Cooperative ISAC Under Spoofing Attacks

Usman Ali, Nicola Blefari Melazzi, and Stefania Bartoletti, *Member, IEEE*

***Abstract*—Recent studies have demonstrated the vulnerability of integrated sensing and communication (ISAC) systems to jamming and spoofing attacks, particularly in scenarios involving single radar systems. However, cooperation among networked sensors can enhance localization accuracy and mitigate such attacks by exploiting spatial consistency. This letter develops a theoretical framework based on the mismatched Cramér-Rao lower bound (MCRLB) to quantify the impact of spoofing on localization performance within cooperative ISAC networks. We examine how varying attack intensities and deployment configurations influence system resilience. Our analysis reveals that cooperative processing significantly reduces localization errors, highlighting the robustness of distributed sensing architectures against adversarial interference.**

***Index Terms*—Joint communication and sensing, cooperative sensing, spoofing, Cramér-Rao bound.**

I. Introduction

INTEGRATED sensing and communication (ISAC) is a key enabler for 6G networks, allowing infrastructure to support both wireless communication and radar-like environmental awareness [1], [2], [3]. Recent studies demonstrated that ISAC systems are exposed to adversarial threats, particularly spoofing attacks that distort target localization by manipulating the received signal [4], [5].

Cooperative sensing using multi-monostatic multiple-input multiple-output (MIMO) configurations enhances resilience by exploiting spatial diversity. In this setting, multiple gNodeBs (gNBs) jointly perform sensing. Since spoofers typically affect one node at a time, unaffected gNBs can cross-validate observations, helping to suppress spoofed signals and maintain localization integrity [6], [7], [8]. It is worth noting that practical implementations of cooperative sensing inherently involve increased computational complexity due to the processing and fusion of measurements from multiple nodes, as commonly discussed in the cooperative sensing literature [9], [10]. Data exchange and fusion in cooperative systems can also introduce processing delays, with the accuracy–latency trade-off strongly influenced by the chosen fusion methodology; although this is beyond the scope of this letter, the reader may refer to [9], [10] for further discussion.

The Cramér-Rao lower bound (CRLB) is widely used to evaluate the performance of localization systems under ideal (non-adversarial) conditions. However, it does not account for estimation bias introduced by spoofing. To address this limitation, we adopt the mismatched CRLB (MCRLB) framework, which accounts for the divergence between the true (attacked) and assumed observation models.

While prior work has explored MCRLB in the context of hardware impairments, such as reconfigurable intelligent surfaces (RIS) calibration errors and phase noise [11]–its application to spoofing attacks remains largely unexplored. This letter fills that gap with the following contributions:

- We propose an MCRLB-based framework to quantify the impact of spoofing attacks on target localization accuracy.
- We analyze localization errors under varying transmit power levels and bias conditions.
- We incorporate the geometrical configuration of gNBs into our framework and show that cooperative sensing across multiple gNB deployments effectively mitigates spoofing by enhancing spatial diversity.

By evaluating different gNB configurations and spoofing attack scenarios, we assess the resilience of cooperative sensing networks against adversarial manipulation.

II. System Model

The system model is a dual-function MIMO architecture where each gNB performs both communication and monostatic radar sensing using co-located transmit and receive arrays. We first describe the baseline setup without spoofing, then extend the model to include spoofing attacks.

A. Baseline System Model

Consider a scenario involving N_{gNB} gNBs, where n-th gNB is equipped with N_{t} transmitting antennas positioned at $(x_{\mathrm{t}}^{(n)}, y_{\mathrm{t}}^{(n)})$, and N_{r} receiving antennas at $(x_{\mathrm{r}}^{(n)}, y_{\mathrm{r}}^{(n)})$, where $N_{\mathrm{t}} < N_{\mathrm{r}}$. Both transmitting and receiving antennas are co-located at the same gNB, i.e., in monostatic configuration, hence $x_{\mathrm{t}}^{(n)} = x_{\mathrm{r}}^{(n)}$ and $y_{\mathrm{t}}^{(n)} = y_{\mathrm{r}}^{(n)}$.

Let $\mathbf{X}_{\mathrm{n}} = \mathbf{w}^{(n)}\mathbf{s}_{\mathrm{c}}^{H} \in \mathbb{C}^{N_{\mathrm{t}} \times T_{\mathrm{n}}}$ be the radar-communication signal transmitted by the n-th gNB, where $\mathbf{w}^{(n)} \in \mathbb{C}^{N_{\mathrm{t}} \times 1}$ is the beamforming vector and $\mathbf{s}_{\mathrm{c}}^{(n)} \in \mathbb{C}^{T_{\mathrm{n}} \times 1}$ represents the transmitted data stream with $T_{\mathrm{n}} > N_{\mathrm{t}}$ being the length of the radar pulse or communication frame. The beamforming vector is defined as $\mathbf{w}^{(n)} = \sqrt{P(1-\rho)}\mathbf{w}_n^{(c)} + \sqrt{P\rho}\mathbf{w}_n^{(s)}$ with $\rho \in (0, 1]$ is the power allocation coefficient, i.e., the fraction of total power allocated to communication and sensing. Here $\mathbf{w}_n^{(s)}$ and $\mathbf{w}_n^{(c)}$ are the beamforming vectors for sensing and

