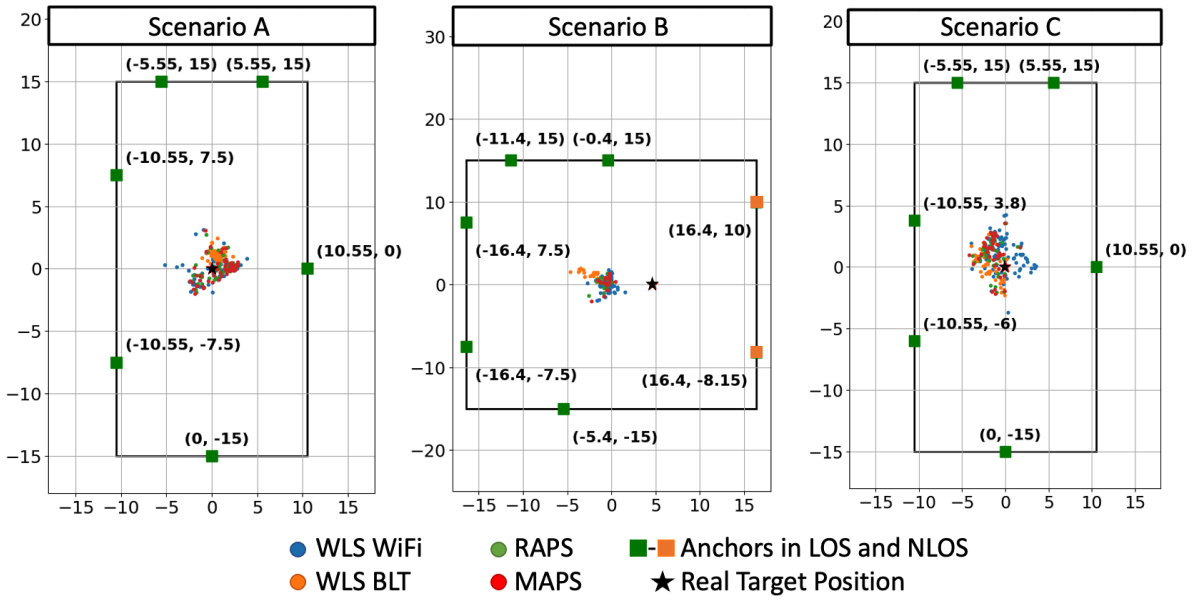


Figure 4.9: Localization performance of the considered algorithms in the investigated experimental scenarios.

the burst size K on the performance of the proposed algorithms was examined. For this purpose, K was varied in the range of 10 to 30.

The results shown in Figure 4.10 (page 58) reveal that increasing the burst size K provides only marginal RMSE improvements, within the range of statistical fluctuations. At the same time, larger K values introduce higher data acquisition latency, which can be critical for time-sensitive IoT localization services. These findings are consistent with the robustness analysis in Section 4.1.2, further confirming the significant influence of Rayleigh fading in real deployments.

Overall, the comparison between experimental and simulation outcomes demonstrates that the proposed hybrid approaches not only replicate the trends observed in controlled tests but also maintain stable accuracy and robustness in realistic IoT environments.

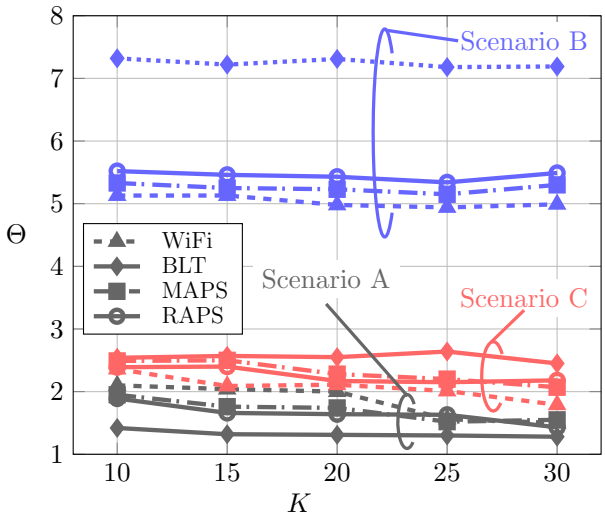


Figure 4.10: Experimental results in terms of Θ as K varies for the different considered scenarios.

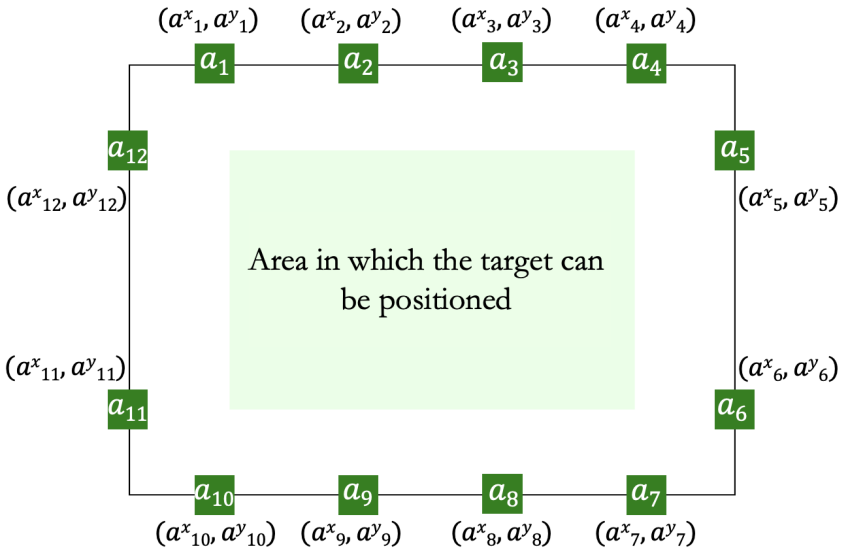


Figure 4.11: Simulated scenario considered for RSS dataset generation.

4.2 Validation of the Joint Techniques–Based Hybrid Approach

4.2.1 Simulation Setup

To evaluate the Joint Techniques–Based hybrid approach described in Section 3.2, simulations were carried out using the scenario depicted in Figure 4.11 (page 58). The simulator was implemented in Python, chosen to facilitate reproducibility and ensure seamless integration with subsequent experimental analyses.

A geometrically simple scenario was designed to ensure consistency between the simulated tests and the subsequent experimental phase. The environment consists of a rectangular area of 90×60 m^2, with 12 anchors uniformly placed along the perimeter at known coordinates. To avoid potential issues related to anchor proximity in multilateration, the target is allowed to move within a smaller subregion of 60×30 m^2. Reference Points (RPs) are arranged on a 1 m grid starting from $(0, 0)$, yielding a total of 1.891 RPs across the area of interest. The noise parameters, including both Gaussian and non-Gaussian components, follow the modeling described in Section 2.2.1.

Finally, the considered ML models have the hyperparameters summarized below.

- *RF*: number of trees in the forest $n\_estimators = 100$; maximum depth of the tree $max\_depth = 15$; minimum number of samples required to split an internal node $min\_samples\_split = 10$.
- *DT*: maximum depth of the tree $max\_depth = 15$; minimum number of samples required to split an internal node $min\_samples\_split = 10$.
- *kNN*: number of neighbouring data points that are considered when making predictions for a new data point $n\_neighbors = 15$; weight function used in prediction $weights = uniform$.

4.2.2 Simulated Dataset

The first dataset serves as the input for training the ML models that form the basis of the fingerprinting algorithm. It is generated using the scenario described above, where the path-loss model in Equation (2.2) is applied to simulate the RSS values for each RP as a function of the distance between the target and every anchor. For each RP, the target performs 10^3 acquisition acts; during each act, a burst of $K = 10$ RSS measurements is collected.

The resulting dataset, stored in CSV format, contains 14 columns, two specifying the RP coordinates and the remaining twelve providing the RSS values of the corresponding anchors, and a total of 1.891×10^7 rows.

A second group of datasets is created for performance analysis, following the same principles as the training dataset but incorporating controlled dynamics to reproduce environmental variability. To emulate anchor unavailability, a subset of anchors $N_{\text{null}} \in \{1, 2, \ldots, 5\}$ is deliberately prevented from transmitting packets to the target, resulting in *null* RSS values in the corresponding fields. This procedure produces five additional datasets, each with 14 columns and 1.891×10^7 rows, reflecting different levels of anchor unavailability and enabling the evaluation of system performance under progressively more challenging operating conditions.

4.2.3 Position Accuracy Benchmark

The Cramér–Rao Lower Bound (CRLB) provides a theoretical lower bound on the variance of any unbiased estimator, thereby defining its best achievable performance. In the context of RSS-based localization, the CRLB specifies the minimum possible positioning error attainable by any estimator at a given location, taking into account environmental conditions and measurement noise [117]. Given its role as a standard benchmark for evaluating localization techniques, the CRLB is adopted in this work as a reference for assessing the proposed methods [118].

The CRLB is defined as

$$\text{CRLB} = \text{trace}\left(\mathbf{F}^{-1}\right) \tag{4.3}$$

where F is the Fisher Information Matrix and trace refers to the sum of its diagonal elements. As defined in [86], F can be computed as

$$\mathbf{F} = [f_{xx}\ f_{xy};\ f_{yx}\ f_{yy}] \tag{4.4}$$

where each element can be calculated as follows

$$f_{\ell,m} = \frac{100 \times K \times n}{\ln^2(10) \times \sigma^2} \left[\sum_{i \in N_a} \frac{(a_{i,\ell} - t^{\ell})(a_{i,m} - t^{m})}{d_i^4} \right]$$

with $\ell, m \in \{x, y\}$.

The Fisher Information Matrix (F) captures how the scenario's geometry, the number and placement of anchors, and variations in RSS measurements caused by environmental noise jointly influence the estimation of key parameters such as the target's coordinates. Analyzing F provides valuable insight into the achievable accuracy of the localization algorithm and enables the derivation of theoretical performance limits, including the CRLB adopted in this work.

4.2.4 Simulation Results

The performance of the proposed algorithm is assessed primarily through the RMSE, the key evaluation metric formally defined in Equation (4.1). In addition, the CRLB, defined in Equation (4.3), is employed as a fundamental benchmark to quantify the theoretical minimum localization error. This dual evaluation allows us to compare the achieved RMSE against the best possible accuracy predicted by estimation theory, providing a rigorous reference for assessing the effectiveness of the proposed approach.

