RIS-Aided Positioning Under Adverse Conditions: Interference from an Unauthorized RIS

Citation for the original published paper (version of record):
Li, M., Chen, H., Pourafzal, A. et al (2026). RIS-Aided Positioning Under Adverse Conditions: Interference from an Unauthorized RIS. IEEE Transactions on Wireless Communications, 25: 21227-21243. http://dx.doi.org/10.1109/TWC.2026.3716222

(article starts on next page)

RIS-Aided Positioning Under Adverse Conditions: Interference From an Unauthorized RIS

Mengting Li, *Member, IEEE*, Hui Chen, *Member, IEEE*, Alireza Pourafzal, *Member, IEEE*, and Henk Wymeersch, *Fellow, IEEE*

***Abstract*—Positioning technology, which aims to determine the geometric state of a device in a global coordinate system, is a key component in integrated sensing and communication systems. In addition to traditional active anchor-based positioning systems, reconfigurable intelligent surfaces (RISs) have shown great potential for enhancing system performance. However, their ability to manipulate electromagnetic waves and ease of deployment pose potential risks, as unauthorized RIS may be intentionally introduced to jeopardize the positioning service. Such an unauthorized RIS can introduce unexpected interference into the legitimate positioning system, distorting the transmitted signals, and leading to degraded positioning accuracy. In this work, we investigate the scenario of RIS-aided positioning in the presence of interference from an unauthorized RIS. Theoretical lower bounds are derived to analyze the impact of unauthorized RIS on channel parameter estimation and positioning accuracy. Several codebook design strategies for unauthorized RIS are evaluated, and various system arrangements are discussed. Simulation results show that unauthorized RIS paths with high power or delay values close to those of legitimate RIS paths significantly degrade positioning accuracy. Furthermore, an unauthorized RIS generates more effective interference when using directional beamforming codebooks compared with a random phase codebook.**

***Index Terms*—Positioning, reconfigurable intelligent surface (RIS), interference, integrated sensing and communication (ISAC).**

I. Introduction

INTEGRATED sensing and communication (ISAC) is envisioned as a core function in modern communication systems, enabling the dual capability of wireless networks to transmit data while simultaneously sensing the environment [1]. Positioning, which refers to estimating the location (and possibly orientation and velocity) of a device from radio measurements, plays a pivotal role in ISAC, assisting communication systems in radio resource management, beamforming, mobility management, etc [2]. By utilizing uplink or downlink pilot signals, geometrical relationships, such as angle and time between a connected user equipment (UE) and base station (BS) anchors can be inferred for a further position estimate [3]. In practical scenarios with multipath, positioning often works together with mapping, unlocking new applications such as digital twins, autonomous systems, and collaborative robots, which rely on accurate information on positioning and the surrounding environment [4].

The reconfigurable intelligent surface (RIS) has emerged as a transformative technology in wireless communication systems, with the ability to reshape channels using its configurable elements [5]. RIS can enhance positioning accuracy by working as additional passive anchors and providing high-resolution angular information, leveraging its large number of RIS elements [6]. Additionally, RIS can be seamlessly integrated into a wide range of positioning systems, from single-input-single-output (SISO) to multiple-input-multiple-output (MIMO) configurations, expanding capabilities from position estimation to orientation estimation [7]. The deployment of multiple RISs can further improve coverage while reducing network costs, at the expense of overhead [8]. In out-of-coverage scenarios, sidelink communication between UEs can leverage RIS anchors to maintain positioning services [6]. Furthermore, advanced RIS implementations, such as near-field processing [9], integration into non-terrestrial networks [10], and innovative RIS types (e.g., active RIS [11] and beyond diagonal RIS [12]), further amplify the potential of ISAC systems to operate in complex environments.

Despite the importance of location information, the misuse of inaccurate location information can have catastrophic consequences, especially for safety-critical applications, such as autonomous vehicles and industrial automation [13]. Two primary sources lead to inaccuracies in the estimated target locations. At the infrastructure level, positioning performance is directly influenced by the available communication system resources, such as the bandwidth and transmit power allocated for pilot signals. However, these resource constraints should be considered during the system design phase, and are usually

Received 3 July 2025; revised 5 December 2025 and 15 May 2026; accepted 17 July 2026. Date of publication 30 July 2026; date of current version 5 August 2026. This work was supported in part by Villum Fonden under Grant VIL59841; in part by Swedish Research Council (VR) under Grant 2023-03821; in part by the Smart Networks and Services (SNS) Joint Undertaking (JU) Project 6G-Distributed Intelligent Sensing and Communication (DISAC) through European Union's Horizon Europe Research and Innovation Program under Grant 101139130; and in part by European Union's Horizon Europe Research and Innovation Program through the Marie Skłodowska-Curie Actions under Grant 101201808 (SMALL-6G). The associate editor coordinating the review of this article and approving it for publication was A. Guerra. *(Corresponding author: Hui Chen.)*

Mengting Li is with the Department of Electrical Engineering, Chalmers University of Technology, 412 58 Gothenburg, Sweden, and also with the Department of Electronic Systems, Aalborg University, 9220 Aalborg, Denmark (e-mail: limeng@chalmers.se).

Hui Chen is with the Department of Electrical Engineering, Chalmers University of Technology, 412 58 Gothenburg, Sweden, and also with the Department of Electronic and Electrical Engineering, University College London, WC1E 7JE London, U.K. (e-mail: hui.chen@chalmers.se).

Alireza Pourafzal and Henk Wymeersch are with the Department of Electrical Engineering, Chalmers University of Technology, 412 58 Gothenburg, Sweden (e-mail: alireza.pourafzal@chalmers.se; henkw@chalmers.se).

Digital Object Identifier 10.1109/TWC.2026.3716222

flexible to control during positioning operations [14]. Another source of errors arises from imperfect prior knowledge of the anchors, which consists of two major factors: geometry errors and hardware impairments [15]. A certain level of geometric errors (e.g., a few degrees of orientation or meters of position) may have a limited impact on communications, where end-to-end channel matters rather than the position information embedded in the channel. In contrast, these errors directly impact the accuracy of UE position estimation [16]. Regarding hardware impairments that exist in communication systems, certain types of factors, such as mutual coupling and antenna displacement error, have shown a greater impact on positioning and require careful calibration [17].

In RIS-aided systems, initial work has investigated the geometry error of RIS anchors in positioning by implementing misspecified Cramér-Rao bound (MCRB) for mismatch analysis [18]. Joint UE localization and RIS calibration algorithms have been proposed to tackle this challenge [19]. Regarding the hardware imperfections of the RIS, a pilot-based phase calibration task is addressed by alternating optimization [20]. In [21], joint localization and failure diagnosis strategies are developed to detect failing pixels while simultaneously locating the UE with high accuracy. However, existing works only consider a limited number of impairment types, requiring practical and scalable calibration algorithms that can deal with a wide range of scenarios.

Beyond system-introduced errors, adversarial threats such as jamming and spoofing pose significant risks to positioning systems, degrading both model-based and learning-based methods through randomized interference or carefully crafted pilot manipulations [22], [23], [24], [25]. While secure sensors and information-theoretic consistency checks can detect geometric or statistical anomalies [26], [27], these solutions often rely on additional trusted devices and thus lack scalability. Recent advances instead explore physical-layer security and privacy for 5G and beyond positioning, including vulnerabilities in RIS-aided positioning, selective positioning reference signal (PRS)-spoofing attacks and defenses in 5G NR [28], and beamforming-based positioning-privacy control in MIMO-orthogonal frequency division multiplexing (OFDM) systems [29]. Coordinated adversarial strategies such as cooperative impersonation in angle-based physical-layer authentication further highlight system sensitivity to array processing [30], while physical-layer threat models show how timing distortions degrade PRS-based positioning accuracy [31]. On the UE side, pilot-signal obfuscation for millimeter-wave (mmWave) MIMO-OFDM location privacy [32], channel state information (CSI)-free fake-path injection [33], and delay-angle information spoofing [34] demonstrate how structured signal manipulation can hide UE positions or mislead untrusted receivers without degrading legitimate positioning. These works highlight that positioning accuracy, privacy, and security are tightly coupled at the physical layer. However, they do not consider RIS-assisted positioning systems.

There are several studies exploring the use of RIS as an adversarial entity in communication systems [35]. In [36], several metasurface manipulation attacks have been identified and classified, showing that the bit error rate (BER) of the legitimate UE pairs is severely degraded. The impact of RIS on the integrated sensing and communication (ISAC) multi-user MIMO system has been studied with an emphasis on signal-to-noise ratio (SNR) [37]. Although SNR directly affects the probability of detection and the position estimate, it does not directly quantify the impact on positioning performance. Specifically, unauthorized RIS deployments can distort pilot signals from legitimate RIS anchors, directly affecting channel parameter extraction tasks and hence the accuracy and reliability of position estimates. Nevertheless, this paper develops an explicit signal and threat model for RIS-aided positioning under unauthorized RIS interference, derives misspecified performance bounds, and evaluates a range of attack and system parameters in a unified framework.

In this work, the objective is to investigate and analyze the impacts of interference from an unauthorized RIS on the performance of an existing RIS-aided positioning system. The contributions of this work can be summarized as follows:

- **Threat-aware problem formulation.** We model a wideband SISO localization system where a legitimate RIS acts as a passive anchor and an unauthorized, passive RIS operates as an external interferer. For this setting, we derive explicit time-frequency signal models for both the interference-free system and the system affected by unauthorized RIS interference under various RIS beamforming profiles.
- **Fundamental limits under model mismatch.** We cast positioning with an unauthorized RIS as a misspecified estimation problem and derive closed-form performance bounds for both channel parameters and the 3D position/clock offset state.[1] Specifically, we obtain the Cramér-Rao bound (CRB) for the assumed interference-free model, the MCRB and mismatched lower bound (MLB) under the true model with unknown interference, and an absolute lower bound (ALB) for state estimation via Jacobian transformation. These bounds separate variance and bias effects and quantify how unauthorized-RIS power, geometry, and path proximity degrade positioning accuracy and induce SNR saturation.
- **Algorithmic validation and design insights.** We implement a fast Fourier transform (FFT)-based grid-search-plus-refinement estimator (mismatched maximum likelihood estimation (MLE)) matched to the interference-free model and use it to validate the derived bounds and to explore harmful and robust operating regimes. Extensive simulations are conducted to compare various unauthorized RIS beamforming strategies, and phase control capabilities, study the interplay between multipath and interference, and analyze different deployment strategies for the legitimate and unauthorized RISs. The results identify which codebooks and geometries are most damaging and yield concrete guidelines for designing resilient RIS-aided positioning systems.

[1]The 3D position refers to the spatial coordinates of the UE, while the clock offset represents the time bias resulting from the lack of synchronization between the BS and the UE.

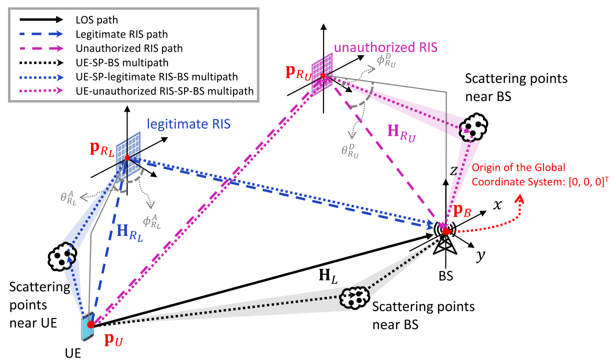


Fig. 1. An illustration of a RIS-aided positioning system in the presence of an unauthorized RIS and multipath.

Notations: Vectors are represented by bold lowercase letters, matrices by bold uppercase letters, and scalars by italicized letters. Unless stated otherwise, all vectors are column vectors. The transpose, inverse, Hermitian, trace, and complex conjugate operations are denoted as $(\cdot)^{\top}$, $(\cdot)^{-1}$, $(\cdot)^{\mathsf{H}}$, $\text{tr}(\cdot)$, and $(\cdot)^{*}$, respectively. The Hadamard product is denoted by $\odot$. The notation $[\cdot]_i$ refers to the i-th element of a vector, while $[\cdot]_{i,j}$ represents the element at the i-th row and j-th column of a matrix. Additionally, the subscript $i:j$ denotes all elements between indices i and j.

II. RIS-Aided Positioning System

We consider a RIS-aided positioning system employing a SISO configuration in a 3D scenario. The SISO configuration is adopted, as it represents a particularly challenging positioning case, where the deployment of a legitimate RIS provides significant performance gain [38], [39], [40], while simultaneously exposing the system's inherent vulnerabilities to unauthorized devices. Then the beamforming design employed by the legitimate RIS is described. Such a system is exposed to an unauthorized RIS (to be discussed in Section III) to interfere with the positioning service, as shown in Fig. 1.

A. Positioning System Model

The single-antenna BS and UE are located at $\mathbf{p}_B, \mathbf{p}_U \in \mathbb{R}^3$, respectively. The legitimate RIS contains N_1 passive reflective elements and its position and orientation are denoted by $\mathbf{p}_{R_L} \in \mathbb{R}^3$ and $\mathbf{o}_{R_L} \in \mathbb{R}^3$, respectively. Note that the Euler angle vector $\mathbf{o}_{R_L}$ is used to determine the rotation matrix $\mathbf{Q}_{R_L}$. The beamforming performance of the RIS will be determined by the phase modulations applied to the RIS elements, i.e., RIS beamforming codebooks.

As shown in Fig. 1, in the absence of the unauthorized RIS, the positioning task is accomplished using signals from the line-of-sight (LOS) path and the legitimate RIS path with multipath effects. The multipath components (MPCs) are generated by reflections from scattering points (SPs) on the scatterers. In this work, we consider single-bounce MPCs (i.e., UE-SP-BS paths) and double-bounce RIS-associated MPCs (i.e., UE-SP-RIS-BS and UE-RIS-SP-BS paths). Higher-order reflections are neglected due to their severe path loss at high-frequency bands [41]. We assume a wideband uplink[2] system employing K subcarriers and transmitting G OFDM symbols for each positioning task.

[2]Equivalent to downlink positioning for SISO systems.