Received 26 April 2025; accepted 25 May 2025. Date of publication 3 June 2025; date of current version 11 September 2025. This work was supported in part by the European Research Council (ERC) under the European Union's Horizon Europe under Grant 101078411; in part by the project SERICS under the NRRP MUR program funded by the EU—NGEU under Grant PE00000014; and in part by the European Union—Next Generation EU under the Italian National Recovery and Resilience Plan (NRRP), Mission 4, Component 2, Investment 1.3, CUP F83C22001690001, E83C22004640001, partnership on "Telecommunications of the Future" under Grant PE00000001—program "RESTART". The associate editor coordinating the review of this article and approving it for publication was G. Brante. *(Corresponding author: Usman Ali.)*

The authors are with the Department of Electronics Engineering and CNIT, University of Rome Tor Vergata, 00139 Rome, Italy (e-mail: usman.ali@uniroma2.it).

Digital Object Identifier 10.1109/LWC.2025.3576194

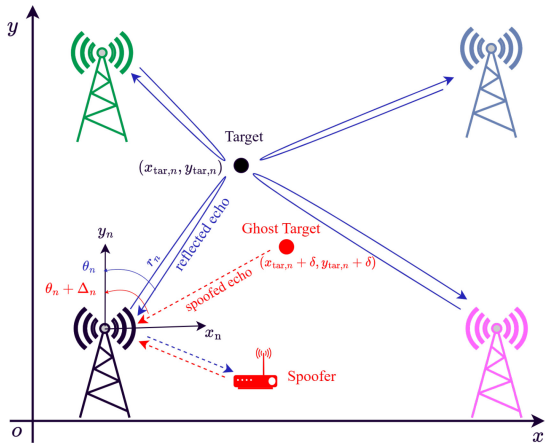

Fig. 1. Example scenario of cooperative monostatic ISAC network with $N_{\mathrm{gNB}} = 4$ gNBs in the presence of a spoofing attack against the bottom left gNB.

communication, respectively. The transmit power at the gNB is constrained by P, such that $\mathbb{E}[\|\mathbf{X}_{\mathrm{n}}\|^2] \leq P$. In this letter, we focus exclusively on the sensing part, following the ISAC system model as defined in [8].

As illustrated in Figure 1, the azimuth angle of the radar echo, denoted by θ_n, is the relative angle between the n-th gNB and the target; r_n be the distance between the n-th gNB and the target. The coordinates of the target can be expressed as $(r_n \sin(\theta_n), r_n \cos(\theta_n))$.

By transmitting $\mathbf{X}_n$, the reflected echo signal at the n-th gNB is given by

$$\mathbf{y}_n = \alpha_n \mathbf{A}(\theta_n)\mathbf{X}_n + \mathbf{z}_n \tag{1}$$

with $\mathbf{A}(\theta_n) \triangleq \mathbf{b}(\theta_n)\mathbf{a}^{\mathrm{H}}(\theta_n)$, where α_n, $\mathbf{a}(\theta_n) \in \mathbb{C}^{N_{\mathrm{t}}}$ and $\mathbf{b}(\theta_n) \in \mathbb{C}^{N_{\mathrm{r}}}$ are reflection coefficient, steering vectors of the transmit and receive antennas, respectively; $\mathbf{z}_n$ is the noise vector component and is modeled as Additive White Gaussian Noise (AWGN) with $\mathcal{CN}(0, \sigma_n^2)$. The amplitude of the reflected signal at the n-th gNB, denoted by α_n, is affected by both the radar cross-section (RCS), represented by ζ_n, and the round-trip path loss. For free space propagation, the amplitude $|\alpha_n|^2$ can be modeled as $|\alpha_n|^2 = \sigma_n^2 r_n^{-4}$ with $\sigma_n^2 = \frac{\zeta_n \lambda^2}{(4\pi)^3}$ where λ is the wavelength of the transmitted signal. In monostatic sensing, self-interference is assumed negligible, and only the round-trip path between the gNB and target is considered.