Figure 4.12a (page 62) illustrates that, under ideal conditions where all anchors are available, fingerprinting algorithms achieve meter-level accuracy (low Υ), in line with the CRLB, demonstrating the advantage of their simple architectural requirements in terms of anchor availability. By contrast, the WLS algorithm delivers noticeably lower accuracy in this fully accessible scenario. As the number of unavailable anchors N_{null} grows from 1 to 5, however, the performance of fingerprinting methods deteriorates rapidly, reflecting their dependence on the static radio map built during the offline training phase. In comparison, the WLS algorithm degrades much more gradually, showing greater resilience to anchor unavailability. These results indicate that while fingerprinting offers superior accuracy in stable, well-instrumented environments, multilateration-based localization provides a more robust solution when the network configuration is dynamic or partially impaired.

Building on the previously observed behavior of both techniques as N_{null} increases, the hybrid method is now evaluated under the same simulation setup. As shown in Figure 4.12b (page 62), integrating multilateration with fingerprinting yields a marked accuracy improvement over standalone fingerprinting. In particular, for N_{null} values between 1 and 5, the hybrid results closely follow the WLS trend, confirming that the multilateration component plays a key role in sustaining overall performance as anchor availability decreases. These tests also consider cases where N_{null} reaches up to 40% of the total anchors, a configuration useful for understanding extreme behaviors, though unlikely in carefully controlled environments. The hybrid approach proves especially effective for $N_{\text{null}} \leq 2$, where multilateration naturally outperforms fingerprinting and strengthens the combined estimator. For $N_{\text{null}} > 2$, multilateration increasingly dominates the hybrid response, helping maintain robustness under more dynamic

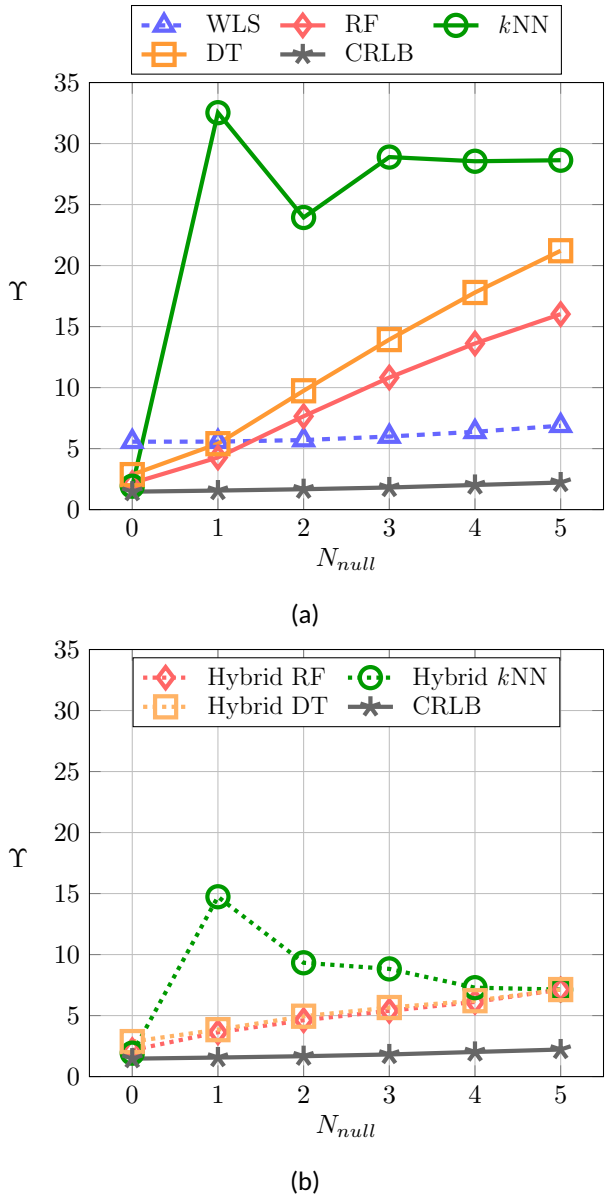


Figure 4.12: Simulated results comparing (a) standard and (b) hybrid approaches.

conditions. Finally, when comparing the two hybrid variants to one another, they mirror the relative performance hierarchy of their fingerprinting bases, while consistently benefiting from the added resilience provided by the multilateration component.

A detailed performance evaluation of the proposed algorithms is now presented for N_{null} values ranging from 0 to 2, focusing on the Cumulative Distribution Function (CDF) of the positioning error ϵ. Initially, only the standard algorithms are considered, since for $N_{\text{null}} = 0$ the hybrid method coincides with the fingerprinting estimates. As illustrated in Figure 4.13a

(page 64), fingerprinting algorithms based on kNN and RF deliver the best accuracy, achieving probabilities of about 65% and 40%, respectively, for $\epsilon < 2$ m. When N_{null} increases to 1, Figure 4.13b (page 64) reveals a clear change in trend: the hybrid approach combining RF with multilateration surpasses the others, reaching nearly 80% probability for $\epsilon < 4$ m. Notably, multilateration alone outperforms each standalone fingerprinting algorithm, demonstrating strong resilience when some anchors are unavailable. This pattern persists as N_{null} grows, as shown in Figure 4.13c (page 64), where multilateration remains the most effective technique and the hybrid solutions progressively converge toward its performance.

4.3 Validation of the Localization Reliability Index

4.3.1 Simulation Setup

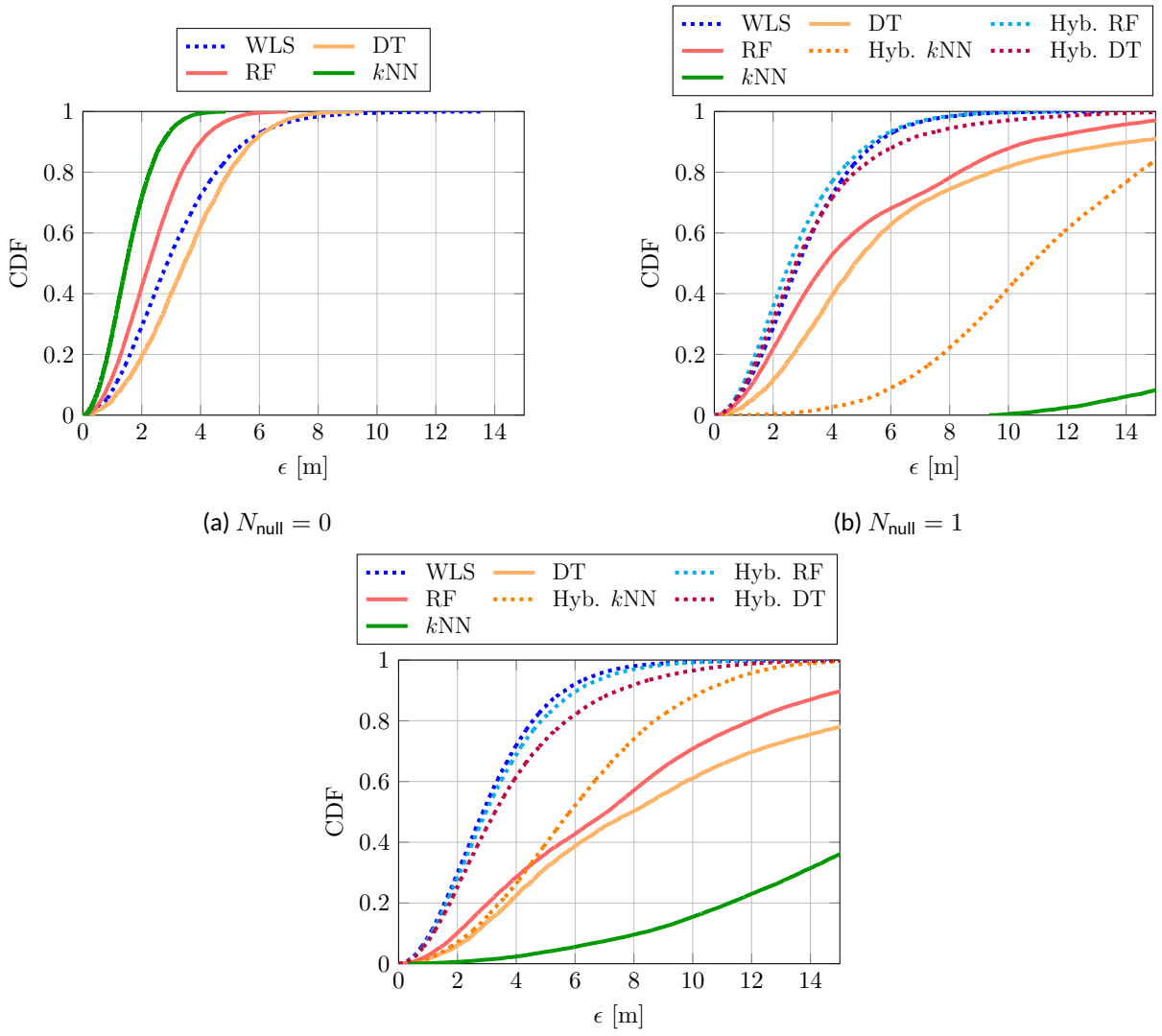
The validation of the proposed index is carried out entirely through simulations, which offer a flexible and controlled framework for analyzing the system's behavior at this stage of the study. MATLAB is employed as the computational environment to model the experimental scenario, encompassing target–anchor communications, malicious anchor activity, the localization process, and the computation of the reliability index.

The simulation configuration is illustrated in Figure 4.14 (page 65). In this setup, $N_A = 7$ anchors are deployed along the perimeter of a rectangular area measuring 100×50 m to evaluate the system's performance in a controlled yet realistic environment. The target is placed at 1000 randomly chosen locations within the red-shaded region, and for each location 1000 independent localization attempts are performed to ensure robust statistical analysis.

The anchors are positioned at fixed and known coordinates to guarantee reproducibility of the experiments. Specifically, their (x, y) locations, expressed in meters, are as follows:

This layout ensures a balanced geometric configuration around the area of interest, providing both sufficient coverage and diversity in anchor geometry to accurately assess the performance of the proposed reliability index.

Consistent with the thesis's broader methodology, a log-normal shadowing model is adopted with $n = 4$ and $\sigma = 2$ dB. The high path loss exponent ($n = 4$) reflects a complex environ-



(a) $N_{\text{null}} = 0$

(b) $N_{\text{null}} = 1$

(c) $N_{\text{null}} = 2$

Figure 4.13: Empirical CDF of ϵ [m] for the algorithms under analysis: (a) $N_{\text{null}} = 0$, (b) $N_{\text{null}} = 1$, and (c) $N_{\text{null}} = 2$.

ment where dense obstacles cause rapid signal decay, while the standard deviation ($\sigma = 2$ dB) captures stochastic fluctuations due to diffraction and scattering. These parameters collectively define a challenging and cluttered communication scenario, in line with standard literature [100].