The interference-free received signal matrix $\tilde{\mathbf{Y}} \in \mathbb{C}^{K\times G}$ is expressed as

$$\tilde{\mathbf{Y}} = \mathbf{Y}_L + \mathbf{Y}_{R_L} + \mathbf{N}, \tag{1}$$

where

$$\mathbf{Y}_L = \mathbf{H}_L \odot \mathbf{X}, \quad \mathbf{Y}_{R_L} = \mathbf{H}_{R_L} \odot \mathbf{X}. \tag{2}$$

The noise matrix $\mathbf{N} \in \mathbb{C}^{K\times G}$ denotes additive white Gaussian noise with zero mean and variance σ^2. The transmitted pilot signal matrix $\mathbf{X} \in \mathbb{C}^{K\times G}$ is

$$\mathbf{X} = \sqrt{P}\,\mathbf{x}\,\mathbf{1}_G^{\mathrm{T}}, \tag{3}$$

where $\mathbf{x} \in \mathbb{C}^{K\times 1}$ is the transmitted pilot vector. The same pilot is used across all transmissions, with transmit power P. The channel matrices corresponding to the LOS and single-bounce MPCs, as well as the legitimate RIS path and its associated MPCs, are given by

$$\mathbf{H}_L = \sum_{m=0}^{M_0} \alpha_{L,m}\, \mathbf{d}(\tau_{L,m})\, \mathbf{1}_G^{\mathrm{T}}, \tag{4}$$

$$\mathbf{H}_{R_L} = \left(\sum_{m=0}^{M_1} \alpha_{R_L,m}\, \mathbf{d}(\tau_{R_L,m})\, \mathbf{1}_G^{\mathrm{T}}\right) \odot \mathbf{A}\big(\boldsymbol{\varphi}_{R_L}^{D}, \boldsymbol{\varphi}_{R_L}^{A}\big), \tag{5}$$

where M_0 and M_1 denote the total numbers of non-LOS single-bounce MPCs and legitimate RIS-associated MPCs, respectively. Assume I SPs in the environment, then $M_0 = I$, $M_1 = 2I$ considering the aforementioned MPCs. The index $m = 0$ corresponds to the main path in each group, i.e., the LOS path and the direct legitimate RIS path, while $m > 0$ indexes the corresponding MPCs:

- $\alpha_{L,0}$ and $\tau_{L,0}$ denote the complex gain and delay of the LOS path, and $\alpha_{L,m}$, $\tau_{L,m}$ for $m > 0$ denote the gains and delays of single-bounce MPCs.
- $\alpha_{R_L,0}$ and $\tau_{R_L,0}$ denote the complex gain and delay of the legitimate RIS path, and $\alpha_{R_L,m}$, $\tau_{R_L,m}$ for $m > 0$ denote the gains and delays of legitimate RIS-associated MPCs.

Here, $\mathbf{d}(\cdot)$ denotes the delay response vector across subcarriers. Its k-th element represents the phase response associated with a specific path (i.e., LOS path, legitimate RIS path, or multipath) delay at the k-th subcarrier, and is given by

$$[\mathbf{d}(\tau)]_k = e^{-j2\pi k\Delta f \tau}. \tag{6}$$

Here, Δf is the subcarrier spacing.

We consider an asynchronous scenario in which a clock offset, denoted by $\Delta\tau$, exists between the BS and the UE. To maintain notational consistency with other distance-related parameters and to facilitate visualization of estimation errors later, the clock offset is expressed with the unit of meter as $B = c\Delta\tau$. Assume the i-th SP is located at $\mathbf{p}_{S,i}$, which generates one single-bounce MPC and two legitimate RIS-associated MPCs (i.e., UE-SP-legitimate RIS-BS and UE-legitimate RIS-SP-BS). The delays of the LOS path, the legitimate RIS path, the corresponding single-bounce multipath, and the UE-legitimate RIS-SP-BS multipath are computed based on distances and the clock offset by

$$\tau_{L,0} = \frac{\|\mathbf{p}_B - \mathbf{p}_U\| + B}{c}, \tag{7}$$

$$\tau_{L,m} = \frac{d_{U,i} + d_{B,i} + B}{c} = \frac{\|\mathbf{p}_U - \mathbf{p}_{S,i}\| + \|\mathbf{p}_B - \mathbf{p}_{S,i}\| + B}{c}, \tag{8}$$

$$\tau_{R_L,0} = \frac{\|\mathbf{p}_U - \mathbf{p}_{R_L}\| + \|\mathbf{p}_B - \mathbf{p}_{R_L}\| + B}{c}, \tag{9}$$

$$\tau_{R_L,m} = \frac{d_{B,i} + d_{R_L,i} + d_{U,R_L} + B}{c} = \frac{\|\mathbf{p}_B - \mathbf{p}_{S,i}\| + \|\mathbf{p}_{R_L} - \mathbf{p}_{S,i}\| + \|\mathbf{p}_U - \mathbf{p}_{R_L}\| + B}{c}. \tag{10}$$

where $d_{U,i}$, $d_{B,i}$, and $d_{R_L,i}$ denote the distances between the i-th SP and the UE, BS, and legitimate RIS, respectively, and d_{U,R_L} denotes the UE-legitimate RIS distance. The delay of UE-SP-legitimate RIS-BS multipath can be obtained similarly to (10). To facilitate the discussion of the delay results in Section VI, we define $d_L = \tau_{L,0} \cdot c$, $d_{R_L} = \tau_{R_L,0} \cdot c$ to represent the pseudoranges corresponding to the LOS path and the legitimate RIS path, respectively.

The matrix $\mathbf{A}(\boldsymbol{\varphi}^D, \boldsymbol{\varphi}^A) \in \mathbb{C}^{K\times G}$ represents the combined RIS response arising from the spatial configuration of the RIS elements and the phase modulation imposed by their controllable reflection coefficients. The angles-of-arrival (AOA) and angles-of-departure (AOD) observed at the RIS side are denoted as $\boldsymbol{\varphi}^A$ and $\boldsymbol{\varphi}^D$, respectively. The entry of this matrix can be obtained by

$$[\mathbf{A}(\boldsymbol{\varphi}^D, \boldsymbol{\varphi}^A)]_{k,g} = \boldsymbol{\omega}_g^\top (\mathbf{a}(\boldsymbol{\varphi}^D) \odot \mathbf{a}(\boldsymbol{\varphi}^A)), \tag{11}$$

where $\boldsymbol{\omega}_g \in \mathbb{C}^{N\times 1}$ is the phase modulation vector with unit norm elements ($|w_{g,n}| = 1$). To consider the discrete phase control for practical RIS, the element $w_{g,n}$ can be further constrained by $w_{g,n} \in \mathcal{S}$, where

$$\mathcal{S} = \left\{ \exp\left(j \left(\frac{2\pi q}{Q} + \frac{\pi}{Q} \right) \right), \quad q = 0, \ldots, Q-1 \right\}. \tag{12}$$

Q is the number of the discrete phase states. The array steering vector under the far-field condition for a certain direction is defined as

$$\mathbf{a}(\boldsymbol{\varphi}) = e^{j \frac{2\pi f_c}{c} \mathbf{Z}^{\mathrm{T}} \mathbf{t}(\boldsymbol{\varphi})}, \tag{13}$$

where matrix $\mathbf{Z} = [\mathbf{z}_1, \ldots, \mathbf{z}_N] \in \mathbb{R}^{3\times N}$ determines the locations of each RIS element under the local coordinate system. The direction vector $\mathbf{t}(\boldsymbol{\varphi})$, representing a specific direction in the local coordinate system, is determined by an azimuth angle ϕ and an elevation angle θ.

We use $\boldsymbol{\varphi}^A_{R_L}$ and $\boldsymbol{\varphi}^D_{R_L}$ to denote the AOA and AOD observed at the legitimate RIS, respectively. The direction vectors for these paths are provided in (14) and (15).

$$\mathbf{t}(\boldsymbol{\varphi}^A_{R_L}) = \mathbf{Q}^{-1}_{R_L} \frac{\mathbf{p}_U - \mathbf{p}_{R_L}}{\|\mathbf{p}_U - \mathbf{p}_{R_L}\|} = \begin{bmatrix} \cos(\phi^A_{R_L})\cos(\theta^A_{R_L}) \\ \sin(\phi^A_{R_L})\cos(\theta^A_{R_L}) \\ \sin(\theta^A_{R_L}) \end{bmatrix}, \tag{14}$$

$$\mathbf{t}(\boldsymbol{\varphi}^D_{R_L}) = \mathbf{Q}^{-1}_{R_L} \frac{\mathbf{p}_B - \mathbf{p}_{R_L}}{\|\mathbf{p}_B - \mathbf{p}_{R_L}\|} = \begin{bmatrix} \cos(\phi^D_{R_L})\cos(\theta^D_{R_L}) \\ \sin(\phi^D_{R_L})\cos(\theta^D_{R_L}) \\ \sin(\theta^D_{R_L}) \end{bmatrix}. \tag{15}$$

B. Legitimate RIS Beamforming

In the following, we discuss the reasonable assumptions for the beamforming design of the legitimate RIS.

1) Beamforming Codebook: The beamforming codebook employed by the legitimate RIS, denoted as $\mathbf{B}_{R_L} = [\mathbf{b}_{R_L,1}, \ldots, \mathbf{b}_{R_L,G}] \in \mathbb{C}^{N\times G}$, is designed based on the level of prior knowledge available to the legitimate system. Two types of codebooks are considered in this work. The first type corresponds to a scenario in which the system has no prior knowledge of the UE location. In this case, random phases are assigned independently to each RIS element, following a uniform distribution over $(0, 2\pi]$ for each orthogonal profile, as commonly used in random phase codebook (RPC) designs [42], [43]. The g-th codeword in the RPC is given by

$$\mathbf{b}^{(1)}_{R_L,g} = e^{j\boldsymbol{\theta}_g}, \quad \boldsymbol{\theta}_g \in \mathbb{R}^{N\times 1}, \quad [\boldsymbol{\theta}_g]_n \sim \mathcal{U}(0, 2\pi]. \tag{16}$$

The second type of codebook assumes that the legitimate RIS has access to coarse information about the UE's location, potentially obtained through initial access procedures or environmental knowledge. In this case, the goal is to steer the reflected beam from the RIS toward the BS using the known BS location and the approximate UE position. Specifically, the AOD from the RIS to the BS is assumed to be accurately known, as the BS is part of the legitimate system and its location information is readily available. In contrast, the AOA from the UE to the RIS is subject to uncertainty. Based on this, a directional beamforming codebook with uncertain AOA (DCUA) is constructed as follows:

$$\mathbf{b}^{(2)}_{R_L,g} = e^{-j\frac{2\pi f_c}{c}\mathbf{Z}^{\mathrm{T}}\left(\mathbf{t}(\tilde{\boldsymbol{\varphi}}^A_{R_L}) + \mathbf{t}(\boldsymbol{\varphi}^D_{R_L})\right)}, \tag{17}$$

where $\tilde{\boldsymbol{\varphi}}^A_{R_L} = \begin{bmatrix} \phi^A_{R_L} + \Delta\phi_g \\ \theta^A_{R_L} + \Delta\theta_g \end{bmatrix}$ and $\Delta\phi_g$, $\Delta\theta_g$ are random perturbations uniformly distributed within a specified uncertainty range.

2) Time-Orthogonal RIS Profile: The time-orthogonal RIS profile is a highly effective method to distinguish between the LoS path and the legitimate RIS path, making it widely used in RIS-aided positioning [40]. This technique involves applying a temporally orthogonal phase profile (based on the original beamforming codebook) to the RIS, followed by a post-processing step at the receiver. Consequently, the final codebook designs incorporating time-orthogonal profiles for the legitimate RIS are denoted as time-orthogonal RPC and time-orthogonal DCUA, i.e., TO-RPC and TO-DCUA, respectively. We employ this technique to enhance the positioning capability of the RIS-aided positioning system.[3] In the following, we present the principles of the time-orthogonal RIS profile used in our positioning system. For ease of notation, we assume G is an even number and

[3]In addition to the benefits offered by time-modulated RIS, this approach may also introduce spectral leakage and generate frequency sidebands. These effects have been investigated in [44] and [45].

define $\mathring{\mathbf{B}}_{R_L} = \left[\mathring{\mathbf{b}}_{R_L,1}\ldots,\mathring{\mathbf{b}}_{R_L,\frac{G}{2}}\right] \in \mathbb{C}^{N\times G/2}$. The extension to odd G follows similarly with appropriate modifications.

The phase modulation vector $\boldsymbol{\omega}_{R_L,g}$ of the legitimate RIS using a time-orthogonal profile is set as

$$\boldsymbol{\omega}_{R_L,1:\frac{G}{2}} = \mathring{\mathbf{b}}_{R_L,1:\frac{G}{2}}, \boldsymbol{\omega}_{R_L,\left(\frac{G}{2}+1\right):G} = -\mathring{\mathbf{b}}_{R_L,1:\frac{G}{2}}, \tag{18}$$

From (4) and (5), we can obtain

$$[\mathbf{Y}_L]_{:,g+\frac{G}{2}} = [\mathbf{Y}_L]_{:,g}, \tag{19}$$

$$[\mathbf{Y}_{R_L}]_{:,g+\frac{G}{2}} = -[\mathbf{Y}_{R_L}]_{:,g}. \tag{20}$$

If there is no unauthorized RIS in the positioning system, the LOS path and the legitimate RIS path can be separated as

$$[\mathring{\mathbf{Y}}_L]_{:,g} = \left([\mathbf{Y}]_{:,g} + [\mathbf{Y}]_{:,g+\frac{G}{2}}\right)/2 = [\mathbf{Y}_L]_{:,g} + \mathring{\mathbf{N}}_L \tag{21}$$

$$[\mathring{\mathbf{Y}}_{R_L}]_{:,g} = \left([\mathbf{Y}]_{:,g} - [\mathbf{Y}]_{:,g+\frac{G}{2}}\right)/2 = [\mathbf{Y}_{R_L}]_{:,g} + \mathring{\mathbf{N}}_{R_L} \tag{22}$$

where $\mathring{\mathbf{Y}}_L$, $\mathring{\mathbf{Y}}_{R_L} \in \mathbb{C}^{K\times\frac{G}{2}}$ are used as updated received signal blocks for positioning. Since the sum of independent Gaussian variables remains Gaussian, $\mathring{\mathbf{N}}_L$ and $\mathring{\mathbf{N}}_{R_L}$ remain additive white Gaussian noise matrices. The employment of orthogonal RIS beamforming design distinguishes RIS path and non-RIS paths. However, the presence of an unauthorized RIS inevitably impacts the accuracy of path separation. These impacts will be discussed in Section III-C.

III. Interference From Unauthorized RIS

RIS technology can also be exploited by adversaries, giving rise to the concept of unauthorized RIS, which is intentionally embedded within the original positioning system due to its low cost and ease of deployment. In this section, we first introduce the threat model, and then update the system model with interference. Finally, we discuss the interference strategies with a focus on beamforming codebook design.