In the case of uniform linear array (ULA) antennas with half-wavelength spacing, $\mathbf{a}(\theta_n)$ and $\mathbf{b}(\theta_n)$ vectors can be expressed as in [7]

$$\mathbf{a}(\theta_n) = \left[e^{-j\frac{N_{\mathrm{t}}-1}{2}\pi\sin(\theta_{\mathrm{n}})}, e^{-j\frac{N_{\mathrm{t}}-3}{2}\pi\sin(\theta_{\mathrm{n}})}, \ldots, e^{j\frac{N_{\mathrm{t}}-1}{2}\pi\sin(\theta_{\mathrm{n}})}\right]^T, \tag{2}$$

and $\mathbf{b}(\theta_n)$ equal to $\mathbf{a}(\theta_n)$ where N_{r} replacing N_{t}.

We consider all gNBs synchronized and connected to a central entity for coordinated sensing and data fusion. Synchronization errors between gNBs are inherent in practical systems and can affect both localization accuracy and spoofing detection. While synchronization offsets are not explicitly modeled here, they can be incorporated as biases in range or delay measurements. For further details on CRLB under synchronization uncertainty, see, e.g., [12].

B. System Model Under Spoofing Attack

Spoofing attacks in ISAC occur when an adversary manipulates signals to create a false target location at $(x_{\mathrm{tar},n} + \delta, y_{\mathrm{tar},n} + \delta)$, causing the receiver to track a ghost target, as shown in Figure 1. Recent studies demonstrated two main threat models for spoofing attacks. In [4], the attacker amplifies the signal power to mask the legitimate target, leading to missed detections. In [5], the attacker manipulates signal timing and carrier frequency, causing the receiver to lock onto the spoofed signal, corrupting the real target's detection.

This letter considers a replay attack in which the adversary reflects a received sensing signal with a controlled delay to simulate a ghost target, resembling a high-gain reflection. This allows the spoofed signal to be received by the legitimate gNB without the need for the attacker to synthesize a fake signal, as in [5]. Extending (1), the received signal at the n-th gNB under a spoofing attack can be expressed as:

$$\mathbf{y}_n = \alpha_n \mathbf{A}(\theta_n)\mathbf{X}_n + G_n \alpha_n \mathbf{A}(\theta_n + \Delta_n)\mathbf{X}_n + \mathbf{z}_n \tag{3}$$

where the first term represents the legitimate signal component from the legitimate target, and the second term represents the spoofed signal component from the ghost target. Here, G_n is an amplitude scaling factor introduced by the attacker, which makes the spoofed signal stronger than the legitimate one, and Δ_n represents the angular bias induced by the attacker.

Multipath propagation is not modeled, as our focus is on analyzing the impact of the spoofer. Nevertheless, beamforming, as shown in prior ISAC studies, can reduce fading effects by enabling single-path observations within narrow beams [7]. For analyses that account for multipath effects, we refer the reader to existing works, e.g., [13].

Therefore, in this letter, we focus on the impact of spoofing-induced ghost targets under line-of-sight propagation conditions and with static targets, isolating their effect on localization accuracy.[1]

III. CRB for Cooperative Sensing

In a cooperative ISAC network, the target coordinates $(x_{\mathrm{tar}}, y_{\mathrm{tar}})$ are mapped from the global reference system to the local reference system of each gNB in receive mode. The transformation ν_n:$(x_{\mathrm{tar}}, y_{\mathrm{tar}}) \rightarrow (x_{\mathrm{tar},n}, y_{\mathrm{tar},n})$ for the n-th gNB depends on the orientation of gNB antenna array ϑ_n between the local and global y-axes. The coordinates are [7]

$$x_{\mathrm{tar},n} = -\left(x_{\mathrm{tar}} - x_{\mathrm{r}}^{(n)}\right)\cos(\vartheta_n) - \left(y_{\mathrm{tar}} - y_{\mathrm{r}}^{(n)}\right)\sin(\vartheta_n), \tag{4}$$

$$y_{\mathrm{tar},n} = -\left(x_{\mathrm{tar}} - x_{\mathrm{r}}^{(n)}\right)\sin(\vartheta_n) + \left(y_{\mathrm{tar}} - y_{\mathrm{r}}^{(n)}\right)\cos(\vartheta_n). \tag{5}$$

The Jacobian matrix for this transformation, $\mathbf{J}_{\nu_n}$, is

$$\mathbf{J}_{\nu_n} = \begin{bmatrix} -\cos(\vartheta_n) & -\sin(\vartheta_n) \\ -\sin(\vartheta_n) & \cos(\vartheta_n) \end{bmatrix}. \tag{6}$$

We consider a scenario where one of the N gNBs receives a spoofed signal, while the remaining $N-1$ gNBs receive

[1]Doppler effects are not considered here, as velocity estimation is outside the scope of our static model, but extending the framework to dynamic scenarios is a future research direction.