To emulate malicious behavior, specifically a byzantine attack following the threat model in 2.4, the attack-related parameters are varied as follows: σ_ω ranges from 1 to 10, the number of

Table 4.3: Anchor coordinates used in the simulated scenario.

Anchor	x **[m]**	y **[m]**
a_1	50	-20
a_2	50	20
a_3	0	25
a_4	-30	25
a_5	-50	0
a_6	-30	-25
a_7	30	-25

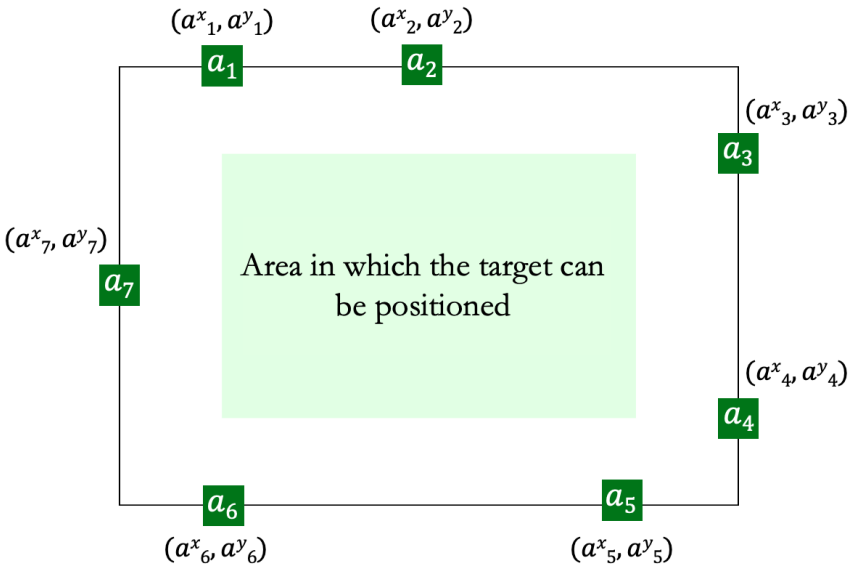


Figure 4.14: Simulated scenario for conducting the investigation.

malicious anchors N_{MU} ranges from 1 to 3, and the detection threshold is fixed at $\zeta = 1.5$. This choice of ζ provides a reasonable margin, as $\zeta\sigma$ serves as the limit beyond which an anchor is declared malicious.

For each configuration, the simulator outputs the actual target position, the estimated position, and the corresponding reliability index for every localization act. To balance the two components of the reliability index in Equation (3.5), the scenario-based and the threat-related terms, a value of $\alpha = 0.5$ is adopted, assigning equal importance to both. Future investigations

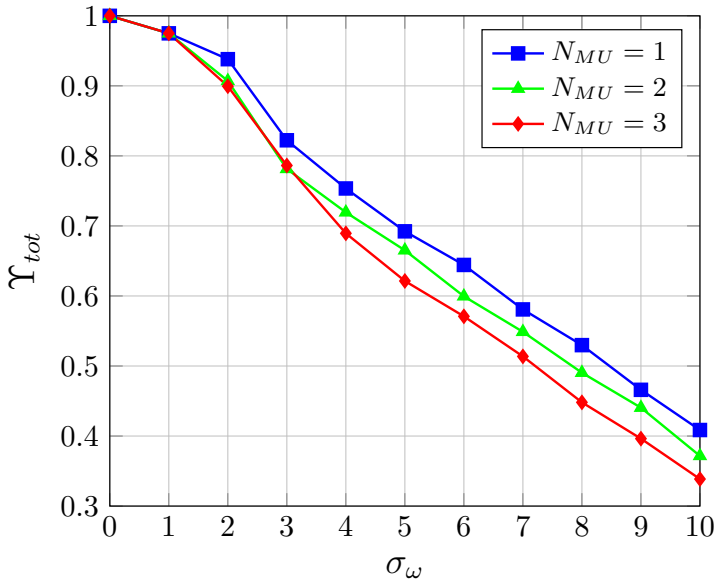


Figure 4.15: Υ_{tot} as a function of σ_ω

will explore different values of α and the integration of additional parameters to further refine the proposed index. Similar considerations apply to alternative deployment scenarios.

4.3.2 Simulation Results

The results, shown in Figure 4.15 (page 66), illustrate the behavior of Υ_{tot}, as a function of σ_ω, with N_{MU} varying from 1 to 3.

It can be observed that consistent trends emerge across all cases, confirming that the proposed composite reliability index effectively captures both the operating scenario conditions and the presence of malicious anchors. As anticipated, increasing the influence of malicious nodes, whether through a larger number of compromised anchors or higher attack intensity, leads to a corresponding decrease in the reliability index.

To validate the effectiveness of the proposed index, it is now compared with the localization accuracy expressed in terms of the RMSE, defined as in Equation (4.1).

In particular, for each configuration, the CDF of the normalized RMSE ($\overline{\Theta}$), scaled to the maximum observed value, is generated together with the CDF of the corresponding Υ_{tot} computed for every position estimate. As shown in Figure 4.16 (page 67), which reports the case of $N_{MU} = 3$ and σ_ω varying from 1 to 10, the two CDFs exhibit almost identical trends, yielding a

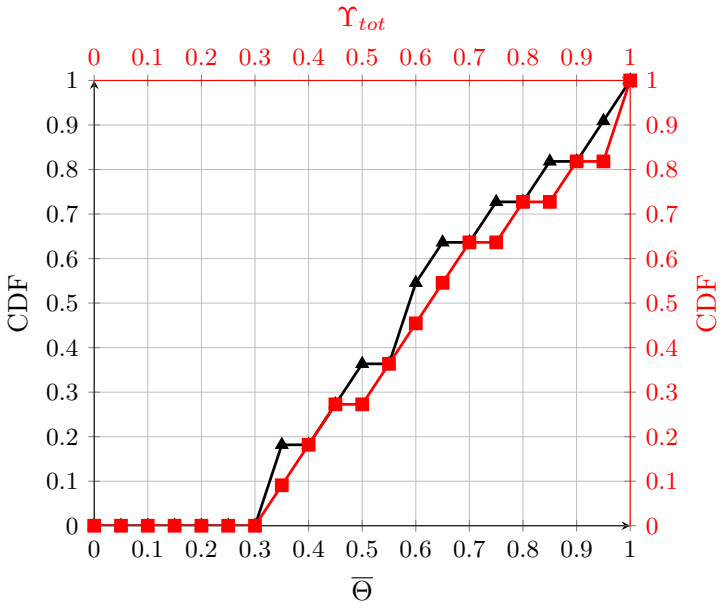


Figure 4.16: Comparison of CDFs for $\overline{\Theta}$ and Υ_{tot}, with $N_{MU} = 3$

Table 4.4: Correlation coefficient ρ between the normalized RMSE and the proposed reliability index, for $N_{MU} \in [1, 3]$.

N_{MU}	ρ
1	0.9872
2	0.9966
3	0.9931

Pearson correlation coefficient $\rho = 0.9931$.

A similar analysis performed across different N_{MU} configurations confirms this strong relationship (see Table 4.4), with ρ consistently ranging between 0.9872 and 0.9966.

These high correlation values demonstrate that the proposed reliability index reliably mirrors the actual localization accuracy: higher reliability directly corresponds to improved positioning performance, thereby validating the effectiveness of the presented approach.

4.4 Validation of Jamming Detection and Mitigation

4.4.1 Simulation Setup

For this validation step, the focus is on assessing the impact of jamming attacks on localization accuracy through simulations in a flexible, controlled setup. Using MATLAB, the scenario is modeled to reproduce target–anchor interactions, generate jamming signals, and apply WLS and SWLS for position estimation. WLS minimizes a weighted sum of squared residuals, prioritizing measurements from closer anchors, while SWLS improves upon this by incorporating the statistical distribution of measurement errors. The adaptable simulation framework enables systematic variation of jamming conditions, offering a solid basis to investigate their influence on localization and to evaluate the effectiveness of mitigation strategies.

The reference simulation scenario, both in terms of geometry and anchor deployment, is consistent with the one described in Section 4.3 and shown in Figure 4.14 (page 65). In this setup, communications between target, anchors, and jammer are modeled using the fundamental equations in (2.2) and (2.12). The parameters are configured as $p_0 = -40$ dBm, $n = 4$, and $\sigma = 2$, which represent standard values in wireless communication [100]. The interference coefficient is fixed at $\alpha = 0.2$, while the jammer is allowed to be positioned arbitrarily within the scenario area.

This reference scenario is further detailed into two distinct configurations, defined by the relative placement of the target and the jammer.

Setup #1: In this configuration, the target and jammer share the same position at $(-25, -5)$. For the constructive–destructive interference case, the number of affected anchors N_{MU} is varied from 1 to 7, progressively analyzing the impact from the closest to the farthest anchor. In the DoS attack scenario, N_{MU} ranges from 1 to 4, assessing how localization degrades when specific anchors are disabled by jamming. Each localization attempt is repeated over 1000 independent trials (B) to ensure statistical reliability.

Setup #2: Here, the target explores the entire red area depicted in Figure 4.14 (page 65), covering all possible positions with a spatial resolution of 1 m. This broader setup enables a comprehensive evaluation of localization performance across the scenario rather than at a fixed target–jammer location. For each position, different malicious anchor configurations

($N_{MU} = 1$ to 7) are tested, with $T = 1000$ per combination. This extensive analysis strengthens statistical robustness and provides an in-depth understanding of jamming effects across the entire rectangular area.

4.4.2 Simulation Results

This section reports the main results of these experiments. First, Setup #1 is used to highlight how each jamming strategy disrupts the position estimation process, providing qualitative evidence of the distortions introduced by malicious users. Then, Setup #2 is employed to quantify the performance degradation using the RMSE metric, while also evaluating the effectiveness of the SWLS algorithm in mitigating interference.

The results presented in the following figures and tables serve to clearly illustrate the differences between the two attack types, as well as the advantages and limitations of statistical-based mitigation strategies.

Impact of Jamming on Position Estimation—Setup #1 is adopted in this part to provide a qualitative assessment of how different jamming strategies alter the localization process. The focus is on distinguishing between constructive–destructive interference and DoS attacks.

When interference is present, the corrupted signals from jammed anchors introduce a bias that repels the estimated positions away from the affected anchor. This repulsion effect is especially visible for $N_{MU} = 1$, as shown in Figure 4.17 (page 70), where the estimates cluster in displaced regions depending on which anchor is compromised. Although the analysis has been extended to all values of N_{MU} from 0 to 7, only the representative cases $N_{MU} = (1, 3, 5)$ are plotted for clarity.