A. Threat Model

We consider a RIS-aided wireless positioning system in which an unauthorized RIS is deliberately deployed to interfere with the positioning process. The adversary's objective is to degrade the positioning accuracy of the UE by increasing estimation error. The unauthorized RIS is assumed to be physically accessible to the adversary, who can freely place and orient it within the environment. The number of elements, orientation, and position of the unauthorized RIS are at the adversary's discretion, limited only by plausible deployment constraints (e.g., within LOS or reflective range of the BS and UE). The adversary controls the phase profile (beamforming codebook) of the unauthorized RIS and may vary its reflection coefficients over time.

Based on the adversary's level of knowledge, we distinguish among three attack scenarios:

- *Blind attack:* In this scenario, the attacker has no prior knowledge of the legitimate RIS-aided positioning system. This represents the simplest attack strategy and does not require specific knowledge of the legitimate system. However, since it generally leads to only limited degradation, it is not expected to be the most effective attack strategy, but it serves as a meaningful baseline case.
- *Geometry-aware attack:* As infrastructure locations are often publicly available or can be readily inferred, it is realistic to assume that the adversary knows the precise locations of the BS and the legitimate RIS. Regarding the UE, we consider both the case in which the attacker has exact location knowledge and the case in which only coarse location information is available. This attack model is particularly feasible in practice, since geometric information is generally easier to acquire than protocol-level information, such as pilot signals. For this reason, the geometry-aware attack constitutes the most practically relevant scenario considered in this work and is therefore of particular importance in our analysis.
- *Worst-case attack:* In this scenario, the attacker is assumed to have complete knowledge of the system, including the exact locations of the legitimate RIS, UE, and BS, as well as the pilot signals and the transmission protocol. Such an attacker can, in principle, severely degrade the positioning performance. Nevertheless, this model relies on strong prior knowledge and therefore should not be regarded as a common practical deployment scenario.

The legitimate system is unaware of the presence or configuration of the unauthorized RIS and continues to operate under the nominal system model, treating all observed signals as arising from the expected channel structure and the known authorized RIS. Countermeasures such as adversarial RIS detection, positioning, or advanced multi-antenna discrimination are out of scope and left as future work.

B. System Model With Interference

Assume an unauthorized RIS is introduced into the previously described positioning system, as illustrated in Fig. 1. The unauthorized RIS contains N_2 passive reflective elements and its position, orientation and its corresponding rotation matrix are denoted by $\mathbf{p}_{R_U} \in \mathbb{R}^3$, $\mathbf{o}_{R_U} \in \mathbb{R}^3$ and $\mathbf{Q}_{R_U}$, respectively. Considering the interference from the unauthorized RIS, the received signal matrix $\mathbf{Y} \in \mathbb{C}^{K\times G}$ is given as

$$\mathbf{Y} = \mathbf{Y}_L + \mathbf{Y}_{R_L} + \mathbf{Y}_{R_U} + \mathbf{N}, \tag{23}$$

where $\mathbf{Y}_{R_U}$ represents the received signals passing through the unauthorized RIS. The matrix $\mathbf{Y}_{R_U}$ can be further expressed as

$$\begin{aligned}\mathbf{Y}_{R_U} &= \mathbf{H}_{R_U} \odot \mathbf{X} \\ &= \left(\sum_{m=0}^{M_2} \alpha_{R_U,m}\,\mathbf{d}(\tau_{R_U,m})\,\mathbf{1}_G^{\mathrm{T}}\right) \odot \mathbf{A}\left(\boldsymbol{\varphi}_{R_U}^{D}, \boldsymbol{\varphi}_{R_U}^{A}\right),\end{aligned} \tag{24}$$

where $\mathbf{H}_{R_U}$ is the channel matrix for the unauthorized RIS-associated paths. Complex channel gains, delays, AOA and AOD of paths involving unauthorized RIS are denoted similarly to legitimate RIS.

TABLE I
SUMMARY OF CODEBOOKS USED BY LEGITIMATE AND UNAUTHORIZED RISs

RIS Type	Codebook Name (Abbreviation)	Description / Characteristics
Legitimate RIS	Time-Orthogonal Random Phase Codebook (TO-RPC)	Employs randomly generated phase shifts. The resulting profiles are orthogonal across transmission time slots.
	Time-Orthogonal Directional Codebook with Uncertain AOA (TO-DCUA)	Aims to steer the RIS beam toward the BS, leveraging knowledge of the BS location and coarse UE location incorporating AOA uncertainties. Codewords are orthogonal across transmission slots.
Unauthorized RIS	Random Phase Codebook (RPC)	Similar to TO-RPC but without applying time-orthogonal profiles.
	Directional Codebook (DC)	Assumes accurate knowledge of both UE and BS positions. Generates fixed beams directed toward the BS.
	Directional Codebook with Uncertain AOA (DCUA)	Similar to TO-DCUA, but does not employ time-orthogonal profiles.
	Directional Codebook with Phase Offset (DCPO)	Extends DC by introducing an additional random phase offset across transmission slots.

C. Codebook Design Strategies

When the legitimate RIS employs the time-orthogonal profile, the presence of an unauthorized RIS inevitably impacts the accuracy of path separation. The received signal blocks in (21) and (22) are updated as

$$[\mathring{\mathbf{Y}}_L]_{:,g} = [\mathbf{Y}_L]_{:,g} + \left([\mathbf{Y}_{R_U}]_{:,g} + [\mathbf{Y}_{R_U}]_{:,g+\frac{G}{2}}\right)/2 + \mathring{\mathbf{N}}_L \tag{25}$$

$$[\mathring{\mathbf{Y}}_{R_L}]_{:,g} = [\mathbf{Y}_{R_L}]_{:,g} + \left([\mathbf{Y}_{R_U}]_{:,g} - [\mathbf{Y}_{R_U}]_{:,g+\frac{G}{2}}\right)/2 + \mathring{\mathbf{N}}_{R_L}. \tag{26}$$

The positioning system aims to separate the propagation paths through post-processing at the receiver, as shown in (21) and (22). However, when accounting for interference from unauthorized RIS, the actual received signal blocks are given by (25) and (26). It can be inferred that the selection of the beamforming codebook employed by the unauthorized RIS, i.e., $\mathbf{B}_{R_U} = [\mathbf{b}_{R_U,1}, \ldots, \mathbf{b}_{R_U,G}] \in \mathbb{C}^{N\times G}$, will have a significant impact on the effectiveness of path separation, affecting the overall positioning accuracy.

In the aforementioned three attack scenarios, the adversary is assumed to possess different levels of knowledge about the legitimate system, which largely determines the design of the codebook employed by the unauthorized RIS. For the blind attack, the RPC codebook can be used at the unauthorized RIS, i.e., $\mathbf{b}^{(1)}_{R_U,g}$, generated analogously to (16). For the geometry-aware attack with prior knowledge of the coarse UE location, the DCUA codebook can be used at the unauthorized RIS, i.e., $\mathbf{b}^{(2)}_{R_U,g}$, generated analogously to (17). For the geometry-aware attack with prior knowledge of the precise UE location, we first consider a codebook that follows classical beamforming principles and steers the reflected beam toward the BS. Based on (11) and (13), the codeword of this directional codebook (DC) for the g-th transmission is given by

$$\mathbf{b}^{(3)}_{R_U,g} = e^{-j\frac{2\pi f_c}{c}\mathbf{Z}^{\mathrm{T}}\left(\mathbf{t}(\boldsymbol{\varphi}^A_{R_U})+\mathbf{t}(\boldsymbol{\varphi}^D_{R_U})\right)}. \tag{27}$$

Without phase variations across time slots, the interference from the unauthorized RIS can be effectively mitigated due to the time-orthogonal profiles employed by the legitimate RIS based on (25) and (26). Hence, the DC for unauthorized RIS can be further strengthened by introducing an additional phase offset for all elements across different transmissions. This offset remains constant during each transmission but varies across time, introducing diversity without altering the overall beam direction. The codeword of this directional codebook with phase offset (DCPO) can be constructed as

$$\mathbf{b}^{(4)}_{R_U,g} = e^{-j\frac{2\pi f_c}{c}\mathbf{Z}^{\mathrm{T}}\left(\mathbf{t}(\boldsymbol{\varphi}^A_{R_U})+\mathbf{t}(\boldsymbol{\varphi}^D_{R_U})\right)-j\,\varphi_g}, \tag{28}$$

where $\varphi_g \sim \mathcal{U}(0, 2\pi]$ is a transmission-dependent global phase offset applied uniformly to all RIS elements. It remains constant for all RIS elements but varies across different transmissions, thereby introducing temporal phase diversity without modifying the beam direction.

For the worst-case attack, the codebook can be specifically designed when the adversary is assumed to possess all relevant system information. In this case, the unauthorized RIS deliberately optimizes its reflection codebook to minimize the residual power of the legitimate RIS path after path separation, subject to the feasible reflection-coefficient constraints imposed by the RIS hardware, formulated as

$$\begin{aligned}\mathbf{B}^{\star}_{R_U} = \arg\min_{\mathbf{B}_{R_U}} \sum_{g=1}^{G/2} \left\| [\mathbf{Y}_{R_L}]_{:,g} + \frac{1}{2}\Delta\mathbf{y}_{R_U,g}(\mathbf{B}_{R_U}) \right\|_2^2 \\ \text{s.t. } [\mathbf{b}_{R_U,g}]_n \in \mathcal{S}_{R_U}, \\ n = 1,\ldots,N, \;\; g = 1,\ldots,G,\end{aligned} \tag{29}$$

where $\Delta\mathbf{y}_{R_U,g}(\mathbf{B}_{R_U}) \triangleq [\mathbf{Y}_{R_U}(\mathbf{B}_{R_U})]_{:,g} - [\mathbf{Y}_{R_U}(\mathbf{B}_{R_U})]_{:,g+G/2}$, and $\mathcal{S}_{R_U}$ denotes the feasible set of RIS reflection coefficients. In the extreme case where the unauthorized RIS path has the same delay and angle of arrival as the legitimate RIS path, the unauthorized RIS could, in principle, choose its codebook such that its reflected signal destructively cancels the legitimate RIS contribution after path separation, thereby severely degrading the system's positioning capability. Nevertheless, this model relies on strong prior knowledge and is therefore impractical. Consequently, we do not provide additional bound derivations or simulations for this scenario. The codebooks used by the legitimate and unauthorized RISs are summarized in Table I.

D. Potential Countermeasures

Although the primary goal of this study is to investigate the potential impact of interference from the unauthorized RIS, it is also valuable to provide insights into possible extensions of current models as well as countermeasures against such threats.

- *Advanced beamforming strategies:* While the SISO setup serves as an appropriate baseline for investigating the impact of an unauthorized RIS, multiple antennas at the BS or UE enable implementing advanced beamforming algorithms with varying levels of prior knowledge of the unauthorized RIS. For instance, the BS or UE can optimize its beamforming algorithm to achieve low gain toward the direction of the unauthorized RIS by implementing nulling operations.
- *Introducing more legitimate RISs:* When two legitimate RISs are deployed in the system, one can assist in the positioning task while the other can employ a specially designed beamforming strategy to suppress the interference from the unauthorized RIS. When more legitimate RISs are available, the reliability of the positioning performance can be further enhanced by appropriately weighting the positioning results obtained from different legitimate RISs. In general, this corresponds to increased redundancy in the system, which can also be achieved by using more antennas or more BSs. However, the overhead of the system will be increased.
- *Advanced pilot signal design:* The design of pilot signals can also be adapted to mitigate the impact of an unauthorized RIS. Rather than using deterministic, globally known pilots, the BS may employ key-driven, user-specific pilot sequences and time-frequency scrambling patterns that are shared only with the intended UE. Such designs (e.g., phase-hopping, subcarrier permutation, or index-modulated pilots) reduce the ability of an unauthorized RIS to maintain coherent phase alignment of its reflected path across pilot symbols and to emulate a geometrically consistent additional link. In practice, this forces the unauthorized RIS either to act as an uncontrolled passive reflector, whose contribution can be partially downweighted in the estimator, or to resort to more complex active strategies, which increases its detectability.

IV. Bound Analysis

Based on the above signal models, we define the channel parameter vector as $\boldsymbol{\eta} = [\boldsymbol{\eta}_L^\top, \boldsymbol{\eta}_{R_L}^\top]^\top = [\tau_{L,0}, \rho_{L,0}, \beta_{L,0}, \phi^A_{R_L}, \theta^A_{R_L}, \tau_{R_L,0}, \rho_{R_L,0}, \beta_{R_L,0}]^\top$, which contains the channel parameters associated with the LOS and legitimate RIS paths. In the vector $\boldsymbol{\eta}$, ρ and β denote the amplitude and phase of the complex channel gain, respectively, i.e., $\alpha = \rho e^{-j\beta}$. The state vector is defined as $\mathbf{s} = [\mathbf{p}_U^\top, B]^\top$, which includes the 3D position of the UE and the clock offset. The parameters related to the MPCs are not included in this bound analysis, as they do not directly contribute to position estimation. In the following, we derive the theoretical lower bounds for channel parameters and state parameters to analyze the degradation in positioning performance resulting from the mismatch between the assumed model (without considering unauthorized RIS) and the true model with unauthorized RIS.

A. CRB Analysis for the Interference-Free Model

The CRB [39] for the interference-free model is first derived, which serves as a reference to evaluate the impact of the presence of an unauthorized RIS.

The channel parameter vectors for the interference-free model and the true model are the same, since the presence of unauthorized RIS will not affect the LOS path and the legitimate RIS path. Based on the signal model in (1) (4) and (5), the Fisher information matrix (FIM) $\boldsymbol{\mathcal{I}}(\boldsymbol{\eta}) \in \mathbb{R}^{8\times 8}$ of the channel estimation is

$$\boldsymbol{\mathcal{I}}(\boldsymbol{\eta}) = \frac{2}{\sigma_n^2}\sum_{k=1}^{K}\sum_{g=1}^{G}\Re\left\{\left(\frac{\partial \tilde{\mu}_{k,g}}{\partial \boldsymbol{\eta}}\right)^{\mathrm{H}}\left(\frac{\partial \tilde{\mu}_{k,g}}{\partial \boldsymbol{\eta}}\right)\right\}, \tag{30}$$

where $\tilde{\mu}_{k,g}$ is the noise-free observation of the received signal $\tilde{\mathbf{Y}}$ in (1). We then define the scalar CRB for channel parameters as

$$\mathrm{CRB}_{\boldsymbol{\eta}} = \sqrt{\mathrm{tr}\Big([\boldsymbol{\mathcal{I}}(\boldsymbol{\eta})^{-1}]_{1:8,1:8}\Big)}. \tag{31}$$

The CRB matrix for the UE states is obtained by

$$\mathbf{C}_{\mathbf{s}} = \boldsymbol{\mathcal{I}}(\mathbf{s})^{-1} = \left[\mathbf{J}_s^\top \boldsymbol{\mathcal{I}}(\boldsymbol{\eta})\mathbf{J}_s\right]^{-1}, \tag{32}$$

where $\mathbf{J}_s = \partial\boldsymbol{\eta}/\partial\mathbf{s}$. The corresponding scalar CRB for the state vector is defined as $\mathrm{CRB}_{\mathbf{s}} = \sqrt{\mathrm{tr}(\mathbf{C}_{\mathbf{s}})}$.