legitimate signals. Without loss of generality, we assume gNB 1 receives the spoofed signal. Given that a single gNB is under a spoofing attack, and assuming a cooperative sensing system with joint detection, we consider that the system identifies a single target and utilizes all available measurements to estimate its location. In this cooperative setup, where all gNBs collaborate to localize the target, the Fisher information matrix (FIM) for the target position (x, y) is obtained by summing the appropriately transformed FIMs contributed by each individual gNB, as in [8]

$$\mathbf{F}(x, y) = \sum_{n=1}^{N} \mathbf{J}_{\nu_n}^T \mathbf{F}\big(x_{\text{tar},n}, y_{\text{tar},n}\big)\mathbf{J}_{\nu_n}, \tag{7}$$

where $\mathbf{F}(x_{\text{tar},n}, y_{\text{tar},n})$ is the FIM related to the estimation in the local reference frame of the n-th gNB. Then the CRLB is

$$\text{CRLB} = \text{tr}\left(\left(\sum_{n=1}^{N} \mathbf{J}_{\nu_n}^T \mathbf{F}\big(x_{\text{tar},n}, y_{\text{tar},n}\big)\mathbf{J}_{\nu_n}\right)^{-1}\right). \tag{8}$$

We apply the MCRLB framework for the spoofed gNB, which we will define in Section III-B, while the standard CRLB is used for the other $N-1$ gNBs. The resulting lower bound (LB) is then given by

$$\text{LB} = \left(\text{MCRLB}^{(1)} + \sum_{n=2}^{N} \text{CRLB}^{(n)}\right)^{(1/2)}. \tag{9}$$

where $\text{MCRLB}^{(1)}$ and $\text{CRLB}^{(n)}$ are computed using (19) and (8), respectively. In the absence of spoofing, $\text{MCRLB}^{(1)}$ reduces to $\text{CRLB}^{(1)}$.

If a spoofing detection mechanism is in place and the receiver can detect spoofing using techniques like the Minimum Description Length (MDL) criterion [14], the problem reduces to standard estimation governed by the classical CRLB. MDL methods estimate the number of sources from the covariance matrix, enabling detection of anomalies due to spoofing. In such cases, adaptive suppression techniques can be applied. However, this letter focuses on the more realistic worst-case scenario where spoofing remains undetected, justifying the use of the MCRLB to assess the resulting estimation bias and performance degradation.

A. CRLB Without Spoofing Attacks

In this section, we assume that the n-th gNB does not have any spoofing effect, i.e., $\mathbf{y}_n$ is given by (1). We define a channel parameter vector as $\boldsymbol{\psi}^{(n)} = [\alpha_n, \theta_n]$. The deterministic CRLB for unbiased estimation of the channel parameters at the n-th gNB, $\hat{\boldsymbol{\psi}}^{(n)} = [\alpha_n, \theta_n]$, can be expressed as $\mathbf{F}^{-1}$, where $\mathbf{F}$ represents the FIM and is defined as [11]

$$[\mathbf{F}(\alpha_n, \theta_n)]_{\text{i,j}} = \frac{1}{\sigma_n^2} \Re\left\{ \frac{\partial \boldsymbol{\mu}_n^{\text{H}}}{\partial \boldsymbol{\psi}_i^{(n)}} \frac{\partial \boldsymbol{\mu}_n}{\partial \boldsymbol{\psi}_j^{(n)}} \right\} \tag{10}$$

with $\boldsymbol{\mu}^{(n)} = \alpha_n \mathbf{A}(\theta_n)\mathbf{X}_n$ being the mean of $\mathbf{y}_n$ at the n-th gNB. The FIM in Cartesian coordinates can be obtained as [8]

$$\mathbf{F}\big(x_{\text{tar},n}, y_{\text{tar},n}\big) = \mathbf{J}_n^T \mathbf{F}(\alpha_n, \theta_n)\mathbf{J}_n, \tag{11}$$

where $\mathbf{J}_n$ is the Jacobian matrix of the transformation from polar to Cartesian coordinates. By substituting (11) into (8), the CRLB can be obtained.

B. MCRLB Under Spoofing Attacks

In this section, we assume that a spoofing attack affects the received signal at the n-th gNB, i.e., $\mathbf{y}_n$ is given by (3). The radar processing relies on (1), i.e., it does not account for spoofing effects. Using the MCRLB framework, we quantify the impact of this mismatch on the accuracy of channel parameter estimation, highlighting the performance degradation caused by model misspecification.