In the DoS case, the disruption mechanism differs: jammed anchors are completely removed from the localization process, and the system must rely on the remaining ones. As reported in Figure 4.18 (page 70), the absence of information enlarges the uncertainty area around the true target, leading to a wider and less dense cloud of estimates. This trade-off contrasts with the interference case, where all anchors contribute but with degraded quality. These results confirm that DoS attacks primarily reduce the quantity of usable data, while interference attacks degrade the quality of the data itself.

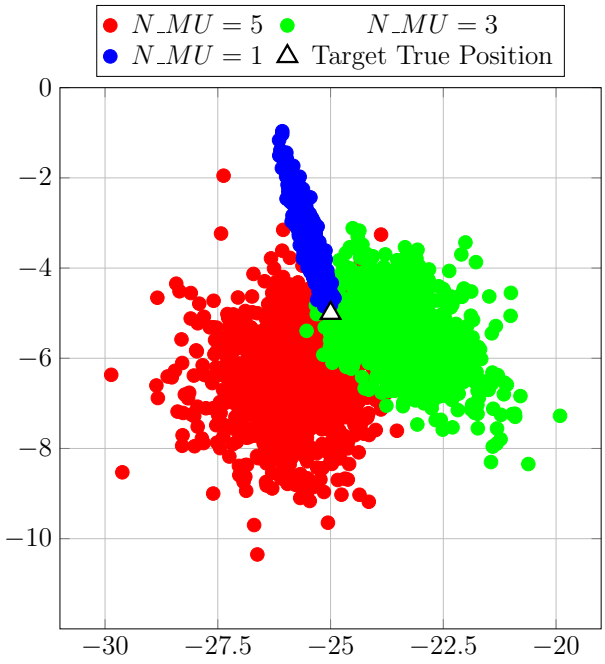


Figure 4.17: WLS position estimation under constructive-destructive jamming interference for N_{MU} equals 1, 3, and 5.

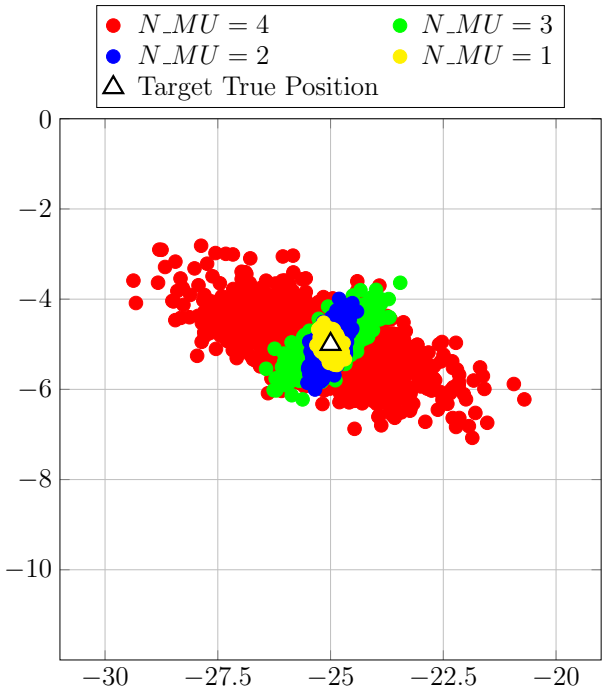


Figure 4.18: WLS position estimation under jamming DoS for N_{MU} equals 1, 2, 3, and 4.

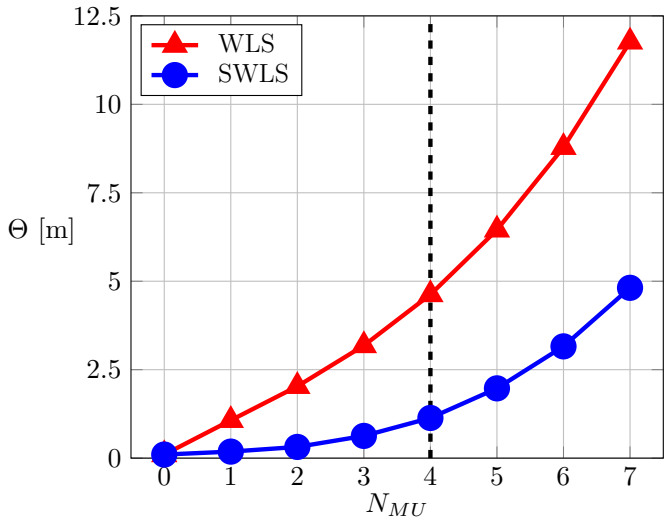


Figure 4.19: Comparison of Θ for WLS and SWLS as N_{MU} varies

Performance Evaluation and Mitigation Strategy—Setup #2 is then used to analyze the impact of constructive–destructive interference in more detail and to test a mitigation approach. This type of attack is considered the most critical, as the anchors remain active but the reliability of their measurements is compromised.

The analysis relies on the RMSE to quantify the deviation between estimated and actual positions, as defined in Equation (4.1). Figure 4.19 (page 71) shows that with the WLS algorithm, Θ grows rapidly with the number of malicious users, reaching about 11.8 m for $N_{MU} = 7$. In contrast, SWLS achieves lower errors, rising only up to around 4.8 m under the same conditions, thus demonstrating its effectiveness in reducing the impact of interference.

Nevertheless, SWLS faces limitations when too many anchors are jammed. By discarding anchors with anomalous RSS variance, the algorithm may end up with fewer than three anchors, making multilateration impossible. To address this, the malicious-anchor detection rule is refined, replacing the fixed-threshold condition in Equation (3.11) with the adaptive formulation in Equation (3.12). This makes the detection sensitive to the system's average noise level and the variability across anchors, improving robustness. An empirical choice of $\zeta = 0.2$ was found to balance detection accuracy and reliability.

Table 4.5 summarizes these outcomes. For high jamming levels ($N_{MU} = 4$–7), SWLS mostly underestimates the number of malicious anchors, but missed multilateration attempts remain

Table 4.5: Performance of SWLS in identifying jammed anchors and multilateration failures.

N_{MU}	N_{MU} **Underest. (%)**	N_{MU} **Overest. (%)**	N_{MU} **Exact Identif. (%)**	**Missed Multilat. (%)**
7	100	0	0	0.9134
6	99.99	0	0.0021	0.6220
5	99.72	0.00003	0.2803	0.2803
4	96.94	0.0008	3.06	0.0007
3	85.82	0.23	13.96	0.0102
2	54.36	5.23	40.41	0.0675
1	30.86	30.86	69.14	0.2899

below 1%. For lighter jamming conditions, exact identification improves (up to 69.14% for $N_{MU} = 1$), showing that the modified SWLS approach enhances detection and maintains localization accuracy under interference.

Chapter 5

From Research to Impact: a Smart Agriculture Case Study

Over the three years of technological research and development presented in this thesis, the focus has gradually moved beyond purely academic investigation toward the creation of concrete added value. This chapter does not aim to re-discuss the technical details of the methods introduced earlier, but rather to demonstrate their practical significance by showing how LBS can prove crucial even in real-world scenarios.

In this perspective, the chapter presents Agricultural Geolocation and Resource Optimization System (AGROS), an entrepreneurial idea that builds upon the trustworthy LBS framework and localization techniques developed in this thesis, while extending them into a broader IoT-based platform for smart agriculture. The integration of these technologies within AGROS serves as a PoC: it validates the idea that LBS are not only a theoretical construct, but also a key enabler of innovation and sustainability in practice.

The choice of smart agriculture as a case study is not accidental. Sardinia, my homeland, is an island where agriculture represents far more than an economic activity: it is a cornerstone of cultural identity, local traditions, and territorial heritage. By embedding the trustworthy LBS framework into an IoT ecosystem tailored for agriculture, this work illustrates how rigorous scientific research can evolve into entrepreneurial innovation, supporting both environmental stewardship and economic growth.

5.1 Agricultural Geolocation and Resource Optimization System (AGROS)

Traditional agriculture faces multiple challenges, such as water scarcity, rising energy costs, and the need for sustainable practices that limit waste while ensuring high productivity. Existing solutions for precision agriculture often rely on GPS-based services, which, despite their widespread adoption, suffer from limitations in rural and semi-indoor environments: poor accuracy under vegetation or hilly terrain, high dependency on costly high-precision receivers, and incompatibility with low-power IoT devices.

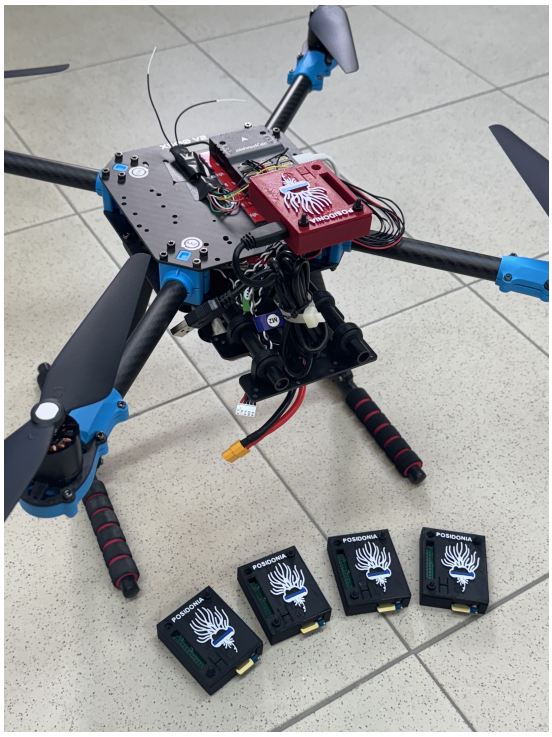
AGROS addresses these challenges by introducing localization technologies independent of GPS, enabling cost-effective, energy-efficient, and resilient solutions adaptable to heterogeneous agricultural contexts. By providing granular, real-time awareness of soil conditions, crops, and agricultural assets, the system supports data-driven decision-making, ensuring optimized use of resources such as water, fertilizers, and energy.

AGROS is built upon the POSIDONIA framework, extending its trustworthy LBS architecture to the agricultural domain. The system is designed as a modular, multi-layered platform that integrates:

- *IoT-based sensing*: geolocated, low-cost sensors are deployed across the field to monitor key parameters such as soil humidity, temperature, and luminosity. Associating each measurement with a precise position enables high-granularity monitoring and forms the foundation of the context-aware services envisioned in POSIDONIA.