B. MCRB and MLB Analysis for Channel Parameters

With the MCRB and mismatched lower bound (MLB) analyzed below, we quantify the performance degradation caused by the presence of an unauthorized RIS in the positioning system. We denote $\mathbf{y} \in \mathbb{C}^{GK} = \mathrm{vec}(\mathbf{Y})$ as the received signal vector for the true model (that is, in the presence of the unauthorized RIS). The probability density function (PDF) of the true model can be expressed as $p(\mathbf{y}|\bar{\boldsymbol{\eta}})$, where $\bar{\boldsymbol{\eta}}$ is the vector of true channel parameters that contains all the channel parameters. Similarly, the PDF of the misspecified model is expressed as $\tilde{p}(\mathbf{y}|\boldsymbol{\eta})$.

1) Pseudo-True Parameter: The pseudo-true parameter is the point that minimizes the Kullback-Leibler (KL) divergence between $p(\mathbf{y}|\bar{\boldsymbol{\eta}})$ and $\tilde{p}(\mathbf{y}|\boldsymbol{\eta})$. It is defined as [46]

$$\boldsymbol{\eta}_0 = \arg\min_{\boldsymbol{\eta}} D_{\mathrm{KL}}\left(p(\mathbf{y} \mid \bar{\boldsymbol{\eta}}) \,\|\, \tilde{p}(\mathbf{y} \mid \boldsymbol{\eta})\right). \tag{33}$$

$\boldsymbol{\mu}(\boldsymbol{\eta})$ and $\tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})$ are the noise-free received signal vectors for the true model and the interference-free model, respectively. The difference between these two vectors is defined as $\boldsymbol{\epsilon}(\boldsymbol{\eta}) \triangleq \boldsymbol{\mu}(\boldsymbol{\eta}) - \tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})$. Another interpretation of the pseudo-true parameter $\boldsymbol{\eta}_0$ is

$$\boldsymbol{\eta}_0 = \arg\min_{\boldsymbol{\eta}} \|\boldsymbol{\epsilon}(\boldsymbol{\eta})\|^2. \tag{34}$$

2) MCRB and MLB: Under model mismatch caused by the presence of an unauthorized RIS, the Fisher information matrices admit two possible generalizations, denoted by $\mathbf{A}_{\eta_0}$ and $\mathbf{B}_{\eta_0}$. Following the theory of the MCRB [47], it can be expressed as

$$\mathrm{MCRB}(\boldsymbol{\eta}_0) = \mathbf{A}_{\boldsymbol{\eta}_0}^{-1}\mathbf{B}_{\boldsymbol{\eta}_0}\mathbf{A}_{\boldsymbol{\eta}_0}^{-1}. \tag{35}$$

The matrices $\mathbf{A}_{\boldsymbol{\eta}_0}$ and $\mathbf{B}_{\boldsymbol{\eta}_0}$ are both evaluated at the pseudo-true parameter $\boldsymbol{\eta}_0$. When the assumed model coincides with the true model, i.e., there is no model mismatch, $\mathbf{A}_{\boldsymbol{\eta}_0} = -\mathbf{B}_{\boldsymbol{\eta}_0}$ and (35) reduces to the classical CRB.

To account for the estimator performance under model misspecification, the mismatched lower bound (MLB) for channel parameter estimation can be expressed as

$$\mathrm{MLB}_{\mathrm{ch}}(\boldsymbol{\eta}_0) = \underbrace{\mathbf{A}_{\boldsymbol{\eta}_0}^{-1}\mathbf{B}_{\boldsymbol{\eta}_0}\mathbf{A}_{\boldsymbol{\eta}_0}^{-1}}_{\mathrm{MCRB}(\boldsymbol{\eta}_0)} + \underbrace{(\bar{\boldsymbol{\eta}} - \boldsymbol{\eta}_0)(\bar{\boldsymbol{\eta}} - \boldsymbol{\eta}_0)^\top}_{\mathrm{Bias}(\boldsymbol{\eta}_0)}. \quad (36)$$

As shown in (36), the MLB consists of two terms: the MCRB term and the bias term. The MCRB represents the variance-related component and varies with SNR similarly to the conventional CRB; hence, the MLB is dominated by the MCRB at low SNR. In contrast, the bias term is independent of transmit power and captures the systematic error caused by the mismatch between the assumed and true models, thereby determining the estimator performance floor at high SNR. The elements in matrices $\mathbf{A}_{\boldsymbol{\eta}_0}$ and $\mathbf{B}_{\boldsymbol{\eta}_0}$ are defined as

$$\begin{aligned}\left[\mathbf{A}_{\boldsymbol{\eta}_0}\right]_{i,j} &= \int \frac{\partial^2 \ln \tilde{p}(\mathbf{y}\mid\boldsymbol{\eta})}{\partial\eta_i\partial\eta_j} p(\mathbf{y}\mid\bar{\boldsymbol{\eta}})\,\mathrm{d}\mathbf{y}\Big|_{\boldsymbol{\eta}=\boldsymbol{\eta}_0} \\ &= \mathbb{E}_{p(\mathbf{y}\mid\bar{\boldsymbol{\eta}})}\left[\frac{\partial^2}{\partial\eta_i\partial\eta_j}\ln\tilde{p}(\mathbf{y}\mid\boldsymbol{\eta})\right]_{\boldsymbol{\eta}=\boldsymbol{\eta}_0}, \end{aligned} \quad (37)$$

$$\begin{aligned}\left[\mathbf{B}_{\boldsymbol{\eta}_0}\right]_{i,j} &= \int \frac{\partial}{\partial\eta_i}\ln\tilde{p}(\mathbf{y}\mid\boldsymbol{\eta})\,\frac{\partial}{\partial\eta_j}\ln\tilde{p}(\mathbf{y}\mid\boldsymbol{\eta})\,p(\mathbf{y}\mid\bar{\boldsymbol{\eta}})\,\mathrm{d}\mathbf{y}\Big|_{\boldsymbol{\eta}=\boldsymbol{\eta}_0} \\ &= \mathbb{E}_{p(\mathbf{y}\mid\bar{\boldsymbol{\eta}})}\left[\frac{\partial}{\partial\eta_i}\ln\tilde{p}(\mathbf{y}\mid\boldsymbol{\eta})\,\frac{\partial}{\partial\eta_j}\ln\tilde{p}(\mathbf{y}\mid\boldsymbol{\eta})\right]\Bigg|_{\boldsymbol{\eta}=\boldsymbol{\eta}_0}. \end{aligned} \quad (38)$$

The detailed derivations of these two matrices can be found in [48].

C. Absolute Lower Bound for 3D Positioning

Estimation of position and clock offset from the estimated channel parameter vector in the presence of an unauthorized RIS is also a mismatched estimation problem. The MLB for the state vector is given by

$$\mathrm{MLB}_{\mathbf{s}}(\mathbf{s}_0) = \mathrm{MCRB}(\mathbf{s}_0) + (\bar{\mathbf{s}} - \mathbf{s}_0)(\bar{\mathbf{s}} - \mathbf{s}_0)^\top, \quad (39)$$

where $\bar{\mathbf{s}}$ and $\mathbf{s}_0$ are the true and pseudo-true state parameter vectors, respectively. The pseudo-true state vector $\mathbf{s}_0$ can be obtained as [17]

$$\mathbf{s}_0 = \arg\min_{\mathbf{s}} \left(\boldsymbol{\eta}_0 - \boldsymbol{\eta}(\mathbf{s})\right)^\top \boldsymbol{\mathcal{I}}(\bar{\boldsymbol{\eta}})\left(\boldsymbol{\eta}_0 - \boldsymbol{\eta}(\mathbf{s})\right). \quad (40)$$

The MCRB for the state vector can, in principle, be derived using calculations similar to those in Section IV-B. However, this derivation becomes computationally demanding, especially for 3D scenarios with massive transmissions. Since the MLB converges to its bias term at high SNR, we focus on the bias component in the following analysis. Let $\mathbf{A}_s = [\mathbf{I}_3, \mathbf{0}_{3\times 1}]$ and $\mathbf{a}_B = [\mathbf{0}_{1\times 3}, 1]$ extract the UE position and clock offset from $(\bar{\mathbf{s}} - \mathbf{s}_0)(\bar{\mathbf{s}} - \mathbf{s}_0)^\top$, respectively. The scalar ALBs for UE position and clock-offset estimation are defined as $\mathrm{ALB}_{\mathrm{pos}} = \sqrt{\mathrm{tr}(\mathbf{A}_s(\bar{\mathbf{s}} - \mathbf{s}_0)(\bar{\mathbf{s}} - \mathbf{s}_0)^\top\mathbf{A}_s^\top)}$ and $\mathrm{ALB}_B = |\mathbf{a}_B(\bar{\mathbf{s}} - \mathbf{s}_0)|$.

V. Positioning Algorithms

Based on the models described in Section III, the positioning problem under interference from an unauthorized RIS is formulated as follows. Given the observations $\mathbf{Y}$ in (23), the first step is to estimate the channel parameter vector $\boldsymbol{\eta}$. Subsequently, the state vector $\mathbf{s}$ is determined.[4]

In the following, we enhance the robustness of the low-complexity estimation algorithm with respect to delay estimation under interference. The coarse estimates obtained from this algorithm can be further refined using maximum likelihood estimator (MLE). For convenience of algorithm development later, here we define the non-redundant channel parameter vector as $\boldsymbol{\eta}_N = [\tau_{L,0}, \phi_{R_L}^A, \theta_{R_L}^A, \tau_{R_L,0}]^\top$.

A. Low-Complexity Estimation

In the absence of interference from an unauthorized RIS, the received signals from the LOS and legitimate RIS paths can be effectively separated by employing an orthogonal RIS profile on the legitimate RIS, as shown in (21) and (22). In this case, the delays of the LOS and legitimate RIS paths can be estimated by applying a discrete Fourier transform (DFT) to the corresponding channel frequency responses, as demonstrated in [6]. However, in the actual signal model, interference from an unauthorized RIS degrades the path separation performance, as shown in (25) and (26). The following section presents an approach to estimating delays in the presence of an unauthorized RIS.

1) LOS Channel Parameter Estimation: For the LOS path, interference from the unauthorized RIS has minimal impact on the received signals, as the LOS path signal power is significantly higher than that of the unauthorized RIS path. The latter experiences a greater propagation loss due to its longer link distance, an effect that is particularly pronounced in the mmWave and higher frequency bands [41]. Consequently, the LOS path delay can still be accurately estimated by applying a DFT to the estimated channel response of the LOS path. To this end, we first estimate the channel response vector of LOS path $\hat{\mathbf{h}}_L \in \mathbb{C}^K$ as

$$\hat{\mathbf{h}}_L = \sum_{g=1}^{G/2}\left[\mathring{\mathbf{Y}}_L\right]_{:,g} \odot \mathbf{x}^*. \quad (41)$$

The estimated delay of the LOS path $\hat{\tau}_L$ is then obtained by

$$\hat{\tau}_{L,0} = \arg\max_{\tau}\left|\mathbf{d}^{\mathrm{H}}(\tau)\hat{\mathbf{h}}_L\right|. \quad (42)$$

2) RIS Channel Parameter Estimation: Estimating the delay of the legitimate RIS path is more challenging due to interference from the unauthorized RIS. The estimated channel response for the legitimate RIS path is given by

$$\hat{\mathbf{H}}_{R_L} = \mathring{\mathbf{Y}}_{R_L} \odot \left(\mathbf{x}^*\mathbf{1}_{G/2}^\top\right) \in \mathbb{C}^{K\times G/2}. \quad (43)$$

If we apply a method similar to the one shown in (42), the estimated delay for the legitimate RIS is given by

$$\hat{\tau}_{R_L,0} = \arg\max_{\tau}\|\mathbf{d}^{\mathrm{H}}(\tau)\hat{\mathbf{H}}_{R_L}\|. \quad (44)$$

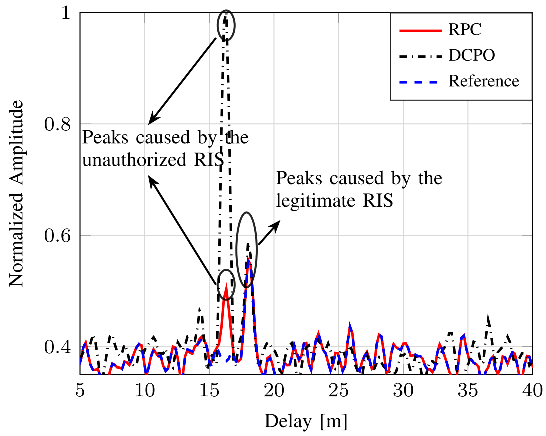


Fig. 2. DFT results for estimating d_{R_L} when the legitimate RIS employs TO-RPC and the unauthorized RIS employs either the RPC or DCPO. The remaining simulation parameters are summarized in Table II.

However, directly applying a DFT to $\hat{\mathbf{H}}_{R_L}$ and selecting the delay corresponding to the maximum value as implemented in [6] is unlikely to yield the correct delay estimate. As shown in Fig. 2, the presence of the unauthorized RIS introduces multiple significant peaks, whereas only a single dominant peak appears in the reference case without interference. When comparing results obtained using RPC and DCPO for the unauthorized RIS, the interference-induced peak can even surpass the legitimate RIS peak, leading to incorrect delay estimation if the LOS path method is applied. To address this issue, we identify all prominent peaks in the DFT result for $\hat{\mathbf{H}}_{R_L}$ using a one-dimensional search.