1) True and Assumed Models for Radar Observation: The true observation model incorporates the presence of bias in channel parameters due to spoofing attacks, representing the actual behavior of the received signal. Rewriting (3), gives,

$$\bar{\mathbf{y}}_n = \hat{\alpha}_n \mathbf{b}\Big(\hat{\theta}_n\Big)\mathbf{a}^{\text{H}}\Big(\hat{\theta}_n\Big)\mathbf{X}_n + \bar{\alpha}_n \mathbf{b}(\bar{\theta}_n)\mathbf{a}^{\text{H}}(\bar{\theta}_n)\mathbf{X}_n + \mathbf{z}_n \tag{12}$$

where $\hat{\alpha}_n$ and $\hat{\theta}_n$ are the true amplitude and true angle of the legitimate signal, respectively, and $\boldsymbol{\psi}_0^{(n)} = [\hat{\alpha}_n, \hat{\theta}_n]$ is a vector of true channel parameters at the n-th gNB. While $\bar{\alpha}_n = G_n \alpha_n$, and $\bar{\theta}_n = \theta_n + \Delta_n$ are the amplitude and angle of spoofed signal, introduced by the attacker. The probability density function (pdf) of the true observation model $\bar{\mathbf{y}}_n$ in (12) is given by

$$g(\bar{\mathbf{y}}_n) = \frac{1}{\pi {\sigma_n}^2} e^{-\frac{1}{\sigma_n^2}\left\|\bar{\mathbf{y}}_n - \boldsymbol{\mu}_T^{(n)}\right\|^2}, \tag{13}$$

where $\boldsymbol{\mu}_T^{(n)} = \hat{\alpha}_n \mathbf{b}(\hat{\theta}_n)\mathbf{a}^{\text{H}}(\hat{\theta}_n)\mathbf{X}_n + \bar{\alpha}_n \mathbf{b}(\bar{\theta}_n)\mathbf{a}^{\text{H}}(\bar{\theta}_n)\mathbf{X}_n$ represents the true mean signal.

In contrast to the true model, the assumed model disregards the spoofing effect; the assumed observation model for $\mathbf{y_n}$ in (1) is given by

$$g\Big(\mathbf{y}_n \mid \boldsymbol{\psi}^{(n)}\Big) = \frac{1}{\pi {\sigma_n}^2} e^{-\frac{1}{\sigma_n^2}\left\|\mathbf{y}_n - \boldsymbol{\mu}_M^{(n)}(\psi^{(n)})\right\|^2}, \tag{14}$$

where $\boldsymbol{\mu}_M^{(n)}(\psi^{(n)}) = \alpha_n \mathbf{b}(\theta_n)\mathbf{a}^{\text{H}}(\theta_n)\mathbf{X}_n$, and $\boldsymbol{\psi}^{(n)} = [\alpha_n, \theta_n]$ is a vector of unknown channel parameters at the n-th gNB.

2) Pseudo-True Parameter: The pseudo-true parameter, used to analyze model misspecification in Section III-B3, is defined as the parameter that minimizes the Kullback-Leibler (KL) divergence between the true pdf and the assumed pdf

$$\boldsymbol{\psi}_A^{(n)} = \arg\min_{\boldsymbol{\psi}^{(n)}} \mathcal{D}\big(g(\bar{\mathbf{y}}_n) \| g\Big(\mathbf{y}_n \mid \boldsymbol{\psi}^{(n)}\Big), \tag{15}$$

Using the equivalence provided in the [15], we have

$$\boldsymbol{\psi}_A^{(n)} = \arg\min_{\boldsymbol{\psi}^{(n)}} \|\boldsymbol{\mu}_T^{(n)} - \boldsymbol{\mu}_M^{(n)}\Big(\boldsymbol{\psi}^{(n)}\Big)\|^2. \tag{16}$$

For pseudo-true parameters $\boldsymbol{\psi}_A^{(n)} = [\alpha_A^{(n)}, \theta_A^{(n)}]$, we get

$$\Big(\alpha_A^{(n)}, \theta_A^{(n)}\Big) = \arg\min_{\alpha_n, \theta_n} \|\boldsymbol{\mu}_T^{(n)} - \alpha_n \boldsymbol{q}^{(n)}(\theta_n)\|^2 \tag{17}$$

where $\boldsymbol{q}^{(n)}(\theta_n) = \mathbf{b}(\theta_n)\mathbf{a}^{\text{H}}(\theta_n)\mathbf{X}_n$. From (17), $\alpha_A^{(n)}$ is obtained as $\alpha_A^{(n)} = \boldsymbol{q}^{(n)}(\theta_n)^{\dagger}\boldsymbol{\mu}_T^{(n)}$, where $\dagger$ is pseudo inverse of $\boldsymbol{q}^{(n)}(\theta_n)$. By putting $\alpha_A^{(n)}$ back in (17), we have [11]

$$\theta_A^{(n)} = \arg\max_{\theta_n} |\boldsymbol{q}^{(n)}(\theta_n)^H \boldsymbol{\mu}_T^{(n)}|^2 \tag{18}$$