- *Mobile robotics*: autonomous Unmanned Aerial Vehicles (UAVs, i.e., drones) and Unmanned Ground Vehicles (UGVs, e.g., robotic rovers) extend monitoring capabilities by collecting geo-referenced data even in GPS-denied areas (see Figure 5.1, page 75).

- *GPS-free positioning and reliability*: the localization algorithms and trust mechanisms developed in this thesis are embedded into both static sensors and mobile robots, ensuring accurate geo-referenced data collection and autonomous navigation even in GPS-denied environments, thus overcoming the limitations of satellite-based systems.



(a) Prototype UAV used in AGROS

(b) Prototype UGV used in AGROS

Figure 5.1: Mobile robotic platforms integrated in the AGROS system: (a) UAV and (b) UGV.

- *Edge and cloud processing*: consistent with POSIDONIA's layered design, data is first pre-processed at edge nodes and then forwarded via Low-Power Wide-Area Network (LPWAN) (e.g., LoRa) or mobile networks to the cloud. This hybrid edge–cloud chain reduces latency, improves scalability, and enhances system resilience.

- *Decision support and digital twin*: leveraging the trust and reliability concepts of POSIDONIA, AGROS provides farmers with interactive dashboards, anomaly alerts, and predictive insights through a digital twin of the field. This enables proactive and data-driven management of resources such as water, fertilizers, and energy.

5.2 Field Validation and Impact

The first validation of AGROS was carried out in two experimental testbeds in Sardinia. In the first site, a small olive grove in Dorgali (Figure 5.2a, page 76), the localized deployment of sen-

(a) Olive grove testbed in Dorgali

(b) Vineyard testbed in Sardara

Figure 5.2: Experimental testbeds for AGROS validation.

sors highlighted significant micro-variations in temperature, UV exposure, and soil humidity even within a limited area. The second site, a larger vineyard in Sardara (Figure 5.2b, page 76), provided a more complex environment characterized by heterogeneous terrain and multiple crops, which was used to test the integrated monitoring system combining fixed sensors and autonomous robots.

The results demonstrated that even within relatively small agricultural plots, significant micro-climatic differences can substantially influence crop health and productivity. Variations in soil humidity, temperature, and UV exposure were observed across neighboring areas, underscoring the importance of high-granularity monitoring. Such fine-grained visibility translates directly into actionable insights; the platform's dashboard, shown in Figure 5.3 (page 78), provides operators with the tools for this granular land monitoring and data-driven decision support. For instance, the ability to precisely identify water-stressed zones facilitated targeted irrigation, reducing unnecessary water usage while optimizing both resource efficiency and op-

erational costs. Beyond irrigation, these findings suggest that localized monitoring can support precision interventions in fertilization and pest control, ultimately enhancing sustainability, improving yields, and reducing the environmental footprint of agricultural practices.

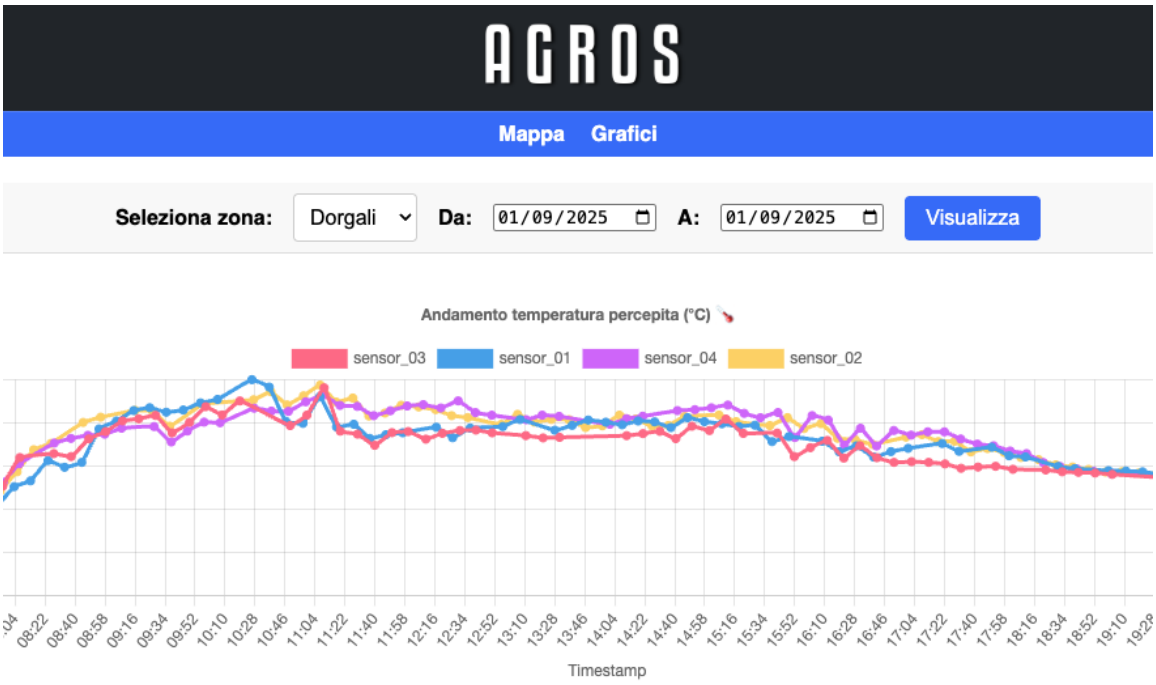
Alignment with the POSIDONIA Framework

This field validation serves as a concrete instantiation of the architectural principles envisioned in the POSIDONIA project. Specifically, the deployment mirrors the heterogeneous IoT scenario discussed in previous chapters, where a diverse set of static and mobile nodes operates within a distributed architecture via the Fog-Edge-Cloud continuum. In the context of AGROS, the abstract layers of POSIDONIA are mapped to physical components as follows:

- **Heterogeneous IoT Network (Physical Layer):** Composed of the low-power environmental sensors and the mobile robotic units (UGVs/UAVs). These represent the heterogeneous data sources that generate raw telemetry and position data, adhering to the green design by maintaining minimal power consumption.
- **Edge/Fog Layer:** Constituted by the Raspberry Pi-based aggregation nodes and gateways. These devices act as the intelligent middle layer responsible for data collection, preliminary local processing (e.g., filtering and protocol translation), and secure forwarding to the internet. This layer implements the local intelligence required to manage the connectivity between the resource-constrained field devices and the global infrastructure.
- **Cloud Layer and Digital Twin:** Represented by the centralized AGROS platform and backend analytics. Here, the computationally intensive operations, such as historical time-series analysis, global anomaly detection, and the DT visualization, are offloaded from the edge, ensuring system scalability and interoperability.

Furthermore, this setup validates the necessity of the trustworthy LBS mechanisms proposed in the thesis. In such a resource-constrained scenario, the reliability of the position and data source, originating from the heterogeneous network and processed at the edge, is critical. Untrusted data could lead to incorrect automated decisions (e.g., erroneous irrigation com-

(a) Map view for spatial monitoring.



(b) Chart view for time-series data analysis.

Figure 5.3: The AGROS platform dashboard. (a) The map view provides tools for granular spatial monitoring, while (b) the chart view shows time-series analysis.

mands triggered by the cloud), mirroring the threat mitigation logic central to the POSIDONIA vision.

It is important to note that the testbeds have been active only for a few months, and the current focus is primarily on validating the LBS concept and the feasibility of precise monitoring in smart agriculture. The integration of UAVs and UGVs is, at this stage, being tested in laboratory environments, with particular emphasis on autonomous navigation and GPS-free positioning techniques. These include vision-based and LiDAR-based guidance, complemented by the support of RSS-based localization methods developed in this thesis.

AGROS thus represents the natural evolution of the POSIDONIA framework, transforming rigorous academic research into a real-world platform that bridges IoT, trustworthy localization, and sustainable agriculture. This case study confirms that the LBS principles discussed in this thesis extend beyond theoretical analysis, enabling tangible value in strategic domains where reliability, resilience, and sustainability are essential drivers of innovation.

Chapter 6

Conclusions and Future Work

This thesis has presented a comprehensive framework for trustworthy and GPS-free localization in IoT environments, addressing the full research pipeline from theoretical design to simulation, experimental validation, and real-world deployment. The proposed contributions have tackled fundamental challenges of LBS in terms of *accuracy*, *robustness*, and *security*, introducing hybrid algorithms, a novel reliability index, and enhanced mitigation strategies against adversarial threats such as jamming.

By integrating the proposed solutions into a unified framework, this research advances the state of the art in IoT localization, showing that reliable and energy-efficient LBS can be achieved using commodity devices and standard wireless technologies. The presented case study in smart agriculture confirms the practical relevance of LBS and the proposed methods by demonstrating how scientific innovation can be transformed into tangible value through real-world deployments. In doing so, this thesis highlights the potential of trustworthy GPS-free localization to deliver accurate, resilient, and reliable LBS across diverse sectors, where they serve as key enablers of innovation and sustainability.

Overall, this work lays the groundwork for the next generation of trustworthy LBS in IoT, combining methodological innovation with practical applicability and paving the way for future research and industrial adoption.

6.1 Summary of Contributions

This thesis presented a comprehensive framework for trustworthy, GPS-free IoT localization, from theoretical design to experimental validation and real-world application. The main scientific and technical contributions, along with the key results achieved, are summarized as follows:

- *Data Fusion–Based Hybrid Approach*—MAPS and RAPS are proposed to leverage simultaneous RSS measurements from heterogeneous wireless technologies. MAPS dynamically selects the most reliable technology per anchor, while RAPS fuses all measurements via multi-interface WLS. On average, both hybrid approaches improve RMSE over single-technology baselines, proving particularly valuable when the most reliable technology is unknown a priori. Specifically, RAPS achieves the highest accuracy when technologies have comparable reliability (at higher complexity), whereas MAPS is more efficient when one clearly dominates. From a security perspective, MAPS further enhances robustness by discarding tampered or unreliable measurements.

- *Joint Techniques–Based Hybrid Approach*—A novel approach is presented that combines range-free fingerprinting with range-based multilateration to improve accuracy and robustness under varying anchor availability. Simulations show that the method matches standard fingerprinting when $N_{null} = 0$, while outperforming multilateration. As N_{null} increases, the hybrid approach surpasses traditional fingerprinting, effectively handling anchor unavailability and obstacles, and enhancing localization reliability in dynamic environments.

- *Reliability Index*—A composite index was introduced to quantify the trustworthiness of each location estimate by combining scenario geometry, channel conditions, and malicious activity. The index showed a very high correlation with the normalized RMSE (Pearson coefficient $\rho > 0.98$), proving its ability to predict positioning accuracy and to signal the presence of compromised anchors.

