CHALMERS
UNIVERSITY OF TECHNOLOGY

Privacy Preservation in Delay-Based Localization Systems: Artificial Noise or Artificial Multipath?

Privacy Preservation in Delay-Based Localization Systems: Artificial Noise or Artificial Multipath?

Yuchen Zhang*, Hui Chen†, and Henk Wymeersch†
*Electrical and Computer Engineering, King Abdullah University of Sciences and Technology, Saudi Arabia
†Department of Electrical Engineering, Chalmers University of Technology, Sweden

***Abstract*—Localization plays an increasingly pivotal role in 5G/6G systems, enabling various applications. This paper focuses on the privacy concerns associated with delay-based localization, where unauthorized base stations attempt to infer the location of the end user. We propose a method to disrupt localization at unauthorized nodes by injecting artificial components into the pilot signal, exploiting model mismatches inherent in these nodes. Specifically, we investigate the effectiveness of two techniques, namely artificial multipath (AM) and artificial noise (AN), in mitigating location leakage. By leveraging the misspecified Cramér-Rao bound framework, we evaluate the impact of these techniques on unauthorized localization performance. Our results demonstrate that pilot manipulation significantly degrades the accuracy of unauthorized localization while minimally affecting legitimate localization. Moreover, we find that the superiority of AM over AN varies depending on the specific scenario.**

***Index Terms*—Secure localization, artificial path, artificial noise, misspecified Crámer-Rao bound.**

I. Introduction

Localization is a fundamental component in 5G/6G systems, facilitating a variety of innovative applications such as collaborative robots and augmented reality [1]. Compared with angle-based localization, delay-based methods have the advantage of cost-effectiveness as only a single antenna is required [2]. Specifically, time-difference-of-arrival (TDOA) can be used with either a downlink positioning reference signal or an uplink sounding reference signal, while multi-round-trip-time (RTT) that utilize both reference signals can support time-of-arrival (TOA)-based localization [3]. A more recent technical report, TR 38.859, has studied TDOA and RTT-based positioning using sideline communications, substantially extending localization coverage [4]. The adoption of large bandwidth signals enhances delay estimation resolution and the resolvability of multipath, making the system capable of dealing with localization tasks in non-line-of-sight (NLOS) scenarios [5].

While location-based services unlock significant new capabilities, they also introduce critical concerns regarding privacy issues, as information leakage to unauthorized entities can monitor private behavior without permission [6]. To address location leakage, various approaches have been introduced at the physical layer. In multi-antenna localization systems, techniques such as null-space beamforming and directional jamming have been proposed to degrade the performance of unauthorized localization by compromising the quality of the received signal [7], [8]. In model-free deep learning-based localization systems, adversarial machine learning has been employed to mitigate location leakage by introducing perturbations to the pilot signal [9]. However, these schemes typically rely on the availability of either the channel state information (CSI) or the utilized neural network at unauthorized nodes. Recently, a location privacy-preserving technique devoid of CSI was introduced in [10]. This method primarily manipulates the pilot signal to generate artificial multipath (AM), thereby disrupting TDOA estimation and consequently impeding localization performance at unauthorized nodes, all without necessitating access to their CSI. Besides, the injection of AMs has been demonstrated to be superior to emitting artificial noise (AN).

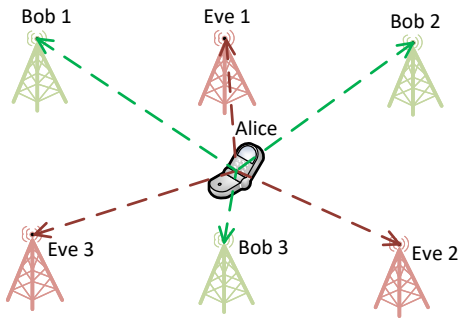

Fig. 1. Illustration of location leakage in a delay-based localization system (e.g., TDOA with 3 anchors, or TOA with 2 anchors up to an ambiguity). Alice modifies the uplink pilot to avoid being localized by the Eves.

To quantify the performance of a localization system, the Cramér-Rao bound (CRB) is usually used. However, CRB fails to account for model mismatches caused by a modified pilot when the (unauthorized) base station (BS) assumes a standard, pre-agreed signal. In such cases, instead of using CRB for privacy protection performance metrics [10]), the misspecified Cramér-Rao bound (MCRB) is preferred [11]. Previous studies using MCRB have effectively analyzed various mismatch scenarios (e.g., using a far-field model in the near-field [12], localization under hardware impairment [13] and geometry error [14], multipath scenarios [15], and reconfigurable intelligent surface-aided systems [16], [17]), demonstrating its

This work was supported, in part, by the Swedish Research Council (project 2023-03821) and Chalmers Area of Advance Transport. This publication is based upon the work supported by the King Abdullah University of Science and Technology (KAUST) Office of Sponsored Research (OSR) under Award ORA-CRG2021-4695.

utility in assessing the impact of mismatch factors.