3) MCRLB Derivation: The MCRLB quantifies the minimum achievable variance of unbiased parameter estimators under a misspecified model. The true data pdf in (13) is generally inaccessible, so estimation algorithms rely on the misspecified model in (14). The MCRLB can be computed as [11]

$$\text{MCRLB} = \underbrace{\left(\boldsymbol{\psi}_0^{(n)} - \boldsymbol{\psi}_A^{(n)}\right)\left(\boldsymbol{\psi}_0^{(n)} - \boldsymbol{\psi}_A^{(n)}\right)^T}_{\text{Bias}} + \mathbf{A}^{-1}\left(\boldsymbol{\psi}_A^{(n)}\right)\mathbf{B}\left(\boldsymbol{\psi}_A^{(n)}\right)\mathbf{A}^{-1}\left(\boldsymbol{\psi}_A^{(n)}\right), \quad (19)$$

where the first term $(\boldsymbol{\psi}_0^{(n)} - \boldsymbol{\psi}_A^{(n)})(\boldsymbol{\psi}_0^{(n)} - \boldsymbol{\psi}_A^{(n)})^T$ is a bias term, whereas $\mathbf{A}$ and $\mathbf{B}$ in the second term are

$$\mathbf{A}_{ij}\left(\boldsymbol{\psi}_A^{(n)}\right) = \mathbb{E}_{g(\bar{\mathbf{y}}_n)}\left[\left.\frac{\partial^2 \ln g\left(\mathbf{y}_n \mid \boldsymbol{\psi}^{(n)}\right)}{\partial \boldsymbol{\psi}_i^{(n)}\, \partial \boldsymbol{\psi}_j^{(n)}}\right|_{\boldsymbol{\psi}^{(n)}=\boldsymbol{\psi}_A^{(n)}}\right],$$

$$\mathbf{B}_{ij}\left(\boldsymbol{\psi}_A^{(n)}\right) = \mathbb{E}_{g(\bar{\mathbf{y}}_n)}\left[\left.\frac{\partial \ln g\left(\mathbf{y}_n \mid \boldsymbol{\psi}^{(n)}\right)}{\partial \boldsymbol{\psi}_i^{(n)}}\frac{\partial \ln g\left(\mathbf{y}_n \mid \boldsymbol{\psi}^{(n)}\right)}{\partial \boldsymbol{\psi}_j^{(n)}}\right|_{\boldsymbol{\psi}^{(n)}=\boldsymbol{\psi}_A^{(n)}}\right]$$

with $\mathbb{E}_{g(\bar{\mathbf{y}}_n)}\{\cdot\}$ indicating the expectation over the true pdf in (13), the terms $\mathbf{A}_{ij}(\boldsymbol{\psi}_A^{(n)})$ and $\mathbf{B}_{ij}(\boldsymbol{\psi}_A^{(n)})$ are derived as described in [16].

IV. Numerical Results

In this section, we evaluate the ISAC network with four monostatic gNBs, which utilize ULAs for antenna arrays located at the corners of a 100-meter square. The target is positioned randomly in the square. The number of transmit antennas (N_{t}) is 16, and the number of receive antennas (N_{r}) is 20. The carrier frequency (f_{c}) is set to 28 GHz, and the number of transmit symbols (T) is 32. The receiver noise power for sensing (σ_n^2) is –103 dBm, and the target radar cross-section (ζ) is 1 m^2. For the observations in (1), the data symbols $\mathbf{X}$ are drawn randomly from the QPSK alphabet, and $\mathbf{w}_n^{(s)} = \frac{\mathbf{a}(\theta_A^{(n)})}{\|\mathbf{a}(\theta_A^{(n)})\|}$ where n is the index of a gNB. Moving counterclockwise from the gNB in the lower-left corner, the following orientation angles are used for each gNB: $\vartheta = \{\frac{\pi}{4}, \pi - \frac{\pi}{4}, \pi + \frac{\pi}{4}, -\frac{\pi}{4}\}$. Our simulations assume 60% power allocation to sensing $(\rho = 0.6)$. In a practical ISAC system, lower sensing power may degrade localization accuracy due to reduced signal strength.[2] Note that coordinated multi-spoofer scenarios are possible in principle, though they are significantly more complex and less common in practice due to the need for precise synchronization among distributed attackers.

To assess the impact of cooperative sensing, we evaluate localization performance under different gNB configurations: (i) four gNBs with no attack, serving as a benchmark; (ii) a single gNB under attack; (iii) two gNBs with one under attack; (iv) three gNBs enhancing spatial diversity with one under attack; and (v) four gNBs with one under attack.

Figure 2 shows LB for target localization as a function of transmit power P, with angular bias $\Delta = 35^\circ$ and amplitude scaling factor $G = 2$ in the spoofed signal received at gNB1. For $N_{\text{gNB}} = 1$, at low power, noise is the primary error source, and the bias term in (19) has little effect. As P increases, noise effects reduce, and the bias term dominates, causing MCRLB to saturate, reflecting the performance limit due to model mismatch. In cooperative setups $(N_{\text{gNB}} \geq 3)$, the system remains resilient, with stable performance that approaches the non-spoofing case.