- *Security mechanisms against Jamming*—An enhanced SWLS method was proposed, incorporating an adaptive statistical threshold to identify and exclude jammed anchors

without compromising localization feasibility. The improved SWLS reduced the localization error by more than 50% compared to standard WLS under constructive–destructive interference, and maintained localization feasibility even when multiple anchors were jammed.

- *Extensive experimental validation*—All proposed hybrid algorithms, the reliability index, and the jamming detection and mitigation mechanism were evaluated through intensive simulations. Additionally, the data fusion–based hybrid approach, central to this research, was validated in real-world field experiments using WiFi and BLE technologies. Results from both simulations and experiments consistently confirm the promise and effectiveness of these solutions.

- *Application to Smart Agriculture*—The trustworthy LBS framework was applied to a real-world smart agriculture case study, integrating advanced IoT sensing and localization techniques. The deployment demonstrated how LBS can support precision farming and resource optimization, highlighting their potential to create tangible value in sectors where sustainability, tradition, and technological innovation converge.

Overall, the research provides a unified, experimentally validated framework that advances the state of the art in energy-efficient and trustworthy GPS-free localization, enabling reliable IoT LBS in both academic and industrial contexts.

6.2 Directions for Future Research

While this thesis provides a comprehensive framework for trustworthy GPS-free localization in IoT environments, several open challenges remain and point to promising directions for future work:

- *Enhanced hybrid algorithms*—Extend the proposed approaches by combining RSS with additional signal features such as AoA, or CSI, to improve accuracy and resilience in multipath-rich or highly dynamic scenarios.

- *Learning-based adaptation*—Investigate the integration of lightweight machine learning methods, including reinforcement and federated learning, to enable localization systems that dynamically adapt to changing environments while maintaining privacy and energy efficiency.

- *Refinement of the Reliability Index*—Expand the index to incorporate further aspects such as temporal stability, user mobility, or cross-technology correlations, and validate its applicability across other wireless standards (e.g., LoRa, UWB, 5G IoT).

- *Broader security coverage*—Extend the current defense mechanisms beyond byzantine and jamming attacks to include threats such as spoofing, replay, sybil, and coordinated attacks, developing proactive anomaly detection and collaborative trust-based approaches.

- *Experimental evaluation of real-world adversarial behavior*—Future work will extend the validation of the proposed algorithms by testing real-world adversarial scenarios (e.g., jamming and byzantine anchors) in controlled environments. This will complement the current simulation-based analysis and provide practical insights into system resilience.

- *Experimental Validation*—Some of the proposed solutions have been assessed exclusively through simulations. Future work will focus on extending their validation to real-world deployments, to confirm their effectiveness under practical operating conditions, and to complement the experimental results already obtained for the hybrid data-fusion approaches.

- *Scalability and large-scale validation*—Evaluate the proposed framework in larger deployments with heterogeneous anchors and realistic IoT traffic, addressing challenges of interoperability and scalability in dense environments.

Bibliography

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] L. S. Vailshery, "Number of internet of things (iot) connected devices worldwide from 2019 to 2030, by vertical." `https://www.statista.com/statistics/1194682/iot-connected-devices-vertically/`.

[3] N. V. R. Kumar, B. S. B. Praveen, A. V. S. Reddy, and B. B. Sam, "Study on iot with reference of m2m and wifi," in *2017 International Conference on Information Communication and Embedded Systems (ICICES)*, pp. 1–6, 2017.

[4] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, and P. Steggles, "Towards a better understanding of context and context-awareness," in *Handheld and Ubiquitous Computing* (H.-W. Gellersen, ed.), (Berlin, Heidelberg), pp. 304–307, Springer Berlin Heidelberg, 1999.

[5] H. A. Karimi, *Telegeoinformatics: Location-Based Computing and Services*. TCRC Press, 2004.

[6] F. Martinelli, "A robot localization system combining rssi and phase shift in uhf-rfid signals," *IEEE Transactions on Control Systems Technology*, vol. 23, no. 5, pp. 1782–1796, 2015.

[7] J. van't Riet, A. Hühn, P. Ketelaar, V.-J. Khan, R. Konig, E. Rozendaal, and P. Markopoulos, "Investigating the effects of location-based advertising in the supermarket: Does

goal congruence trump location congruence?," *Journal of Interactive Advertising*, vol. 16, no. 1, pp. 31–43, 2016.

[8] N. E. Tabbakha, W.-H. Tan, and C.-P. Ooi, "Indoor location and motion tracking system for elderly assisted living home," in *2017 International Conference on Robotics, Automation and Sciences (ICORAS)*, pp. 1–4, 2017.

[9] P. Uphaus, B. Beringer, K. Siemens, A. Ehlers, and H. Rau, "Location-based services – the market: success factors and emerging trends from an exploratory approach," *Journal of Location Based Services*, vol. 15, no. 1, pp. 1–26, 2021.

[10] X. Liang and Y. Kim, "A survey on security attacks and solutions in the iot network," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0853–0859, 2021.

[11] S. M. Asaad and H. S. Maghdid, "A comprehensive review of indoor/outdoor localization solutions in iot era: Research challenges and future perspectives," *Computer Networks*, vol. 212, p. 109041, 2022.

[12] J. Burbank, T. Greene, and N. Kaabouch, "Detecting and mitigating attacks on gps devices," *Sensors*, vol. 24, no. 17, 2024.

[13] T. G. Hailu, X. Guo, H. Si, L. Li, and Y. Zhang, "Theories and methods for indoor positioning systems: A comparative analysis, challenges, and prospective measures," *Sensors*, vol. 24, no. 21, 2024.

[14] G. Pettorru, V. Pilloni, and M. Martalò, "Trustworthy localization in iot networks: A survey of localization techniques, threats, and mitigation," *Sensors*, vol. 24, no. 7, 2024.

[15] C. Wu, Z. Yang, Y. Liu, and W. Xi, "Will: Wireless indoor localization without site survey," in *2012 Proceedings IEEE INFOCOM*, pp. 64–72, 2012.

[16] M. Ali, S. Hur, and Y. Park, "Wi-fi-based effortless indoor positioning system using iot sensors," *Sensors*, vol. 19, p. 1496, Mar 2019.

[17] J. Zheng, K. Li, and X. Zhang, "Wi-fi fingerprint-based indoor localization method via standard particle swarm optimization," *Sensors*, vol. 22, p. 5051, Jul 2022.

[18] Q. Ye, H. Bie, K.-C. Li, X. Fan, L. Gong, X. He, and G. Fang, "Edgeloc: A robust and real-time localization system toward heterogeneous iot devices," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3865–3876, 2022.

[19] B. El Boudani, L. Kanaris, A. Kokkinis, M. Kyriacou, C. Chrysoulas, S. Stavrou, and T. Dagiuklas, "Implementing deep learning techniques in 5g iot networks for 3d indoor positioning: Delta (deep learning-based co-operative architecture)," *Sensors*, vol. 20, p. 5495, Sep 2020.

[20] J. Purohit, X. Wang, S. Mao, X. Sun, and C. Yang, "Fingerprinting-based indoor and outdoor localization with lora and deep learning," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, pp. 1–6, 2020.

[21] B. Jia, W. Qiao, Z. Zong, S. Liu, M. Hijji, J. Del Ser, and K. Muhammad, "A fingerprint-based localization algorithm based on lstm and data expansion method for sparse samples," *Future Generation Computer Systems*, vol. 137, pp. 380–393, 2022.

[22] S. P. Singh and S. Sharma, "Range free localization techniques in wireless sensor networks: A review," *Procedia Computer Science*, vol. 57, pp. 7–16, 2015. 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015).

[23] H. Ghribi, F. Khelifa, A. Jemai, and M. Bassem Ben Salah, "A review of dv-hop localization algorithm," in *2021 31st International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 121–126, 2021.

[24] D. Prashar and K. Jyoti, "Distance error correction based hop localization algorithm for wireless sensor network," in *Wireless Personal Communications*, vol. 106, p. 1465–1488, 2019.

[25] R. Goyat, M. K. Rai, G. Kumar, R. Saha, and T.-H. Kim, "Energy efficient range-free localization algorithm for wireless sensor networks," *Sensors*, vol. 19, p. 3603, Aug 2019.

[26] A. Hadir, Y. Regragui, and N. M. Garcia, "Accurate range-free localization algorithms based on pso for wireless sensor networks," *IEEE Access*, vol. 9, pp. 149906–149924, 2021.

[27] A. Hadir, N. Kaabouch, M.-A. El Houssaini, and J. El Kafi, "Range-free localization approaches based on intelligent swarm optimization for internet of things," *Information*, vol. 14, p. 592, Nov 2023.

[28] L. Gui, F. Xiao, Y. Zhou, F. Shu, and T. Val, "Connectivity based dv-hop localization for internet of things," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8949–8958, 2020.

[29] Z. Turgut, G. Z. G. Aydin, and A. Sertbas, "Indoor localization techniques for smart building environment," *Procedia Computer Science*, vol. 83, pp. 1176–1181, 2016. The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016) / The 6th International Conference on Sustainable Energy Information Technology (SEIT-2016) / Affiliated Workshops.

[30] A. Mackey and P. Spachos, "Energy consumption and proximity accuracy of ble beacons for internet of things applications," in *2018 Global Information Infrastructure and Networking Symposium (GIIS)*, pp. 1–5, 2018.

[31] P. Spachos and K. N. Plataniotis, "Ble beacons for indoor positioning at an interactive iot-based smart museum," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3483–3493, 2020.

[32] M. Aernouts, B. Bellekens, R. Berkvens, and M. Weyn, "A comparison of signal strength localization methods with sigfox," in *2018 15th Workshop on Positioning, Navigation and Communications (WPNC)*, pp. 1–6, 2018.

[33] T. Janssen, R. Berkvens, and M. Weyn, "Rss-based localization and mobility evaluation using a single nb-iot cell," *Sensors*, vol. 20, p. 6172, Oct 2020.

[34] M. B. Jamâa, A. Koubâa, and Y. Kayani, "Easyloc: Rss-based localization made easy," *Procedia Computer Science*, vol. 10, pp. 1127–1133, 2012. ANT 2012 and MobiWIS 2012.

[35] A. Achroufene, Y. Amirat, and A. Chibani, "Rss-based indoor localization using belief function theory," *IEEE Transactions on Automation Science and Engineering*, vol. 16, no. 3, pp. 1163–1180, 2019.