Assuming a total of I local maxima are identified, the estimated delay vector consists of the delay bins corresponding to these recognized peaks, expressed as $\widehat{\boldsymbol{\tau}} = [\widehat{\tau}_1, \cdots, \widehat{\tau}_I]^\top$. The estimated channel parameters of the legitimate RIS, $\hat{\phi}_{R_L}^A, \hat{\theta}_{R_L}^A$, and $\hat{\tau}_{R_L,0}$, are then obtained by solving

$$\left[\hat{\phi}_{R_L}^A, \hat{\theta}_{R_L}^A, \hat{\tau}_{R_L,0}\right] = \arg \max_{\phi,\theta,\tau\in\widehat{\boldsymbol{\tau}}} \mathcal{L}(\phi,\theta,\tau), \tag{45}$$

where

$$\mathcal{L}(\phi,\theta,\tau) = \sum_{g,k} \left| \boldsymbol{\omega}_{R_L,g}^\top e^{\frac{j2\pi}{\lambda_c}\mathbf{Z}^\top \mathbf{t}(\boldsymbol{\varphi})} d_k(\tau) x_k \mathring{y}_{k,g}^* \right|. \tag{46}$$

Moreover, $\mathbf{t}(\boldsymbol{\varphi})$ is derived from ϕ and θ according to (14) (15) and $\mathring{y}_{k,g}$ is the entry of the matrix $\mathring{\mathbf{Y}}$. A 2D search with a specified angular step size is performed for ϕ and θ to solve the problem described in (45).

3) Closed-Form Position Estimation: We next derive a closed-form solution for state vector estimation, based on the estimated AOA pairs $\hat{\phi}_{R_L}^A$, $\hat{\theta}_{R_L}^A$ and delays $\hat{\tau}_{L,0}$, $\hat{\tau}_{R_L,0}$. The key idea is to determine the UE position along the direction vector from the legitimate RIS, given by $\hat{\mathbf{t}} = \mathbf{Q}_{R_L}\mathbf{t}(\hat{\phi}_{R_L}^A, \hat{\theta}_{R_L}^A)$, as shown in (14) (15). To facilitate problem formulation, we define $d_R \triangleq \|\mathbf{p}_B - \mathbf{p}_{R_L}\|$ as the distance between the legitimate RIS and BS. Additionally, we introduce an auxiliary parameter r as the distance between the UE and legitimate RIS, such that

$$\hat{\mathbf{p}}_U(r) = \mathbf{p}_{R_L} + r\hat{\mathbf{t}}. \tag{47}$$

Subtracting (9) from (7), the clock offset is canceled out as

$$r + \underbrace{d_R + c\hat{\tau}_{L,0} - c\hat{\tau}_{R_L,0}}_{\hat{d}_\Delta} = \|\mathbf{p}_U - \mathbf{p}_B\|. \tag{48}$$

After squaring both sides, we obtain

$$(r + \hat{d}_\Delta)^2 = r^2 + 2r\hat{\mathbf{t}}^\top(\mathbf{p}_{R_L} - \mathbf{p}_B) + d_R^2, \tag{49}$$

and the closed-form solution of the auxiliary parameter r is

$$r = \frac{\hat{d}_\Delta^2 - d_R^2}{2\hat{\mathbf{t}}^\top(\mathbf{p}_{R_L} - \mathbf{p}_B) - 2\hat{d}_\Delta}. \tag{50}$$

The estimated parameter $\hat{r}$ is then substituted in (47) to obtain $\hat{\mathbf{p}}_U$, while B can be estimated accordingly. In interference-free scenarios, a MLE can be employed to achieve higher positioning accuracy [40]. The output of the low-complexity estimator can serve as an initial point for MLE, followed by iterative gradient-based refinement.

B. Mismatched Maximum Likelihood Estimator

MLE can be used to estimate the optimal channel parameters. However, the true received signal vector $\mathbf{y}$ is observed in the presence of the unauthorized RIS in our case, and the MLE does not know the signal model of the unauthorized RIS path. Therefore, there is a mismatch between the signal model assumed by the estimator and the true signal model. The channel parameters estimated by the mismatched MLE can be given as

$$\hat{\boldsymbol{\eta}}_{\text{MLE}} = \arg \max_{\boldsymbol{\eta}} \ln \tilde{p}(\mathbf{y}|\boldsymbol{\eta}), \tag{51}$$

where $\ln \tilde{p}(\mathbf{y}|\boldsymbol{\eta})$ is the log-likelihood of the mismatched model (1). The estimated $\boldsymbol{\eta}_N$ obtained from the first step of the low-complexity estimator can be used as an initial estimate for the following refining estimation process. Based on (51), the refined estimation is formulated as

$$\hat{\boldsymbol{\eta}}_{\text{MLE}} = \arg \min_{\boldsymbol{\eta}} \|\mathbf{y} - \tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})\|^2. \tag{52}$$

To further refine the initial estimate of $\boldsymbol{\eta}_N$, the estimation is optimized as follows [6].

$$\hat{\boldsymbol{\eta}}_N = \arg \min_{\boldsymbol{\eta}_N} \left\|\mathring{\boldsymbol{\mu}} - \mathbf{M}(\boldsymbol{\eta}_N)\mathbf{M}^\dagger(\boldsymbol{\eta}_N)\mathring{\boldsymbol{\mu}}\right\|, \tag{53}$$

where $\mathbf{M}^\dagger = (\mathbf{M}^{\text{H}}\mathbf{M})^{-1}\mathbf{M}^{\text{H}}$, $\mathring{\boldsymbol{\mu}} = \text{vec}(\mathring{\mathbf{Y}}_L + \mathring{\mathbf{Y}}_{R_L})$, and $\mathbf{M}(\boldsymbol{\eta}_N) = [\mathbf{m}_L, \mathbf{m}_{R_L}]$, with $\mathbf{m}_L = \text{vec}(\mathbf{d}(\tau_{L,0})\mathbf{1}_G^\text{T} \odot \mathbf{X})$ and $\mathbf{m}_{R_L} = \text{vec}(\mathbf{d}(\tau_{R_L,0})\mathbf{1}_G^\text{T} \odot \mathbf{A}(\boldsymbol{\varphi}_{R_L}^D, \boldsymbol{\varphi}_{R_L}^A) \odot \mathbf{X})$. The nuisance gain vector $[\alpha_{L,0}, \alpha_{R_L,0}]^\text{T}$ is eliminated by projection onto the column space of $\mathbf{M}(\boldsymbol{\eta}_N)$.

With the refined $\boldsymbol{\eta}_N$ and the initial state parameters obtained in (53), the refined state parameter vector using mismatched MLE is obtained as

$$\hat{\mathbf{s}} = \arg \min_{\mathbf{s}} \left(\hat{\boldsymbol{\eta}}_N - \boldsymbol{\eta}_N(\mathbf{s})\right)^\top \boldsymbol{\mathcal{I}}(\boldsymbol{\eta}_N) \left(\hat{\boldsymbol{\eta}}_N - \boldsymbol{\eta}_N(\mathbf{s})\right), \tag{54}$$

where $\boldsymbol{\mathcal{I}}(\boldsymbol{\eta}_N) \in \mathbb{R}^{4\times 4}$ is the equivalent FIM which can be simply obtained from the submatrix of $\boldsymbol{\mathcal{I}}(\boldsymbol{\eta})$.

[4]The complex channel gains for each path are also estimated but treated as nuisance parameters and are not included in the state vector.

TABLE II
DEFAULT PARAMETER SETTINGS

Signal & Frequency Parameters	
Center frequency	30 GHz
Bandwidth	400 MHz
Number of subcarriers	K = 512
Number of symbols	G = 192
Noise figure	10 dB
clock offset	$B = 5$ m
Geometry Parameters	
BS position	$\mathbf{p}_B = [0,0,0]^\top$
UE position	$\mathbf{p}_U = [1,4,-2]^\top$
Dimensions of legitimate RIS	$N = 10 \times 10$
Dimensions of unauthorized RIS	$M = 10 \times 10$
Legitimate RIS position	$\mathbf{p}_{R_L} = [-2,4,0]^\top$
Legitimate RIS orientation	$\mathbf{o}_{R_L} = [0,0,0]^\top$
Unauthorized RIS position	$\mathbf{p}_{R_U} = [2,5,0]^\top$
Unauthorized RIS orientation	$\mathbf{o}_{R_U} = [0,0,0]^\top$

C. Computational Complexity

Aligned with the signal model, K denotes the number of subcarriers, G the number of symbols, N_1 the number of elements in the legitimate RIS, I the number of candidate delays retained after the one-dimensional scan, and $N_\phi \times N_\theta$ represents the size of the angular grid.

In the coarse stage, forming the per-profile observations and performing the delay-domain FFTs over K subcarriers and G symbols requires $\mathcal{O}(GK \log K)$ operations. For each retained delay, the subsequent (ϕ, θ) grid search evaluates the RIS steering vector and a symbol-domain inner product at every angular grid point, leading to a complexity of $\mathcal{O}(IN_1N_\phi N_\theta G)$. The refinement stage incurs an additional cost that is linear in GK per iteration; since the number of refinement iterations is small and fixed in our simulations, it can be treated as a constant factor. Overall, for one BS-UE pair and a single legitimate RIS, the resulting complexity scales as

$$\mathcal{O}\big(G(K \log K + IN_1N_\phi N_\theta)\big), \tag{55}$$

where the hidden constants depend on simulation-level choices (e.g., I, N_1).

When multiple legitimate RISs and UEs are present, time-orthogonal profiles can be assigned to each BS-UE-RIS link, enabling separation at the BS. In this case, the total positioning complexity scales linearly with the number of legitimate RISs and linearly with the number of UEs, and can be further reduced by parallel implementation. We emphasize that our goal is not to design an ultra-low-complexity estimator, but to employ a conventional grid-search-plus-refinement mismatched MLE that is general, easy to implement, and suitable as a benchmark for assessing the impact of an unauthorized RIS on positioning performance.

VI. NUMERICAL SIMULATIONS

We consider a 3D RIS-aided positioning scenario involving one legitimate RIS and one unauthorized RIS, as illustrated in Fig. 1. The default simulation parameters are summarized in Table II. We select 30 GHz as the carrier frequency, which falls within 5G NR Frequency Range 2 (FR2). FR2 is well suited to RIS-aided positioning due to its large available bandwidth

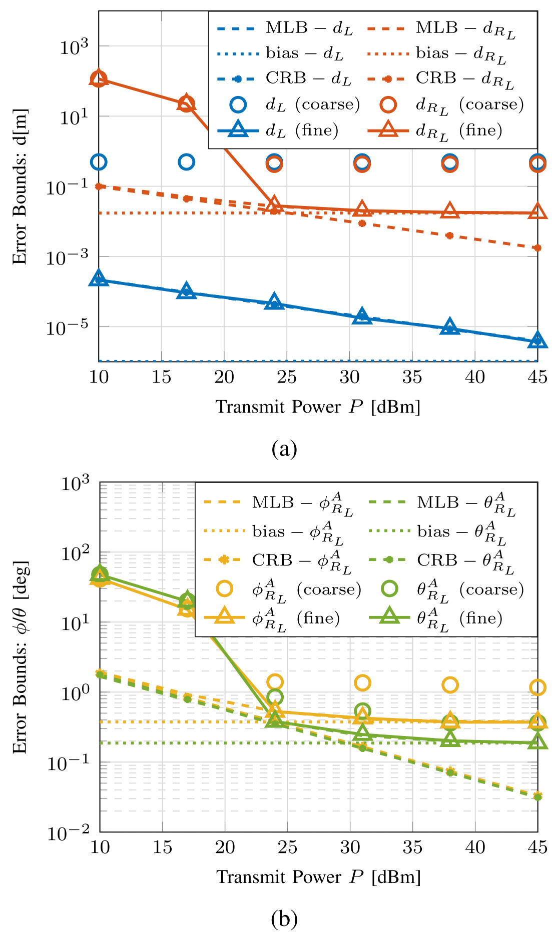


Fig. 3. Theoretical bounds and estimation results for channel parameters: (a) delay estimates for the LOS and legitimate RIS paths (d_L and d_{R_L}); (b) AOA estimates for the legitimate RIS path ($\phi^A_{R_L}$ and $\theta^A_{R_L}$). Displayed metrics include the CRB, MLB, bias term, and RMSE for both coarse and fine estimations. The legitimate RIS employs the TO-RPC scheme, while the unauthorized RIS uses the RPC scheme.

and short wavelength, which enable high delay resolution and large array apertures. In addition, RIS is particularly useful at mmWave frequencies, where signals are more vulnerable to blockage, thereby enhancing positioning robustness. A total of $K = 512$ subcarriers are utilized as pilot signals for positioning. The transmitted symbol vector $\mathbf{x}$ consists of random unit-modulus signals, where each element has a unit amplitude and a phase uniformly distributed in the range $[0, 2\pi)$. Unless stated otherwise, the legitimate RIS employs TO-RPC.

A. Bounds and Estimation Results

For the low-complexity estimation, the resolution of the grid search for ϕ and θ in (45) is set to 1.6°. The search area around the true UE position, as mentioned in (45), is defined as a $2\times2\times2$ m^3 space with a step size of 0.2 m in each of the three dimensions. Fig. 3 shows derived bounds and the RMSE of the estimation results for channel parameter estimation in terms of d_L, d_{R_L}, $\phi^A_{R_L}$ and $\theta^A_{R_L}$. The coarse estimation represents the results obtained from the low-complexity estimation process, while the fine results refer to the estimations refined through MLE. The CRBs of the interference-free model, the MLBs

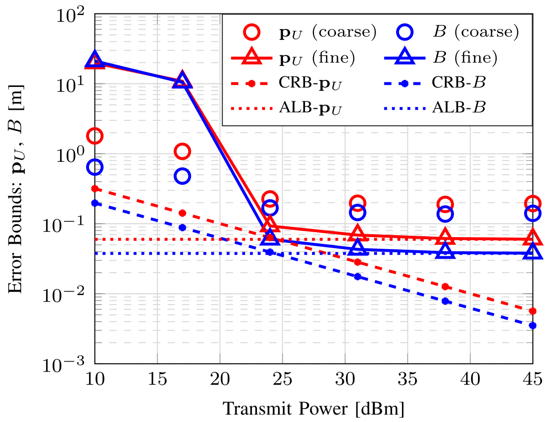


Fig. 4. Theoretical bounds and estimation results for the state parameters $\mathbf{p}_U$ and B. Displayed metrics include the CRB, MLB, bias term, and RMSE for both coarse and fine estimations. The legitimate RIS employs the TO-RPC scheme, while the unauthorized RIS uses the RPC scheme.