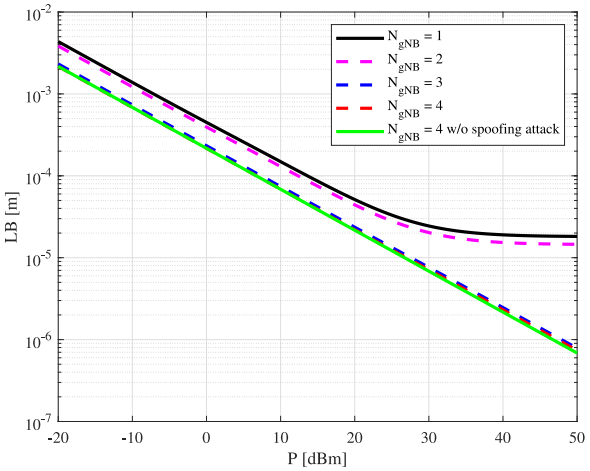

Fig. 2. LB as a function of transmit power (P) by fixing $\Delta = 35^\circ$, $G = 2$, and $\rho = 0.6$.

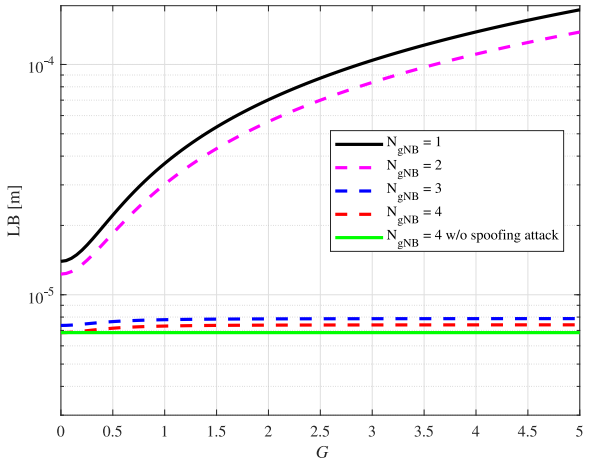

Fig. 3. LB as a function of G by fixing $\Delta = 0^\circ$, $P = 30$ dBm and $\rho = 0.6$.

Figure 3 shows the impact of G on localization accuracy with fixed $\Delta = 0^\circ$. At small G, LB is low, indicating no spoofing. However, as G increases slightly, LB rises, demonstrating that even weak spoofed signals can cause errors when perfectly aligned with the legitimate signal. This sharp rise continues with increasing G, highlighting the system's sensitivity to spoofing. In contrast, multi-gNB systems show greater robustness due to spatial diversity.

Figure 4 examines the effect of G with $\Delta = 35^\circ$. In the low-G region $(G \in [0-1])$, LB remains low. In the moderate-G region $(1 - 3)$, LB increases for single- and two-gNB systems due to combined amplitude and angular biases. In the high-G region $(G > 3)$, single and two-gNB setups show high LB, while multi-gNB systems remain resilient. Spatial

[2]For example, the LB with N_{gNB}=1 goes from 2.410^{-5} m with $\rho = 0.6$ to 2.2×10^{-5} m with $\rho = 1$ (for $P = 30$ dBm). This changes with N_{gNB}=4, where it goes from 6.7×10^{-6} m with $\rho = 0.6$ to 5×10^{-6} m with $\rho = 1$.

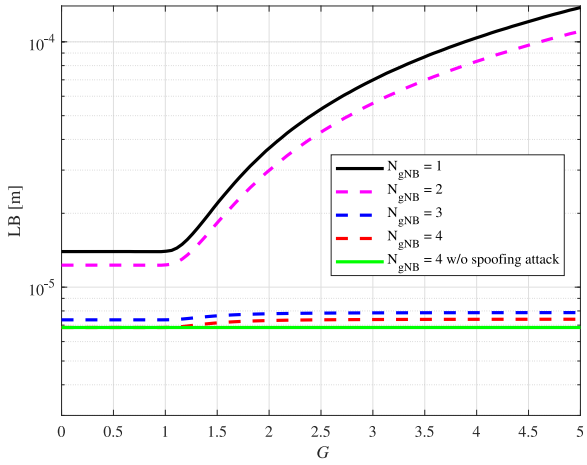

Fig. 4. LB as a function of G by fixing $\Delta = 35°$, $P = 30$ dBm and $\rho = 0.6$.