In this work, we examine an uplink delay-based orthogonal frequency division multiplexing (OFDM) localization system, reevaluating and comparing the effectiveness of AN and AM in protecting end user location information from unauthorized BSs by considering model mismatch (see Fig. 1). Our main contributions are summarized as follows:

- We define a scenario in which an end device sends a pilot, altered by injecting artificial components, to induce erroneous position estimation at unauthorized BSs, exploiting the model mismatch present in unauthorized nodes;
- Two strategies for mitigating location leakage are investigated (AN and AM injection), whose performance is systematically quantified through MCRB-based analyses;
- Numerical results show that pilot manipulation significantly degrades unauthorized localization performance, with minimal impact on legitimate localization. Additionally, AM does not consistently outperform AN, emphasizing the necessity of selecting location privacy-preserving techniques based on the specific situation.

II. System Model

As illustrated in Fig. 1, we consider an uplink TDOA-based localization system in which several synchronized (legitimate) single-antenna BSs (Bobs) infer the location of single-antenna user equipment (UE) (Alice) based on the delays estimated from the received uplink pilot. Due to its broadcasting nature, the pilot sent from Alice could also be eavesdropped by unauthorized single-antenna BSs (Eves), leading to potential threat of location leakage.

A. Signal Model

Considering an OFDM system with line-of-sight (LOS) condition, Alice sends pilot $\mathbf{v} \in \mathbb{C}^{M\times 1}$ across M subcarriers with a total bandwidth W. Here, $\|\mathbf{v}\| = \sqrt{P}$, where P denotes the transmit power. The signal received by a receiver (Bob or Eve) is given by

$$\mathbf{y} = \alpha \mathbf{d}(\tau) \odot \mathbf{v} + \mathbf{n}, \tag{1}$$

where α is the complex channel gain, τ is the delay, $[\mathbf{d}(\tau)]_m = e^{-\jmath 2\pi m \Delta f \tau}$ is the phase shifts across subcarriers, and $\mathbf{n} \sim \mathcal{CN}(\mathbf{0}, N_0 \Delta f \mathbf{I}_M)$ is the additive Gaussian white noise (AWGN) with single-side power spectral density (PSD) N_0. Essentially, if the pilot $\mathbf{v}$ is publicly known, Alice's location can be eavesdropped upon in a two-stage process utilizing the delay estimations from various Eves. Note that NLOS paths are not considered in the received signal, which is left for future work. Nevertheless, the proposed analysis can also be applied to cases with multipath, provided the LOS is resolvable.

B. Location Leakage Mitigation Strategies

We describe two methods that Alice and Bob can employ to mitigate location leakage and thus preserve Alice's privacy: AN and AM injection. In the next section, we will then discuss localization performance at Eve under mismatch caused by the AN and AM, to evaluate the performance of the privacy preservation schemes. For simplicity and without loss of generality, we consider $\mathbf{v} = \sqrt{P/M}\mathbf{1}_M$ and introduce $P_M = P/M$.

1) Artificial Noise: Under the AN strategy, the pilot is manipulated by integrating an AWGN-like perturbation as [18]

$$\mathbf{s} = \tilde{\gamma}\sqrt{P_M}\mathbf{1}_M + \tilde{\gamma}\sqrt{\tilde{\beta}}\mathbf{z}, \tag{2}$$

where $\mathbf{z} \in \mathbb{C}^M$ is drawn from the standard complex normal distribution and then normalized to ensure $\|\mathbf{z}\| = \sqrt{P_M}$, $\tilde{\beta}$ characterizes the relative strength of the AN component, and $\tilde{\gamma}$ is a normalization factor to maintain $\|\mathbf{s}\| = \sqrt{P}$. Then, the signal received at a receiver is given by

$$\mathbf{y} = \alpha\tilde{\gamma}\sqrt{P_M}\mathbf{d}(\tau) + \alpha\tilde{\gamma}\sqrt{\tilde{\beta}}\mathbf{d}(\tau) \odot \mathbf{z} + \mathbf{n}. \tag{3}$$