[36] J. Du, C. Yuan, M. Yue, and T. Ma, "A novel localization algorithm based on rssi and multilateration for indoor environments," *Electronics*, vol. 11, p. 289, Jan 2022.

[37] F. Carpi, M. Martalò, L. Davoli, A. Cilfone, Y. Yu, Y. Wang, and G. Ferrari, "Experimental analysis of rssi-based localization algorithms with nlos pre-mitigation for iot applications," *Computer Networks*, vol. 225, p. 109663, 2023.

[38] H. Kwasme and S. Ekin, "Rssi-based localization using lorawan technology," *IEEE Access*, vol. 7, pp. 99856–99866, 2019.

[39] K.-H. Lam, C.-C. Cheung, and W.-C. Lee, "Rssi-based lora localization systems for large-scale indoor and outdoor environments," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 12, pp. 11778–11791, 2019.

[40] G. Qiao, A. Muhammad, M. Muzzammil, M. Shoaib Khan, M. O. Tariq, and M. S. Khan, "Addressing the directionality challenge through rssi-based multilateration technique, to localize nodes in underwater wsns by using magneto-inductive communication," *Journal of Marine Science and Engineering*, vol. 10, p. 530, Apr 2022.

[41] F. Zafari, A. Gkelias, and K. K. Leung, "A survey of indoor localization systems and technologies," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2568–2599, 2019.

[42] T. Wang, H. Ding, H. Xiong, and L. Zheng, "A compensated multi-anchors tof-based localization algorithm for asynchronous wireless sensor networks," *IEEE Access*, vol. 7, pp. 64162–64176, 2019.

[43] A. Comuniello, A. De Angelis, A. Moschitta, and P. Carbone, "Using bluetooth low energy technology to perform tof-based positioning," *Electronics*, vol. 11, p. 111, Dec 2021.

[44] P. N. Beuchat, H. Hesse, A. Domahidi, and J. Lygeros, "Enabling optimization-based localization for iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5639–5650, 2019.

[45] T. Han, X. Lu, and Q. Lan, "Pattern recognition based kalman filter for indoor localization using tdoa algorithm," *Applied Mathematical Modelling*, vol. 34, no. 10, pp. 2893–2900, 2010.

[46] G. Wang, W. Zhu, and N. Ansari, "Robust tdoa-based localization for iot via joint source position and nlos error estimation," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8529–8541, 2019.

[47] W. Zhao, X. Duan, D. Tian, J. Zhou, S. Xia, Y. Sun, Y. Wu, and X. Ran, "An sdp-based tdoa localization method for wireless sensor networks," in *2021 International Conference on Control, Automation and Information Sciences (ICCAIS)*, pp. 381–386, 2021.

[48] D. Neunteufel, S. Grebien, and H. Arthaber, "Indoor positioning of low-cost narrowband iot nodes: Evaluation of a tdoa approach in a retail environment," *Sensors*, vol. 22, p. 2663, Mar 2022.

[49] M. Martalò, S. Perri, G. Verdano, F. De Mola, F. Monica, and G. Ferrari, "Improved uwb tdoa-based positioning using a single hotspot for industrial iot applications," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 3915–3925, 2022.

[50] M. Martalò, S. Perri, G. Verdano, F. De Mola, F. Monica, and G. Ferrari, "Hybrid uwb-inertial tdoa-based target tracking with concentrated anchors," *IEEE Internet of Things Journal*, vol. 10, no. 14, pp. 12676–12689, 2023.

[51] C. Bouras, A. Gkamas, V. Kokkinos, and N. Papachristos, "Time difference of arrival localization study for sar systems over lorawan," *Procedia Computer Science*, vol. 175, pp. 292–299, 2020. The 17th International Conference on Mobile Systems and Pervasive Computing (MobiSPC),The 15th International Conference on Future Networks and Communications (FNC),The 10th International Conference on Sustainable Energy Information Technology.

[52] J. Pospisil, R. Fujdiak, and K. Mikhaylov, "Investigation of the performance of tdoa-based localization over lorawan in theory and practice," *Sensors*, vol. 20, p. 5464, Sep 2020.

[53] S. Wielandt and L. Strycker, "Indoor multipath assisted angle of arrival localization," *Sensors*, vol. 17, p. 2522, Nov 2017.

[54] S. Monfared, A. Delepaut, M. Van Eeckhaute, P. De Doncker, and F. Horlin, "Iterative localization method using aoa for iot sensor networks," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, pp. 1–6, 2019.

[55] Z. HajiAkhondi-Meybodi, M. Salimibeni, A. Mohammadi, and K. N. Plataniotis, "Bluetooth low energy and cnn-based angle of arrival localization in presence of rayleigh fading," in *ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 7913–7917, 2021.

[56] T.-C. Tai, K. C.-J. Lin, and Y.-C. Tseng, "Toward reliable localization by unequal aoa tracking," in *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*, MobiSys '19, (New York, NY, USA), p. 444–456, Association for Computing Machinery, 2019.

[57] M. Heydariaan, H. Dabirian, and O. Gnawali, "Anguloc: Concurrent angle of arrival estimation for indoor localization with uwb radios," in *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 112–119, 2020.

[58] Z. Hajiakhondi-Meybodi, M. Salimibeni, K. N. Plataniotis, and A. Mohammadi, "Bluetooth low energy-based angle of arrival estimation via switch antenna array for indoor localization," in *2020 IEEE 23rd International Conference on Information Fusion (FUSION)*, pp. 1–6, 2020.

[59] A. Zandamela, A. Chiumento, N. Marchetti, and A. Narbudowicz, "Angle of arrival estimation via small iot devices: Miniaturized arrays vs. mimo antennas," *IEEE Internet of Things Magazine*, vol. 5, no. 2, pp. 146–152, 2022.

[60] G. Guo, R. Chen, F. Ye, X. Peng, Z. Liu, and Y. Pan, "Indoor smartphone localization: A hybrid wifi rtt-rss ranging approach," *IEEE Access*, vol. 7, pp. 176767–176781, 2019.

[61] T. L. N. Nguyen, T. D. Vy, and Y. Shin, "An efficient hybrid rss-aoa localization for 3d wireless sensor networks," *Sensors*, vol. 19, p. 2121, May 2019.

[62] X. Li, E. Leitinger, and F. Tufvesson, "Rss-based localization of low-power iot devices exploiting aoa and range information," in *2020 54th Asilomar Conference on Signals, Systems, and Computers*, pp. 651–656, 2020.

[63] T. Wang, H. Xiong, H. Ding, and L. Zheng, "A hybrid localization algorithm based on tof and tdoa for asynchronous wireless sensor networks," *IEEE Access*, vol. 7, pp. 158981–158988, 2019.

[64] H. Chen, T. Ballal, N. Saeed, M.-S. Alouini, and T. Y. Al-Naffouri, "A joint tdoa-pdoa localization approach using particle swarm optimization," *IEEE Wireless Communications Letters*, vol. 9, no. 8, pp. 1240–1244, 2020.

[65] R. C. Luo and T.-J. Hsiao, "Indoor localization system based on hybrid wi-fi/ble and hierarchical topological fingerprinting approach," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 10791–10806, 2019.

[66] S. Monica and F. Bergenti, "Hybrid indoor localization using wifi and uwb technologies," *Electronics*, vol. 8, p. 334, Mar 2019.

[67] G. Kia, L. Ruotsalainen, and J. Talvitie, "Toward accurate indoor positioning: An rss-based fusion of uwb and machine-learning-enhanced wifi," *Sensors*, vol. 22, p. 3204, Apr 2022.

[68] X. Guo, N. Ansari, L. Li, and L. Duan, "A hybrid positioning system for location-based services: Design and implementation," *IEEE Communications Magazine*, vol. 58, no. 5, pp. 90–96, 2020.

[69] A. Mittal and A. Shrivastava, "Detecting continuous jamming attack using ultra-low power rssi circuit," in *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 49–52, 2022.

[70] F. t. Zahra, Y. S. Bostanci, and M. Soyturk, "The consequences of jamming attacks on wireless iot networks: Evaluating the performance metrics in noiseless and noisy environments," in *2023 31st Signal Processing and Communications Applications Conference (SIU)*, pp. 1–4, 2023.

[71] N. López-Vilos, C. Valencia-Cordero, R. D. Souza, and S. Montejo-Sánchez, "Clustering-based energy-efficient self-healing strategy for wsns under jamming attacks," *Sensors*, vol. 23, p. 6894, Aug 2023.

[72] G. Pettorru, G. Nurcis, V. Pilloni, and M. Martalò, "How do jamming attacks impact the performance of rss-based localization techniques?," in *ICC 2025 - IEEE International Conference on Communications*, pp. 2707–2712, 2025.

[73] M. Ghahramani, R. Javidan, M. Shojafar, R. Taheri, M. Alazab, and R. Tafazolli, "Rss: An energy-efficient approach for securing iot service protocols against the dos attack," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3619–3635, 2021.

[74] M. S. Abdalzaher, M. Elwekeil, T. Wang, and S. Zhang, "A deep autoencoder trust model for mitigating jamming attack in iot assisted by cognitive radio," *IEEE Systems Journal*, vol. 16, no. 3, pp. 3635–3645, 2022.

[75] D. Darsena, G. Gelli, I. Iudice, and F. Verde, "Detection and blind channel estimation for uav-aided wireless sensor networks in smart cities under mobile jamming attack," *IEEE Internet of Things Journal*, vol. 9, no. 14, pp. 11932–11950, 2022.

[76] N. Alikh and A. Rajabzadeh, "Using a lightweight security mechanism to detect and localize jamming attack in wireless sensor networks," *Optik*, vol. 271, p. 170099, 2022.

[77] I. Sudha, M. A. Mustafa, R. Suguna, S. Karupusamy, V. Ammisetty, S. N. Shavkatovich, M. Ramalingam, and P. Kanani, "Pulse jamming attack detection using swarm intelligence in wireless sensor networks," *Optik*, vol. 272, p. 170251, 2023.

[78] L. Shi, Q. Liu, J. Shao, and Y. Cheng, "Distributed localization in wireless sensor networks under denial-of-service attacks," *IEEE Control Systems Letters*, vol. 5, no. 2, pp. 493–498, 2021.

[79] J. R. Douceur, "The sybil attack," in *International workshop on peer-to-peer systems*, pp. 251–260, Springer, 2002.

[80] B. Pestourie, V. Beroulle, and N. Fourty, "Security evaluation with an indoor uwb localization open platform: Acknowledgment attack case study," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–7, 2019.