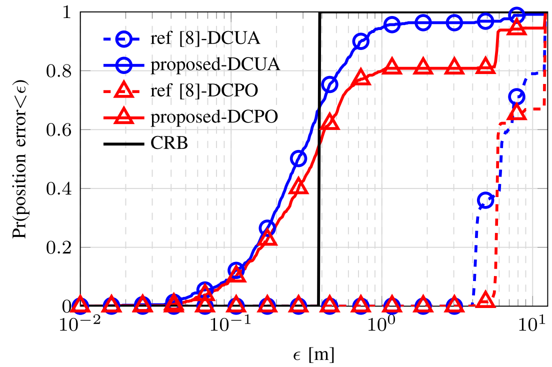


Fig. 5. CDF comparison of the UE position estimation error for different positioning algorithms, with the unauthorized RIS employing DCUA and DCPO (P = 30 dBm).

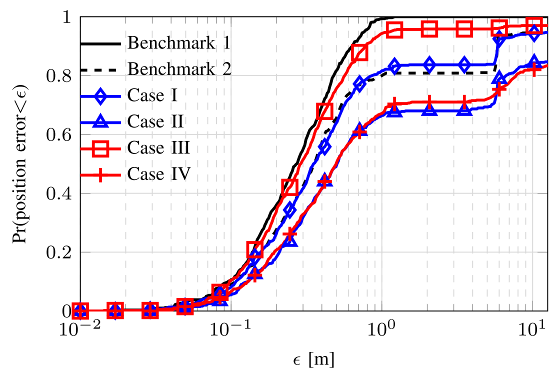


Fig. 6. Evaluation of multipath effects on the estimator in terms of CDF, with the unauthorized RIS employing the DCPO beamforming codebook (P = 30 dBm). Benchmark 1 represents the case without interference or MPCs, while Benchmark 2 only considers interference. Cases I and II include both interference and MPCs, with RCS values of 0.5 m^2 and 1 m^2, respectively. Cases III and IV consider only the effect of MPCs, using the same RCS values as Cases I and II.

as well as the bias of the corresponding MLBs serve as the benchmarks for estimators. As the transmit power increases, the MCRB term decreases with SNR, whereas the bias term remains unchanged. As shown in Figs. 3 and 4, the proposed mismatched MLE approaches the MLB as the transmit power P increases, and eventually converges to the error floor induced by the corresponding bias term when P is sufficiently large.

Specifically, the delay result for the LOS path is particularly different from the other parameters. The CRB and MLB for this parameter are nearly identical, with the bias of its MLB being less than 10^{-6} m, which can be considered negligible. This indicates that the presence of an unauthorized RIS has a minimal impact on the LOS path, as the LOS path is considerably stronger than the path associated with the unauthorized RIS. For the delay of the legitimate RIS path, the difference between its MLB and the CRB becomes apparent when the transmit power exceeds 25 dBm, as the MLB gradually converges toward the bias term. The coarse estimation result saturates at a level higher than the MLB, whereas the refined estimation result aligns with the MLB when the transmit power exceeds 24 dBm.

The bounds and estimation results for the AOA of the legitimate RIS path are shown in Fig. 3 (b). A similar trend can be observed for the bounds of ϕ and θ, while the bias for ϕ is slightly larger than that for θ at this specific location. It can be inferred that the unauthorized RIS has minimal impact on the performance of the estimators when the transmit power is low, as the performance is primarily limited by noise effects at this stage. However, as the transmit power increases, the bias term of the MLB becomes dominant, ultimately setting the lower bound on performance. Moreover, with varying relative positions of the legitimate RIS and the unauthorized RIS, interference from the unauthorized RIS can have different impacts on the legitimate RIS path, leading to relatively higher or lower MLB and bias values in terms of delay and AOA. The results in Fig. 3 demonstrate the effectiveness of the positioning algorithms and the derived bounds.

The derived bounds and the RMSE of the estimation results for UE position and clock offset estimation, i.e., $\mathbf{p}_U$ and B are detailed in Fig. 4. The CRB bounds (dashed lines with circle markers) represent the theoretical lower bounds for positioning accuracy in the absence of an unauthorized RIS. The ALBs for the UE position and clock offset correspond to the bias terms of the MLBs when interference from an unauthorized RIS is present, as discussed in Section IV-C. At low transmit power levels, the coarse estimation results exhibit smaller estimation errors compared to the refined estimation results. This occurs because the grid search used in coarse estimation is confined to a $2 \times 2 \times 2\,\mathrm{m}^3$ region, providing a constrained search space that improves robustness under low transmit power conditions. In contrast, the optimization process in refined estimation is not restricted to this area, making its advantages less evident at lower power levels. However, as the transmit power increases beyond 24 dBm, the refined estimation results for the state parameters converge toward the ALBs, which ultimately serve as their lower bound.

As mentioned in Section V-A, the use of DCUA and DCPO could introduce challenges in estimating the legitimate RIS path parameters. Using the algorithm proposed in [6] may select the peak caused by the unauthorized RIS (as shown

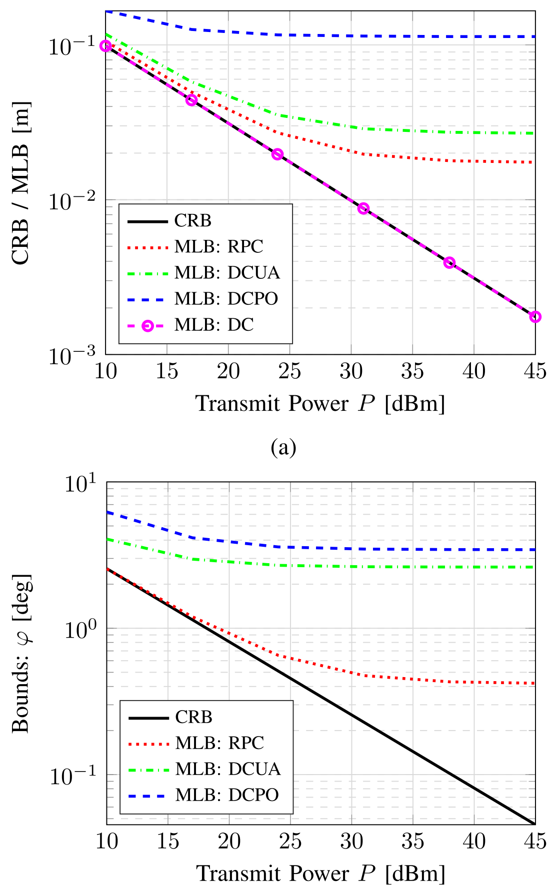


Fig. 7. CRB and MLB results with different unauthorized RIS beamforming codebooks for estimation of (a) the delay: d_{R_L} and (b) AOA: $\boldsymbol{\varphi}^A_{R_L}$ of the legitimate RIS path, respectively. The bounds for AOA are calculated based on the root mean square of the values of $\phi^A_{R_L}$ and $\theta^A_{R_L}$ for simplicity. The legitimate RIS employs the TO-RPC scheme.

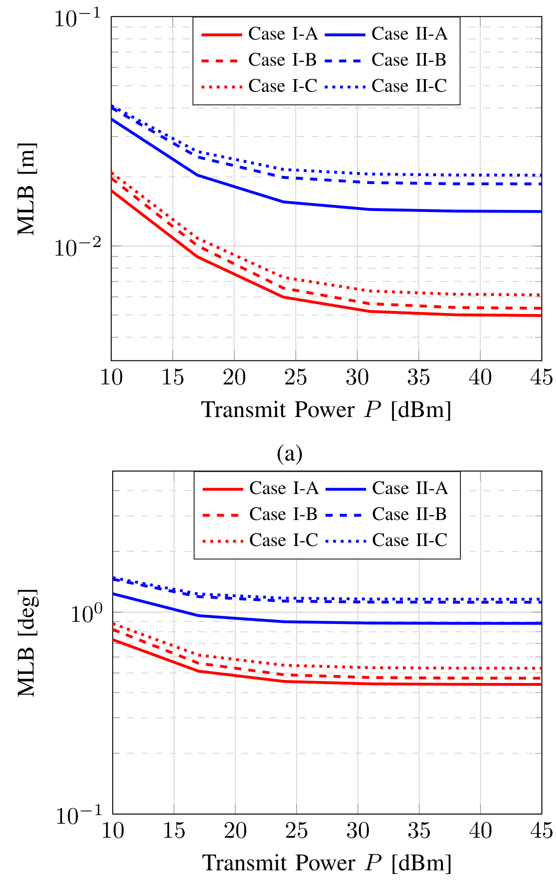


Fig. 8. MLB results for estimating the legitimate RIS path parameters: (a) equivalent propagation distance d_{R_L} and (b) AOA $\boldsymbol{\varphi}_{R_L}$. The legitimate RIS uses TO-DCUA, while the unauthorized RIS uses DCUA in Case I and DCPO in Case II. Phase-control settings are: A) continuous/continuous, B) 2-bit/3-bit, and C) 2-bit/4-bit for the legitimate/unauthorized RISs, respectively.

in Fig. 2) and produce large errors in RIS path channel estimation. The CDF results of RMSE in terms of $\mathbf{p}_U$ using the algorithm in [6] and the proposed one are compared in Fig. 5 to evaluate the estimator performance when the unauthorized RIS employs DCPO. The CDF of CRB here is considered as the result without interference. As observed, the proposed algorithm can achieve much better positioning performance than the method in the literature when DCUA or DCPO is used for unauthorized RIS. It can also be observed that the unauthorized RIS using DCPO creates a more adverse condition compared to DCUA, as it is more likely to result in higher positioning estimation errors.

B. The Effect of MPCs

We further examine the impact of the presence of MPCs. We assume two clusters located near the BS and UE, as propagation channels in outdoor LOS FR2 scenarios are typically dominated by a strong LOS path and only a few scattering clusters [41], [49], [50]. The impact of MPCs originating far from the BS or UE is negligible due to the high path loss. It is worth noting that the MPCs considered here do not contribute to the positioning task, as the surrounding environments of the BS and UE are generally uncontrollable and the precise locations of the scatterers are typically unknown in practice. For the first cluster, the three SPs are randomly distributed within a 1-meter radius sphere centered at $[1,1,2]^\top$ (closer to the BS), while the three SPs of the second cluster are randomly distributed within a 1-meter radius sphere centered at $[-1,3,1]^\top$ (closer to the UE). Each cluster contains three SPs, resulting in three single-bounce MPCs, six legitimate RIS-associated MPCs, and six unauthorized RIS-associated MPCs. Therefore, a total of 30 MPCs are considered for the two clusters. The channel gains of the UE-SP-BS, UE-legitimate RIS-SP-BS, and UE-unauthorized RIS-SP-BS paths are defined, respectively, as $|\alpha_{L,m}| = \frac{\sqrt{4\pi c_{L,i}}\,\lambda_c}{16\pi^2 d_{U,i} d_{B,i}}$, $|\alpha_{R_L,m}| = \frac{\sqrt{4\pi c_{R_L,i}}\,\lambda_c^2}{64\pi^3 d_{B,i} d_{R_L,i} d_{R_L,U}}$, and $|\alpha_{R_U,m}| = \frac{\sqrt{4\pi c_{R_U,i}}\,\lambda_c^2}{64\pi^3 d_{B,i} d_{R_U,i} d_{R_U,U}}$, where $c_{L,i}$, $c_{R_L,i}$, and $c_{R_U,i}$ denote the RCS coefficients of the i-th SP for the corresponding paths, respectively. All MPCs are assigned identical RCS coefficients, and the transmit power is set to 30 dBm.

Comparisons of the impacts caused by MPCs, interference, and their combined effects are presented in Fig. 6. The cumulative distribution function (CDF) results are obtained from 600 independent realizations. When the radar cross

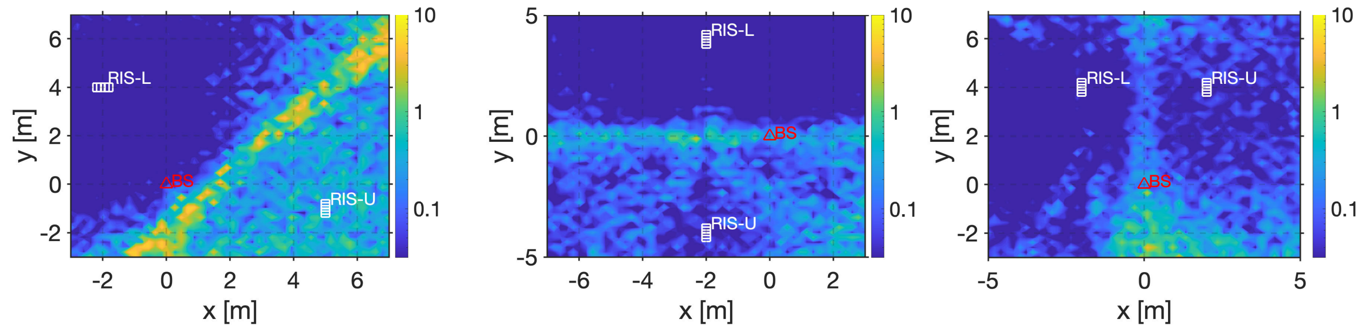


Fig. 9. Visualization of $\mathrm{ALB}_{\mathrm{pos}}$ for different UE locations within a 10×10 m^2 area, with the BS fixed at $[0,0,0]^\top$. Two RISs are positioned on the same plane as the BS, 2 m above the UE. Three scenarios are considered, with results shown in (a), (b), and (c), respectively: Scenario 1 involves two RISs perpendicular to each other; Scenario 2 involves two RISs aligned along the same line facing the same direction; and Scenario 3 involves two RISs aligned along the same line but facing each other. The legitimate and unauthorized RISs employ TO-RPC and DCUA, respectively.

section (RCS) value is set to 0.5 m^2, the influence of MPCs is limited, as indicated by the similarity of the CDF curve to that of the baseline scenario. It is also observed that positioning performance in the presence of both interference and MPCs (with a RCS of 0.5 m^2) is much worse than in the scenario with only MPCs. These results suggest that, at lower RCS values, performance degradation is primarily driven by interference from the unauthorized RIS. As the RCS increases from 0.5 m^2 to 1 m^2, the impact of MPCs becomes more pronounced, resulting in degraded positioning performance compared to the scenario with interference alone. Comparing the CDF results for the scenarios with both interference and MPCs to those with only MPCs (at a RCS of 1 m^2), no significant difference is observed. This suggests that, at higher RCS values, the influence of MPCs outweighs that of the unauthorized RIS.