2) Artificial Multipath: The concept of AM was introduced in [10], whose key idea is to manipulate the pilot by integrating perturbations, thereby creating AMs. This compromises the delay estimations, and hence localization performance of unauthorized nodes who are unaware of the manipulation. Specifically, the pilot is constructed as

$$\mathbf{s} = \gamma\mathbf{v} + \gamma\mathbf{v} \odot \sum_{l=1}^{L} \sqrt{\beta_l}\mathbf{d}(\delta_l), \tag{4}$$

where L is the number of artificial paths, β_l characterizes the relative strength of the l-th component in the pilot, δ_l is the l-th differential delay, and γ is a normalization factor to keep $\|\mathbf{s}\| = \sqrt{P}$. Similar to [9], for the paths to be physically realizable with a time-domain filter, we consider that $\min_l \delta_l \geq 0$ and $\max_l \delta_l < T_{\text{CP}}$, where T_{CP} is the OFDM cyclic prefix (CP) duration. The signal received at a receiver is expressed by

$$\mathbf{y} = \alpha\gamma \sum_{l=0}^{L} \sqrt{\beta_l}\sqrt{P_M}\mathbf{d}(\tau + \delta_l) + \mathbf{n}, \tag{5}$$

where $\beta_0 = 1$ and $\delta_0 = 0$.

III. Localization under Model Mismatch

From the perspective of Eves, model mismatch occurs as the assumed pilot is $\mathbf{v}$ while the actual pilot is $\mathbf{s}$, resulting in a misspecified estimation problem, whose performance limit should be analyzed through the MCRB [11].

A. MCRB Fundamentals

Specifically, for a parameter $\boldsymbol{\theta} \in \mathbb{R}^{K\times 1}$, the lower bound (LB) matrix for the mean squared error of a mismatched estimator is provided by [11]

$$\text{LB}(\boldsymbol{\theta}, \boldsymbol{\theta}_0) = \underbrace{\mathbf{A}_{\boldsymbol{\theta}_0}^{-1}\mathbf{B}_{\boldsymbol{\theta}_0}\mathbf{A}_{\boldsymbol{\theta}_0}^{-1}}_{\text{MCRB}(\boldsymbol{\theta}_0)} + \underbrace{(\boldsymbol{\theta} - \boldsymbol{\theta}_0)(\boldsymbol{\theta} - \boldsymbol{\theta}_0)^{\top}}_{\text{Bias}(\boldsymbol{\theta}_0)}. \tag{6}$$

Here, $\boldsymbol{\theta}_0$ denotes the pseudo-true parameter obtained by [11]

$$\boldsymbol{\theta}_0 = \arg\min_{\boldsymbol{\eta}} \mathcal{D}(f_{\text{T}}(\mathbf{y}|\boldsymbol{\theta}) \,||\, f_{\text{M}}(\mathbf{y}|\boldsymbol{\eta})), \tag{7}$$

where $\boldsymbol{\eta}$ represents the parameter under mismatched model, and $\mathcal{D}(f_{\text{T}}(\mathbf{y}|\boldsymbol{\theta}) \,||\, f_{\text{M}}(\mathbf{y}|\boldsymbol{\eta})) = \int_{f_T} f_{\text{T}}(\mathbf{y}|\boldsymbol{\theta}) \ln \frac{f_{\text{T}}(\mathbf{y}|\boldsymbol{\theta})}{f_{\text{M}}(\mathbf{y}|\boldsymbol{\eta})} \mathrm{d}\mathbf{y}$ denotes the Kullback-Leibler (KL) divergence between the true

probability distribution function (PDF) $f_{\mathrm{T}}(\mathbf{y}|\boldsymbol{\theta})$ and the mismatched PDF $f_{\mathrm{M}}(\mathbf{y}|\boldsymbol{\eta})$. Besides, $\mathbf{A}_{\boldsymbol{\theta}_0}$ and $\mathbf{B}_{\boldsymbol{\theta}_0}$ represent two generalizations of the Fisher information matrix (FIM), whose elements in the i-th row and the j-th column are determined by [11]

$$\begin{aligned}[\mathbf{A}_{\boldsymbol{\theta}_0}]_{i,j} =& 2\mathrm{Re}\left[\left(\frac{\partial^2\boldsymbol{\mu}(\boldsymbol{\eta})}{\partial[\boldsymbol{\eta}]_i\partial[\boldsymbol{\eta}]_j}\right)^{\mathsf{H}}\mathbf{C}_{\mathrm{M}}^{-1}\boldsymbol{\epsilon}(\boldsymbol{\eta})\right.\\ &\left.-\left(\frac{\partial\boldsymbol{\mu}(\boldsymbol{\eta})}{\partial[\boldsymbol{\eta}]_i}\right)^{\mathsf{H}}\mathbf{C}_{\mathrm{M}}^{-1}\left(\frac{\partial\boldsymbol{\mu}(\boldsymbol{\eta})}{\partial[\boldsymbol{\eta}]_j}\right)\right]\Bigg|_{\boldsymbol{\eta}=\boldsymbol{\theta}_0}\end{aligned} \tag{8}$$