[81] X. Sun, H. Ai, J. Tao, T. Hu, and Y. Cheng, "Bert-adloc: A secure crowdsourced indoor localization system based on ble fingerprints," *Applied Soft Computing*, vol. 104, p. 107237, 2021.

[82] A. O. Bang and U. P. Rao, "A novel decentralized security architecture against sybil attack in rpl-based iot networks: a focus on smart home use case.," *The Journal of Supercomputing*, vol. 77, p. 13703–13738, 2021.

[83] X.-g. Z. Shi Dong and W. gang Zhou, "A security localization algorithm based on dv-hop against sybil attack in wireless sensor networks.," *Journal of Electrical Engineering & Technology*, vol. 15, p. 919–926, 2020.

[84] Y. Yuan, Y. Huang, and Y. Yuan, "Prsloc: Sybil attack detection for localization with private observers using differential privacy," *Computers & Security*, vol. 131, p. 103289, 2023.

[85] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 2, pp. 774–786, 2011.

[86] B. Mukhopadhyay, S. Srirangarajan, and S. Kar, "Rss-based localization in the presence of malicious nodes in sensor networks," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1–16, 2021.

[87] Y. Liu, J. Peng, X. Liu, Y. Xie, and Z. Tang, "An attack-resistant weighted least squares localization algorithm based on rssi," in *Science and Technologies for Smart Cities* (S. Paiva, S. I. Lopes, R. Zitouni, N. Gupta, S. F. Lopes, and T. Yonezawa, eds.), (Cham), pp. 476–494, Springer International Publishing, 2021.

[88] Y. Li, S. Ma, G. Yang, and K.-K. Wong, "Secure localization and velocity estimation in mobile iot networks with malicious attacks," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6878–6892, 2021.

[89] C. Wang, J. Luo, X. Liu, and X. He, "Secure and reliable indoor localization based on multitask collaborative learning for large-scale buildings," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22291–22303, 2022.

[90] Z. Teng, C. Du, M. Li, H. Zhang, and W. Zhu, "A wormhole attack detection algorithm integrated with the node trust optimization model in wsns," *IEEE Sensors Journal*, vol. 22, no. 7, pp. 7361–7370, 2022.

[91] D. Han, M. Liu, T.-H. Weng, C. Tang, M. D. Marino, and K.-C. Li, "A novel secure dv-hop localization algorithm against wormhole attacks," *Telecommunication Systems*, vol. 80, pp. 413–430, 2022.

[92] T. G. Ruchi Garg and S. Kumar, "Wormhole attack detection and recovery for secure range-free localization in large-scale wireless sensor networks.," *Peer-to-Peer Networking and Applications*, vol. 16, p. 2833–2849, 2023.

[93] T. G. Ruchi Garg and S. Kumar, "Range-free localization in wsn against wormhole attack using farkas' lemma.," *Wireless Networks*, vol. 29, p. 2029–2043, 2023.

[94] O. Cheikhrouhou and A. Koubâa, "Blockloc: Secure localization in the internet of things using blockchain," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 629–634, 2019.

[95] Z. Guan, Z. Liu, X. Wen, Q. Wan, and W. Xu, "Trusted fingerprint localization for multimedia devices based on blockchain," *Information Sciences*, vol. 643, p. 119231, 2023.

[96] Q. Ye, X. Fan, H. Bie, D. Puthal, T. Wu, X. Song, and G. Fang, "Se-loc: Security-enhanced indoor localization with semi-supervised deep learning," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 5, pp. 2964–2977, 2023.

[97] G. G. Gebremariam, J. Panda, and S. Indu, "Secure localization techniques in wireless sensor networks against routing attacks based on hybrid machine learning models," *Alexandria Engineering Journal*, vol. 82, pp. 82–100, 2023.

[98] P. Kaliyar, W. B. Jaballah, M. Conti, and C. Lal, "Lidl: Localization with early detection of sybil and wormhole attacks in iot networks," *Computers & Security*, vol. 94, p. 101849, 2020.

[99] A. Goldsmith, *Wireless Communications*. USA: Cambridge University Press, 2005.

[100] T. Rappaport, *Wireless Communications: Principles and Practice*. USA: Prentice Hall PTR, 2nd ed., 2001.

[101] G. Wang, H. Chen, Y. Li, and M. Jin, "On received-signal-strength based localization with unknown transmit power and path loss exponent," *IEEE Wireless Communications Letters*, vol. 1, no. 5, pp. 536–539, 2012.

[102] F. Subhan, A. Khan, S. Saleem, S. Ahmed, M. Imran, Z. Asghar, and J. I. Bangash, "Experimental analysis of received signals strength in bluetooth low energy (ble) and its effect on distance and position estimation," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 2, p. e3793, 2022.

[103] K. Cengiz, "Comprehensive analysis on least squares lateration for indoor positioning systems," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2842–2856, 2021. DOI: 10.1109/JIOT.2020.3020888.

[104] G. Pettorru, V. Pilloni, and M. Martalò, "A hybrid wifi/bluetooth rss dataset with application to multilateration-based localization," in *2023 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, pp. 293–298, 2023.

[105] G. Pettorru, V. Pilloni, and M. Martalò, "Robust range-based localization approaches leveraging multiple wireless interfaces." Manuscript under review, 2025.

[106] J. Yuan, Y.-C. Liang, J. Joung, G. Feng, and E. G. Larsson, "Intelligent reflecting surface-assisted cognitive radio system," *IEEE Transactions on Communications*, vol. 69, no. 1, pp. 675–687, 2020.

[107] Q. D. Vo and P. De, "A survey of fingerprint-based outdoor localization," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 491–506, 2016.

[108] G. Pettorru, V. Pilloni, and M. Martaló, "Multilateration-assisted fingerprinting-based localization for dynamic iot environments," in *2025 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, pp. 1–6, 2025.

[109] S. M. Asaad and H. S. Maghdid, "A comprehensive review of indoor/outdoor localization solutions in iot era: Research challenges and future perspectives," *Computer Networks*, vol. 212, p. 109041, 2022.

[110] G. Pettorru, A. Coni, V. Pilloni, and M. Martalò, "A reliability index for position estimation in trustworthy location-based services," in *2025 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, pp. 1–6, 2025.

[111] P. Tarrío, A. M. Bernardos, and J. R. Casar, "Weighted least squares techniques for improved received signal strength based localization," *Sensors*, vol. 11, no. 9, pp. 8569–8592, 2011.

[112] M. Bonamente and M. Bonamente, "Functions of random variables and error propagation," *Statistics and Analysis of Scientific Data*, pp. 55–83, 2017.

[113] D. Green, "pyshark." `https://github.com/KimiNewt/pyshark`. [Online; accessed 1-Oct-2025].

[114] I. Harvey, "bluepy." `https://github.com/IanHarvey/bluepy`. [Online; accessed 1-Oct-2025].

[115] L. D'Alfonso, M. Tropea, G. Fedele, and F. D. Rango, "Indoor positioning error analysis using a cooperative multi-technology simultaneous localization and signal mapping in a vehicular environment," in *2024 14th International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, pp. 1–6, 2024.

[116] G. Pettorru, "Hybrid dataset for RSS-based localization." [Online; accessed 1-Oct-2025].

[117] J. Moon, C. Laoudias, R. Guan, S. Kim, D. Zeinalipour-Yazti, and C. G. Panayiotou, "Cramér–rao lower bound analysis of differential signal strength fingerprinting for crowd-sourced iot localization," *IEEE Internet of Things Journal*, vol. 10, no. 11, pp. 9690–9702, 2023.

[118] T. Holotyak, S. Voloshynovskiy, J. Rolim, and I. Prudyus, "Improved solution of cramer-rao lower bound for toa/rss localization," in *Proceedings of International Conference on Modern Problem of Radio Engineering, Telecommunications and Computer Science*, pp. 292–294, 2012.

List of Acronyms

Table 6.1: List of used acronyms (in alphabetical order).

Acronym	**Definition**
AGROS	Agricultural Geolocation and Resource Optimization System
ANN	Artificial Neural Network
AoA	Angle of Arrival
AP	Access Point
BLE	Bluetooth Low Energy
CDF	Cumulative Distribution Function
CNN	Convolutional Neural Network
CRLB	Cramér–Rao Lower Bound
CSI	Channel State Information
CSO	Chicken Swarm Optimization
DL	Deep Learning
DoS	Denial-of-Service
DV-Hop	Distance Vector–Hop

Continued on next page

Table 6.1 (continued)

Acronym	Definition
FEC	Fog, Edge, and Cloud
GPS	Global Positioning System
IoT	Internet of Things
kNN	k-Nearest Neighbors
LBS	Location-Based Services
LoRa	Long-Range
LOS	Line of Sight
LPWAN	Low-Power Wide-Area Network
LS	Least Squares
LSTM	Long Short-Term Memory
LTE	Long-Term Evolution
M2H	Machine-to-Human
M2M	Machine-to-Machine
MAPS	Multi-Interface Adaptive Positioning System
MIMO	Multiple-Input Multiple-Output
ML	Machine Learning
MLE	Maximum Likelihood Estimation
NB-IoT	Narrowband IoT
NLOS	Non Line of Sight
NLS	Non-Linear Least Squares
PDoA	Phase Difference of Arrival

Continued on next page

Table 6.1 (continued)

Acronym	Definition
PoC	Proof of Concept
POSIDONIA	POSition Information with Digital twin Offloading in trustworthy Next-generation Internet Applications
PSO	Particle Swarm Optimization
RAPS	Redundant Anchors Positioning System
RF	Random Forest
RMSE	Root Mean Square Error
RPs	Reference Points
RSS	Received Signal Strength
RTT	Round-Trip Time
SDP	Semi-Definite Programming
SDR	Software-Defined Radio
SNR	Signal-to-Noise Ratio
SWLS	Secure Weighted Least Squares
TDoA	Time Difference of Arrival
ToA	Time of Arrival
ToF	Time of Flight
UAV	Unmanned Aerial Vehicles
UGV	Unmanned Ground Vehicles
UWB	Ultra-Wideband

Continued on next page

Table 6.1 (continued)

Acronym	Definition
WLS	Weighted Least Squares
WSN	Wireless Sensor Network


Acknowledgments

This thesis was produced while attending the PhD programme in Electronic and Computer Engineering at the University of Cagliari, Cycle XXXVIII, with the support of a scholarship financed by the Ministerial Decree no. 351 of 9th April 2022, based on the NRRP - funded by the European Union - NextGenerationEU - Mission 4 ”Education and Research”, Component 1 ”Enhancement of the offer of educational services: from nurseries to universities” - Investment 4.1 “Extension of the number of research doctorates and innovative doctorates for public administration and cultural heritage”