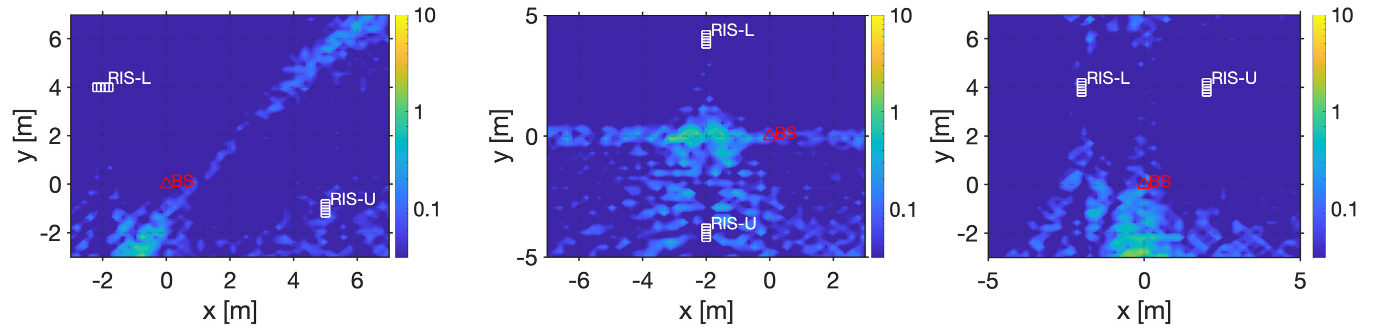
C. The Effect of Beamforming Codebook

In this subsection, we consider the effects of using different beamforming codebooks as well as the discrete phase control for both legitimate RIS and unauthorized RIS. The default simulation settings are provided in Table II. Since the adversary is generally assumed to possess knowledge comparable to or greater than that of the legitimate system, when legitimate RIS employs TO-RPC scheme, RPC, DCUA, and DCPO are considered at unauthorized RIS side. When the legitimate RIS employs TO-DCUA scheme, DCUA and DCPO are considered at the unauthorized RIS side. For both TO-DCUA and DCUA schemes, the AOA deviations in (17) are set as $\Delta\phi_g \sim \mathcal{U}[-10^\circ, 10^\circ]$ and $\Delta\theta_g \sim \mathcal{U}[-5^\circ, 5^\circ]$.

We first consider the case where the legitimate RIS employs the TO-RPC scheme, while the unauthorized RIS adopts different beamforming strategies. The CRB and MLB for estimating the delay of the legitimate RIS path, d_{R_L}, and the AOA, $\boldsymbol{\varphi}^A_{R_L}$, are compared in Fig. 7.[5] The CRB results provide a benchmark for performance in the absence of an unauthorized RIS. It is observed that the MLB obtained with DC aligns with the CRB, indicating unsuccessful interference. The DC, detailed in (27), remains unchanged as g varies. Consequently, the legitimate RIS path could effectively be separated from the received signals as $[\mathbf{Y}_{R_U}]_{:,k} = [\mathbf{Y}_{R_U}]_{:,k+\frac{G}{2}}$. As a result, the positioning system experiences negligible interference from the unauthorized RIS. Besides, it can be observed that, at low transmit power, the MLB and CRB exhibit minimal differences when a random beamforming codebook is used, indicating a negligible impact from the unauthorized RIS in this case. However, for the two directional codebooks, higher MLB values are observed across all legitimate RIS channel parameters compared to those obtained with the RPC. This indicates that employing DCUA or DCPO on the unauthorized RIS can generate stronger interference compared to using RPC. When comparing the results for the two directional codebooks, a higher MLB is observed when using DCPO for legitimate RIS path parameters. This indicates that DCPO induces stronger and more effective interference compared to DCUA.

Fig. 8 presents the MLB results for estimating the channel parameters of the legitimate RIS when the TO-DCUA scheme is applied at the legitimate RIS. The effects of using discrete phase states at both the legitimate RIS and unauthorized RIS sides are also depicted. For the discrete phase control, two quantization levels are evaluated: 2-bit and 3-bit, corresponding to $Q = 4$ and $Q = 8$, respectively. The results obtained when both the legitimate and unauthorized RISs use continuous phase values are included as benchmarks. It can be observed that the MLBs increase when the unauthorized RIS has a higher phase resolution (i.e., more discrete phase states) than the legitimate RIS. Moreover, the unauthorized RIS employing the DCPO scheme introduces stronger interference compared with the DCUA scheme. Compared with Fig. 7, where the legitimate RIS uses the TO-RPC codebook, the MLB results in Fig. 8 (for unauthorized RIS configurations using DCUA and DCPO) are substantially lower. This is expected, as the signals received at the BS from the legitimate RIS are statistically stronger when TO-DCUA is used instead of TO-RPC. Consequently, the interference produced by the unauthorized RIS under the same beamforming strategies becomes less effective, resulting in lower MLB values.

[5] The bounds for $\boldsymbol{\varphi}$ are obtained by taking the square root of the sum of the results for ϕ and θ.



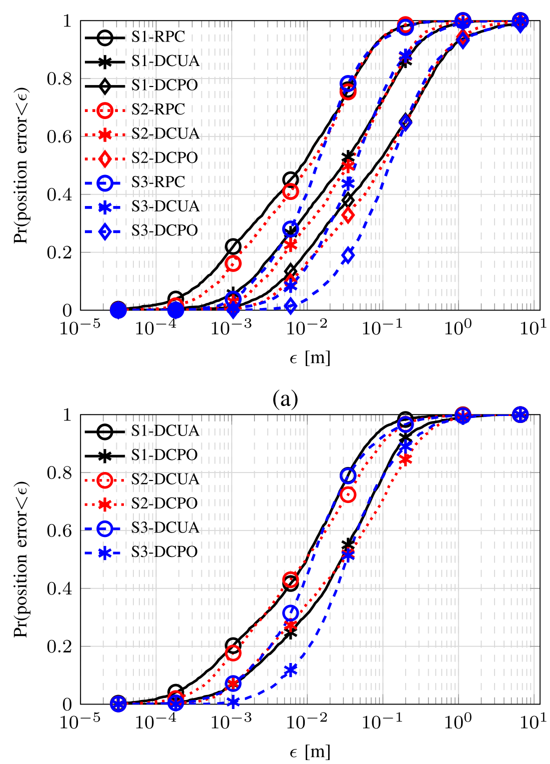
(a)-Scenario 1 (b)-Scenario 2 (c)-Scenario 3

Fig. 10. Visualization of ALB_{pos} for different UE locations within a 10×10 m^2 area, with the BS fixed at $[0,0,0]^\top$. Two RISs are positioned on the same plane as the BS, 2 m above the UE. Three scenarios are considered, with results shown in (a), (b), and (c), respectively: Scenario 1 involves two RISs perpendicular to each other; Scenario 2 involves two RISs aligned along the same line facing the same direction; and Scenario 3 involves two RISs aligned along the same line but facing each other. The legitimate and unauthorized RISs employ TO-DCUA and DCUA, respectively.

D. The ALB With Different UE Locations

The positioning performance and the interference impact are highly dependent on the specific system configuration, i.e., the relative locations of the BS, UE, and RISs. As discussed in Section IV-C, the ALB of the UE position can serve as a benchmark to evaluate the positioning capacity. In this subsection, we focus on three typical system configurations with random UE locations to investigate the positioning capability by calculating the ALB for UE position estimation within a 10×10 m^2. The BS is fixed at $[0,0,0]^\top$ and the UE is placed in an unknown position in the $z = -2$ plane. The specific locations of the legitimate RIS and unauthorized RIS for the three scenarios are: (a) Scenario 1: Two RISs are perpendicular to each other with $\mathbf{p}_{R_L} = [-2,4,0]^\top$, $\mathbf{p}_{R_U} = [5,-1,0]^\top$; (b) Scenario 2: Two RISs are aligned along the same line and face the same direction with $\mathbf{p}_{R_L} = [-2,4,0]^\top$, $\mathbf{p}_{R_U} = [-2,-4,0]^\top$; (c) Scenario 3: Two RISs are aligned along the same line and face each other with $\mathbf{p}_{R_L} = [-2,4,0]^\top$, $\mathbf{p}_{R_U} = [2,4,0]^\top$. The results for three typical scenarios when legitimate and unauthorized RISs employ TO-RPC and DCUA are illustrated in Fig. 9. By carefully analyzing the light-colored areas (which denote a higher ALB and poorer positioning performance) across the three scenarios, it becomes evident that UE positions resulting in a shorter unauthorized RIS path and a longer legitimate RIS path tend to have higher ALB. This is because the unauthorized RIS path exhibits a higher power level compared to the legitimate path, leading to stronger interference. Moreover, a clearly visible strip-shaped region can be observed in each scenario (particularly noticeable in the results using directional codebooks). These highlighted strip areas are caused by the close link distances of the legitimate RIS and unauthorized RIS paths. The poor positioning capability in these areas is not due to stronger signals from the unauthorized RIS. Instead, it is primarily attributed to ambiguity in the channel parameter optimization process with the mismatched MLE, caused by similar path delays. Identical or nearly identical delays in the RIS path make it less likely to achieve a clear and sharp global optimum for the cost function.

In addition, the angle-resolving capability of a RIS plate diminishes when the incident angle is parallel to its plane.



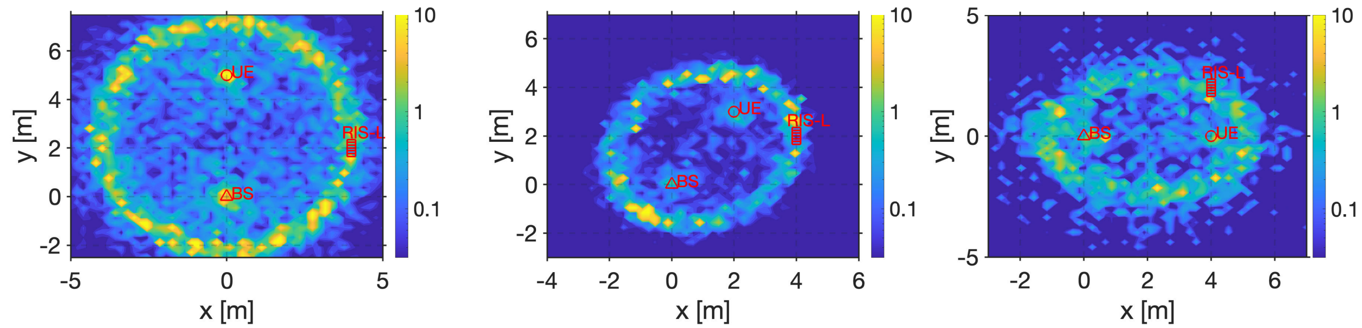
(a)

(b)

Fig. 11. The CDF results of ALB_{pos} under different unauthorized RIS beamforming schemes are shown for the three typical scenarios, where the legitimate RIS employs (a) TO-RPC and (b) TO-DCUA, respectively.

UE locations that result in large incident angles (relative to the local coordinate system of the legitimate RIS) and similar RIS path delay to that of the unauthorized RIS path at the same time are more likely to exhibit the highest ALB within the calculated area.

The results for three typical scenarios when legitimate and unauthorized RISs employ TO-DCUA and DCUA are illustrated in Fig. 10. Compared with Fig. 9, the ALB exhibits an overall reduction, in agreement with the results presented in Fig. 7 and Fig. 8. For the results considering other beamforming scheme pairs for both RISs across the



(a) (b) (c)

Fig. 12. Visualization of ALB_{pos} for different locations of an unauthorized RIS within a 10×10 m^2 area, with the BS and legitimate RIS fixed at $[0, 0, 0]^\top$ and $[4, 2, 0]^\top$, respectively. Three different UE locations are considered: (a) UE and BS are vertically aligned; (b) BS and UE are aligned along a hypotenuse; (c) UE and BS are horizontally aligned. The legitimate and unauthorized RISs employ the TO-RPC and DCPO, respectively.

three scenarios, the CDFs of the ALB are summarized in Fig. 11, providing an alternative perspective on the positioning performance. It is evident that the unauthorized RIS using the DCPO scheme yields the strongest interference, as it can accurately direct the reflected beam toward the BS. Comparing the CDF curves in Fig. 11(a) and Fig. 11(b), we observe that the positioning performance with TO-RPC versus RPC for the legitimate and unauthorized RISs is similar to that with TO-DCUA versus DCUA, since the received signal powers from both the legitimate and unauthorized RISs remain at comparable levels in each case. As observed, the CDF results for Scenarios 1 and 2 exhibit similar trends. In Scenario 3, the curves for all beamforming codebooks rise more slowly in the low-error region compared with the other scenarios, although they still converge as the error approaches 1 m. It is also worth noting that the positioning error obtained using directional codebooks (i.e., DCUA and DCPO) may exceed the limit of $\sqrt{2 \times 2 \times 2}$ m, since the ALB is based on an MLE-driven optimization that does not restrict the search space to a bounded region as in coarse estimation. Although not all possible system configurations are examined, useful insights can be drawn from the analysis of the three representative scenarios. Based on the ALB results, it can be concluded that, regardless of the specific system arrangement, regions where the unauthorized RIS path is shorter and the legitimate RIS path is longer tend to exhibit higher ALB values. Moreover, areas where the link distances of the legitimate and unauthorized RIS paths are comparable lead to even poorer positioning performance.

E. The ALB With Different Locations of Unauthorized RIS

Given that the original RIS-aided positioning system has fixed locations for the legitimate RIS, BS, and UE, an interesting aspect to explore is how to strategically position the unauthorized RIS to generate intense interference. In the following, we calculate the ALB for three different scenarios as the location of unauthorized RIS changes within a 10×10 m^2 area. Note that RISs, BS, and UE are positioned at the same height to facilitate an easier analysis of the underlying principles. The legitimate and unauthorized RISs employ the TO-RPC and DCPO, respectively. The BS and legitimate RIS are fixed at $[0, 0, 0]^\top$ and $[4, 2, 0]^\top$, respectively and the UE locations for three scenarios are: (a) Scenario 1: UE and BS are vertically aligned with $\mathbf{p}_U = [0, 5, 0]^\top$; (b) Scenario 2: UE and BS are aligned along a hypotenuse with $\mathbf{p}_U = [2, 3, 0]^\top$; (c) Scenario 3: UE and BS are horizontally aligned with $\mathbf{p}_U = [4, 0, 0]^\top$. The visualization of the positioning error as the unauthorized RIS changes its location is presented in Fig. 12. Only the results with the legitimate RIS and unauthorized RIS using TO-RPC and DCPO are provided, as similar patterns are observed when using other beamforming schemes.