and

$$\begin{aligned}[\mathbf{B}_{\boldsymbol{\theta}_0}]_{i,j} =& 4\mathrm{Re}\left[\boldsymbol{\epsilon}(\boldsymbol{\eta})^{\mathsf{H}}\mathbf{C}_{\mathrm{M}}^{-1}\frac{\partial\boldsymbol{\mu}(\boldsymbol{\eta})}{\partial[\boldsymbol{\eta}]_i}\right]\mathrm{Re}\left[\boldsymbol{\epsilon}(\boldsymbol{\eta})^{\mathsf{H}}\mathbf{C}_{\mathrm{M}}^{-1}\frac{\partial\boldsymbol{\mu}(\boldsymbol{\eta})}{\partial[\boldsymbol{\eta}]_j}\right]\\ &+2\mathrm{Re}\left[\left(\frac{\partial\boldsymbol{\mu}(\boldsymbol{\eta})}{\partial[\boldsymbol{\eta}]_i}\right)^{\mathsf{H}}\mathbf{C}_{\mathrm{M}}^{-1}\left(\frac{\partial\boldsymbol{\mu}(\boldsymbol{\eta})}{\partial[\boldsymbol{\eta}]_j}\right)\right]\Bigg|_{\boldsymbol{\eta}=\boldsymbol{\theta}_0}\end{aligned} \tag{9}$$

respectively. Here, $\mathbf{C}_{\mathrm{M}}$ represents the covariance matrix of $f_{\mathrm{M}}(\mathbf{y}|\boldsymbol{\eta})$, which is irrelevant to $\boldsymbol{\eta}$, and $\boldsymbol{\epsilon}(\boldsymbol{\eta}) = \boldsymbol{\kappa}(\boldsymbol{\theta}) - \boldsymbol{\mu}(\boldsymbol{\eta})$ with $\boldsymbol{\kappa}(\boldsymbol{\theta})$ and $\boldsymbol{\mu}(\boldsymbol{\eta})$ being the noise-free observations under the true and mismatched models, respectively [13], [14].

B. MCRB From Eve's Perspective

Given that delays are independently estimated at various Eves before being combined to estimate Alice's location, determining the localization performance under model mismatch can proceed in two stages:

1) *MCRB for Delay Estimation:* The pseudo-true delays, along with their corresponding MCRBs, are derived, forming another misspecified model regarding delay estimations.
2) *MCRB and LB for Location Estimation:* Leveraging the relationship between delays and location, the MCRB and LB of location estimation are determined.

We will make the assumption of *powerful attackers*, where the only parameter each Eve estimates is the delay τ, while the complex channel gain α is known, and there is no clock offset between Alice and Eve. This assumption leads to a worst-case analysis from the perspective of legitimate nodes. The rationale behind this assumption is that if we can safeguard Alice's location from being leaked to Eves in the worst-case scenario, then more practical cases with weaker Eve would not be worse.

1) MCRB for Delay Estimation Under AM: For the sake of notational convenience, the following derivation concerning delay estimation is performed at a specific Eve without specifying her index. Define noise-free received signals of the true model (5) by $\boldsymbol{q}_{\mathrm{T}}(\tau) = \alpha\gamma\sum_{l=0}^{L}\beta_l\sqrt{P_M}\mathbf{d}(\tau+\delta_l)$ and the mismatched model (1) by $\boldsymbol{q}_{\mathrm{M}}(\tau) = \alpha\sqrt{P_M}\mathbf{d}(\tau)$. The true and mismatched PDFs of the received signal, conditioned on delay, are expressed as $f_{\mathrm{T}}(\mathbf{y}|\tau) \propto \exp\left(-\|\mathbf{y}-\boldsymbol{q}_{\mathrm{T}}(\tau)\|^2/(N_0\Delta f)\right)$ and $f_{\mathrm{M}}(\mathbf{y}|\tau) \propto \exp\left(-\|\mathbf{y}-\boldsymbol{q}_{\mathrm{M}}(\tau)\|^2/(N_0\Delta f)\right)$ By substituting these into (7), the pseudo-true delay can be obtained by