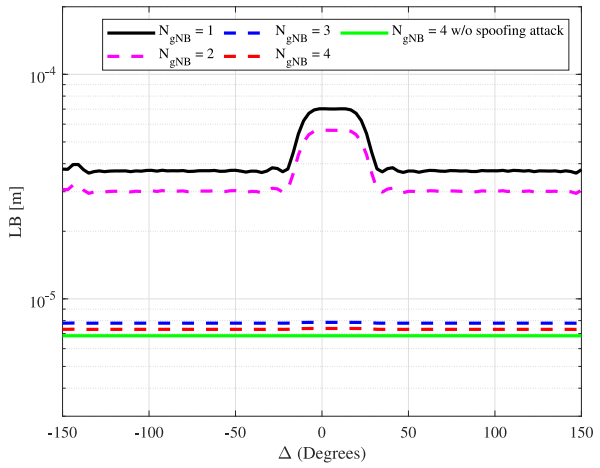

Fig. 5. LB as a function of Δ by fixing $G = 2$, $P = 30$ dBm and $\rho = 0.6$.

diversity effectively mitigates directional inconsistencies, with $N_{\text{gNB}} = 4$ achieving the lowest LB.

Figure 5 shows LB versus angular bias Δ with $G = 20$, $P = 30$ dBm, and $\rho = 0.6$. The peak near $\Delta = 0°$ indicates the worst-case spoofing scenario, where the spoofed signal's power and lack of angular separation cause maximum interference. Any angular deviation allows multi-gNB systems to regain robustness, highlighting the importance of angular diversity in spoofing detection.

V. Final Remarks

This letter proposed a framework to assess localization accuracy in cooperative ISAC networks under spoofing attacks. Results show that multi-gNB configurations enhance robustness by exploiting spatial diversity. While this letter focuses on fundamental performance limits through Fisher Information analysis, the derived bounds offer valuable insights for the design of hybrid spoofing mitigation strategies. For example, machine learning approaches, such as anomaly detection or deep learning classifiers, could incorporate spatial consistency metrics, as analyzed here, as informative features to enhance spoofing detection. Future research may further investigate these promising synergies between model-driven theoretical limits and data-driven detection techniques.

References

[1] "Study on integrated sensing and communication; release 19," 3GPP, Sophia Antipolis, France, Rep. 22.837, Jun. 2024.

[2] S. Bartoletti et al., "Integration of sensing and localization in V2X sidelink communications," *IEEE Commun. Mag.*, vol. 62, no. 8, pp. 185–191, Aug. 2024.

[3] A. Liu et al., "A survey on fundamental limits of integrated sensing and communication," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 994–1034, 2nd Quart. 2022.

[4] G. Chrysanidis, Y. Liu, and A. Argyriou, "A replay attack against ISAC based on OFDM," *IEEE Access*, vol. 12, pp. 20998–21003, 2024.

[5] H. C. Yildirim, M. F. Keskin, H. Wymeersch, and F. Horlin, "OFDM-based JCAS under attack: The dual threat of spoofing and jamming in WLAN sensing," *IEEE Internet Things J.*, vol. 12, no. 10, pp. 14511–14525, May 2025.

[6] M. R. Figueroa, P. K. Bishoyi, and M. Petrova, "Cooperative multi-monostatic sensing for object localization in 6G networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2024, pp. 1–6.

[7] L. Pucci and A. Giorgetti, "Position error bound for cooperative sensing in MIMO-OFDM networks," in *Proc. IEEE 25th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, 2024, pp. 296–300.

[8] F. Zabini, E. Paolini, W. Xu, and A. Giorgetti, "Fundamental limits of cooperative strategies in joint sensing and communication networks," in *Proc. IEEE ICC Workshops*, 2024, pp. 329–334.

[9] M. Manzoni et al., "Wavefield networked sensing: Principles, algorithms and applications," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 181–197, 2025.

[10] D. Tagliaferri et al., "Cooperative coherent multistatic imaging and phase synchronization in networked sensing," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 10, pp. 2905–2921, Oct. 2024.

[11] M. F. Keskin, C. Marcus, O. Eriksson, H. Wymeersch, and V. Koivunen, "On the impact of phase noise on monostatic sensing in OFDM ISAC systems," in *Proc. IEEE Radar Conf. (RadarConf)*. 2023, pp. 1–6.

[12] R. M. Vaghefi and R. M. Buehrer, "Cooperative joint synchronization and localization in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 63, no. 14, pp. 3615–3627, Jul. 2015.

[13] S. Bartoletti, Z. Liu, M. Z. Win, and A. Conti, "Device-free localization of multiple targets in cluttered environments," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 5, pp. 3906–3923, Oct. 2022.

[14] A. Bazzi, D. T. M. Slock, and L. Meilhac, "Detection of the number of superimposed signals using modified MDL criterion: A random matrix approach," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*. 2016, pp. 4593–4597.

[15] 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.

[16] C. Ren, M. N. El Korso, J. Galy, E. Chaumette, P. Larzabal, and A. Renaux, "Performance bounds under misspecification model for MIMO radar application," in *Proc. 23rd Eur. Signal Process. Conf. (EUSIPCO)*. 2015, pp. 514–518.