For all scenarios, a highlighted elliptical ring is clearly observed, indicating that more effective interference can be generated if the unauthorized RIS is positioned along this elliptical ring. To further investigate the relationship between the observed ellipse and the system configuration, a general rule can be established: the observed elliptical ring aligns with an ellipse where the BS and the UE serve as the focal points, and the link distance of the legitimate RIS path corresponds to the major axis length of the ellipse. As shown in Fig. 12, the orientation and size of the ellipse change based on the UE's location and the corresponding link distance of the legitimate RIS path. This observation is reasonable when considering the results from Fig. 9. Positioning the unauthorized RIS near the aforementioned ellipse results in similar link distances for both the legitimate RIS path and the unauthorized RIS path. As discussed in Section VI-D, this similarity leads to poor positioning performance due to increased ambiguity in parameter estimation. Moreover, a higher ALB can also be observed when the unauthorized RIS is positioned close to either the BS or the UE, thereby introducing a high-power unauthorized RIS path. If the agent aims to degrade the positioning performance of two or more UEs, the optimal location for the unauthorized RIS would be at the intersections or overlapping areas of the ellipses corresponding to the different UEs. The above discussions could also be useful for designing mitigation strategies against unexpected interference.

F. Impact of Frequency Band and RIS Hardware Parameters

System settings such as carrier frequency and bandwidth influence the performance of the original positioning system.

Different carrier frequencies result in different path-loss characteristics, which in turn affect the SNR; the impact of SNR variations on the lower bounds has already been examined in our analysis. The choice of bandwidth determines the delay resolution, and a smaller bandwidth leads to a more challenging scenario in which the legitimate RIS and unauthorized RIS paths become harder to separate. Beyond waveform parameters, RIS configurations also affect interference behavior. However, RIS dimensions and element spacing are largely hardware-defined parameters, giving both legitimate and unauthorized parties less flexibility than in beamforming design. Although the corresponding simulation results are not shown here due to space limitations, we observe that interference from an unauthorized RIS becomes more detrimental as its physical aperture increases, particularly when using beamforming strategies that concentrate energy toward the BS (e.g., DCUA and DCPO). Furthermore, different element spacings modify the reflected beamwidth, influencing the likelihood of aligning the unauthorized RIS beam with the BS under DCUA, while having negligible impact on schemes such as RPC and DCPO.

VII. Conclusion

This paper investigates RIS-aided positioning in the presence of interference from an unauthorized RIS. We formulate the system models as well as the threat model. Theoretical analysis and numerical simulations are performed to assess the impact of unauthorized RIS interference on both channel estimation and positioning performance, and to validate the derived bounds and algorithms. The results show that unauthorized RIS interference causes positioning errors to saturate at high SNR due to attack-induced model mismatch. Severe errors arise when the unauthorized RIS path is strong or delay-aligned with the legitimate RIS path, revealing a structural vulnerability of the positioning system. These qualitative trends hold across different attack models, while the degradation level depends strongly on the attacker's system knowledge. In particular, better-informed attackers can induce substantially larger errors by using directional beams, whereas less informed attacks typically cause milder degradation. Future work may focus on extending to multi-user scenarios, developing effective countermeasures through advanced beamforming techniques at the BS, and enhancing the robustness of positioning algorithms to improve the reliability of RIS-aided positioning systems.

References

[1] F. Liu et al., "Integrated sensing and communications: Toward dual-functional wireless networks for 6G and beyond," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 6, pp. 1728–1767, Jun. 2022.

[2] A. Behravan et al., "Positioning and sensing in 6G: Gaps, challenges, and opportunities," *IEEE Veh. Technol. Mag.*, vol. 18, no. 1, pp. 40–48, Mar. 2023.

[3] S. Dwivedi et al., "Positioning in 5G networks," *IEEE Commun. Mag.*, vol. 59, no. 11, pp. 38–44, Nov. 2021.

[4] K. Gao, H. Wang, H. Lv, and W. Liu, "Localization-oriented digital twinning in 6G: A new indoor-positioning paradigm and proof-of-concept," *IEEE Trans. Wireless Commun.*, vol. 23, no. 8, pp. 10473–10486, Aug. 2024.

[5] C. Pan et al., "An overview of signal processing techniques for RIS/IRS-aided wireless systems," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 5, pp. 883–917, Aug. 2022.

[6] H. Chen, P. Zheng, M. F. Keskin, T. Y. Al-Naffouri, and H. Wymeersch, "Multi-RIS-enabled 3D sidelink positioning," *IEEE Trans. Wireless Commun.*, vol. 23, no. 8, pp. 8700–8716, Aug. 2024.

[7] K. Keykhosravi et al., "Leveraging RIS-enabled smart signal propagation for solving infeasible localization problems: Scenarios, key research directions, and open challenges," *IEEE Veh. Technol. Mag.*, vol. 18, no. 2, pp. 20–28, Jun. 2023.

[8] Y. Ma, K. Ota, and M. Dong, "Multi-RIS deployment location optimization for coverage enhancement in outdoor wireless communication networks," *IEEE Trans. Veh. Technol.*, vol. 73, no. 10, pp. 15332–15344, Oct. 2024.

[9] H. Chen et al., "6G localization and sensing in the near field: Features, opportunities, and challenges," *IEEE Wireless Commun.*, vol. 31, no. 4, pp. 260–267, Aug. 2024.

[10] P. Zheng, X. Liu, and T. Y. Al-Naffouri, "LEO- and RIS-empowered user tracking: A Riemannian manifold approach," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 12, pp. 3445–3461, Dec. 2024.

[11] H. Qiu, S. Gong, H. Liu, X. Zhao, and C. Xing, "Active-passive beamforming optimization for RIS-aided mmWave joint localization and communication system," *IEEE Trans. Veh. Technol.*, vol. 74, no. 2, pp. 2941–2957, Feb. 2025.

[12] M. Raeisi et al., "Efficient localization with base station-integrated beyond diagonal RIS," 2024, *arXiv:2411.13295*.

[13] R. Whiton, "Cellular localization for autonomous driving: A function pull approach to safety-critical wireless localization," *IEEE Veh. Technol. Mag.*, vol. 17, no. 4, pp. 28–37, Dec. 2022.

[14] W. Dai, Y. Shen, and M. Z. Win, "Distributed power allocation for cooperative wireless network localization," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 1, pp. 28–40, Jan. 2015.

[15] R. Ghazalian et al., "Calibration in RIS-aided integrated sensing, localization and communication systems," 2024, *arXiv:2409.16931*.

[16] Y. Ge et al., "Experimental validation of single BS 5G mmWave positioning and mapping for intelligent transport," *IEEE Trans. Veh. Technol.*, vol. 73, no. 11, pp. 16744–16757, Nov. 2024.

[17] H. Chen et al., "Modeling and analysis of OFDM-based 5G/6G localization under hardware impairments," *IEEE Trans. Wireless Commun.*, vol. 23, no. 7, pp. 7319–7333, Jul. 2023.

[18] P. Zheng et al., "Misspecified Cramér-Rao bound of RIS-aided localization under geometry mismatch," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Jun. 2023, pp. 1–5.

[19] P. Zheng, H. Chen, T. Ballal, M. Valkama, H. Wymeersch, and T. Y. Al-Naffouri, "JrCUP: Joint RIS calibration and user positioning for 6G wireless systems," *IEEE Trans. Wireless Commun.*, vol. 23, no. 6, pp. 6683–6698, Jun. 2024.

[20] J. Zhang, X. Hu, and C. Zhong, "Phase calibration for intelligent reflecting surfaces assisted millimeter wave communications," *IEEE Trans. Signal Process.*, vol. 70, pp. 1026–1040, 2022.

[21] C. Ozturk, M. F. Keskin, V. Sciancalepore, H. Wymeersch, and S. Gezici, "RIS-aided localization under pixel failures," *IEEE Trans. Wireless Commun.*, vol. 23, no. 8, pp. 8314–8329, Aug. 2024.

[22] C. Goztepe, S. Büyükçorak, G. K. Kurt, and H. Yanikomeroglu, "Localization threats in next-generation wireless networks," *IEEE Commun. Mag.*, vol. 59, no. 9, pp. 51–57, Sep. 2021.

[23] S. Gezici, M. R. Gholami, S. Bayram, and M. Jansson, "Jamming of wireless localization systems," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2660–2676, Jun. 2016.

[24] Y. Zhang et al., "Privacy preservation in delay-based localization systems: Artificial noise or artificial multipath?" in *Proc. IEEE Glob. Comm. Conf.*, Dec. 2024, pp. 2755–2760.

[25] P. Huang, E. Gönültaş, M. Arnold, K. P. Srinath, J. Hoydis, and C. Studer, "Attacking and defending deep-learning-based off-device wireless positioning systems," *IEEE Trans. Wireless Commun.*, vol. 23, no. 8, pp. 8883–8895, Aug. 2024.

[26] J. Zhang, X. Wang, R. S. Blum, and L. M. Kaplan, "Attack detection in sensor network target localization systems with quantized data," *IEEE Trans. Signal Process.*, vol. 66, no. 8, pp. 2070–2085, Apr. 2018.

[27] G. Michieletto, F. Formaggio, A. Cenedese, and S. Tomasin, "Robust localization for secure navigation of UAV formations under GNSS spoofing attack," *IEEE Trans. Autom. Sci. Eng.*, vol. 20, no. 4, pp. 2383–2396, Oct. 2023.

[28] K. Gao, H. Wang, H. Lv, and P. Gao, "Your locations may be lies: Selective-PRS-spoofing attacks and defence on 5G NR positioning systems," in *Proc. IEEE Conf. Comput. Commun.*, May 2023, pp. 1–10.

[29] Y. Zhang et al., "Privacy preservation in MIMO-OFDM localization systems: A beamforming approach," *IEEE Wireless Commun. Lett.*, vol. 14, no. 7, pp. 1979–1983, Jul. 2025.

[30] A. Pourafzal et al., "Cooperative impersonation in angle-based physical layer authentication," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2025, pp. 3321–3326.

[31] G. Focarelli, S. Zanini, I. Palamà, G. Bianchi, and S. Bartoletti, "Positioning security in 5G and beyond: Model and detection of physical layer threats," *IEEE Trans. Wireless Commun.*, vol. 25, pp. 1048–1061, 2025.

[32] L. Italiano et al., "HoloTrace: A location privacy preservation solution for mmWave MIMO-OFDM systems," 2025, *arXiv:2509.23444*.

[33] J. Li and U. Mitra, "Channel state information-free location-privacy enhancement: Fake path injection," *IEEE Trans. Signal Process.*, vol. 72, pp. 3745–3760, 2024.

[34] J. Li and U. Mitra, "Channel state information-free location-privacy enhancement: Delay-angle information spoofing," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2024, pp. 3767–3772.

[35] E. C. Strinati et al., "Reconfigurable, intelligent, and sustainable wireless environments for 6G smart connectivity," *IEEE Commun. Mag.*, vol. 59, no. 10, pp. 99–105, Oct. 2021.

[36] H. Alakoca et al., "Metasurface manipulation attacks: Potential security threats of RIS-aided 6G communications," *IEEE Commun. Mag.*, vol. 61, no. 1, pp. 24–30, Jan. 2023.

[37] S. Rivetti et al., "Destructive and constructive RIS beamforming in an ISAC-multi-user MIMO network," 2024, *arXiv:2404.11314*.

[38] K. Keykhosravi, M. F. Keskin, G. Seco-Granados, P. Popovski, and H. Wymeersch, "RIS-enabled SISO localization under user mobility and spatial-wideband effects," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 5, pp. 1125–1140, Aug. 2022.

[39] K. Keykhosravi, M. F. Keskin, G. Seco-Granados, and H. Wymeersch, "SISO RIS-enabled joint 3D downlink localization and synchronization," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2021, pp. 1–6.

[40] K. Keykhosravi, G. Seco-Granados, G. C. Alexandropoulos, and H. Wymeersch, "RIS-enabled self-localization: Leveraging controllable reflections with zero access points," in *Proc. IEEE Int. Conf. Commun.*, May 2022, pp. 2852–2857.

[41] T. S. Rappaport, G. R. MacCartney, M. K. Samimi, and S. Sun, "Wideband millimeter-wave propagation measurements and channel models for future wireless communication system design," *IEEE Trans. Commun.*, vol. 63, no. 9, pp. 3029–3056, Sep. 2015.

[42] A. M. Nor, O. Fratu, and S. Halunga, "Codebook based RIS passive beamforming solutions: A survey," in *Proc. Adv. Topics Meas. Simul. (ATOMS)*, Aug. 2024, pp. 295–298.

[43] J. An, C. Xu, L. Gan, and L. Hanzo, "Low-complexity channel estimation and passive beamforming for RIS-assisted MIMO systems relying on discrete phase shifts," *IEEE Trans. Commun.*, vol. 70, no. 2, pp. 1245–1260, Feb. 2022.

[44] M. Mizmizi, D. Tagliaferri, and U. Spagnolini, "Wireless communications with space–time modulated metasurfaces," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 6, pp. 1534–1548, Jun. 2024.

[45] M. Najafi, V. Jamali, R. Schober, and H. V. Poor, "Physics-based modeling and scalable optimization of large intelligent reflecting surfaces," *IEEE Trans. Commun.*, vol. 69, no. 4, pp. 2673–2691, Apr. 2021.

[46] S. Fortunati, F. Gini, M. S. Greco, and C. D. Richmond, "Performance bounds for parameter estimation under misspecified models: Fundamental findings and applications," *IEEE Signal Process. Mag.*, vol. 34, no. 6, pp. 142–157, Nov. 2017.

[47] C. D. Richmond and L. L. Horowitz, "Parameter bounds on estimation accuracy under model misspecification," *IEEE Trans. Signal Process.*, vol. 63, no. 9, pp. 2263–2278, May 2015.

[48] C. Ozturk, M. F. Keskin, H. Wymeersch, and S. Gezici, "RIS-aided near-field localization under phase-dependent amplitude variations," *IEEE Trans. Wireless Commun.*, vol. 22, no. 8, pp. 5550–5566, Aug. 2023.

[49] T. S. Rappaport et al., "Millimeter wave mobile communications for 5G cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, 2013.

[50] M. K. Samimi and T. S. Rappaport, "3-D millimeter-wave statistical channel model for 5G wireless system design," *IEEE Trans. Microw. Theory Techn.*, vol. 64, no. 7, pp. 2207–2225, Jul. 2016.