$$\begin{aligned}\tau_0 &= \arg\min_{\eta}\mathcal{D}\left(f_{\mathrm{T}}(\mathbf{y}|\tau)\,||\,f_{\mathrm{M}}(\mathbf{y}|\eta)\right)\\ &= \arg\min_{\eta}\ \|\boldsymbol{q}_{\mathrm{T}}(\tau)-\boldsymbol{q}_{\mathrm{M}}(\eta)\|^2\\ &= \arg\max_{\eta}\ \sum_{m=1}^{M}\sum_{l=0}^{L}\sqrt{\beta_l}\cos\left(2\pi m\Delta f(\tau+\delta_l-\eta)\right).\end{aligned} \tag{10}$$

The above problem can be solved via line search. Then, through algebraic manipulation of (8) and (9), the MCRB regarding delay estimation is a scalar, as expressed in (11) at the bottom of this page, where

$$\xi(\tau_0) = \sum_{m=1}^{M}\sum_{l=0}^{L} m\sqrt{\beta_l}\exp\left(\jmath 2\pi m\Delta f(\tau+\delta_l-\tau_0)\right). \tag{12}$$

Note that the MCRB in (11) degenerates to CRB (as will be introduced in (17)) without model mismatch, i.e., when $\beta_l = 0$ and $\delta_l = 0$ $(l = 1,\ldots,L)$.

2) MCRB for Delay Estimation Under AN: One can derive the MCRB for delay estimation under AN, following a parallel process to that of its AM counterpart. For conciseness, we present the results directly. Specifically, the pseudo-true delay can be obtained by

$$\begin{aligned}\tau_0 = \operatorname*{argmax}_{\eta}\ \sum_{m=1}^{M}&\left(\cos\left(2\pi m\Delta f(\tau-\eta)\right)\right.\\ &\left.+\sqrt{\tilde{\beta}}\,|z_m|\cos\left(2\pi m\Delta f(\tau-\eta)+\angle z_m\right)\right),\end{aligned} \tag{13}$$

which can also be solved through line search. Moreover, the corresponding MCRB is in the same form as (11), albeit with

$$\xi(\tau_0) = \sum_{m=1}^{M} m(1+\sqrt{\tilde{\beta}}z_m)\exp\left(\jmath 2\pi m\Delta f(\tau-\tau_0)\right). \tag{14}$$

Remark 1. *For LOS propagation, under both AM and AN, the pseudo-true delay from Eve i's perspective can be expressed as $\tau_{0,i} = \tau_i + \Delta$, where Δ is independent of i. This is because the bias depends on the added perturbation in* (2) *and* (4) *is independent on Eve i. For multipath scenario, however, Δ may no longer be identical for different Eves.*

3) MCRB and LB for Location Estimation: Based on the results pertaining to delay estimation under model mismatch, we can proceed to evaluate the MCRB and LB of location estimation, achieved through multiple cooperative Eves. Let $\boldsymbol{\tau}_{\mathrm{E}} = [\tau_{\mathrm{E},1},\ldots,\tau_{\mathrm{E},K_{\mathrm{E}}}]^\top$ and $\overline{\boldsymbol{\tau}}_{\mathrm{E}} = [\overline{\tau}_{\mathrm{E},1},\ldots,\overline{\tau}_{\mathrm{E},K_{\mathrm{E}}}]^\top$ represent the ground-truth delays and pseudo-true delays at the Eves, where K_{E} denotes the number of Eves. Let $\mathbf{p}_{\mathrm{A}}$ and $\mathbf{p}_{\mathrm{E},i}$

$$\mathrm{MCRB}(\tau_0) = \frac{\left(6|\alpha|P\gamma\mathrm{Im}\left[\xi(\tau_0)\right]\right)^2 + 3M^2(M+1)(2M+1)N_0\Delta fP}{\left(12\pi\Delta fM^{-\frac{1}{2}}|\alpha|P^{\frac{3}{2}}\gamma\mathrm{Re}\left[\xi(\tau_0)\right] - 6\pi M^{\frac{1}{2}}(M+1)\Delta f|\alpha|P^{\frac{3}{2}} + 2\pi M(M+1)(2M+1)\Delta f|\alpha|P\right)^2} \tag{11}$$

denote the locations of Alice and the i-th Eve, respectively.[1]

Under the powerful attacker assumption, Eve is synchronized to Alice, so $\tau_{\mathrm{E},i} = \|\mathbf{p}_\mathrm{A} - \mathbf{p}_{\mathrm{E},i}\|/c$, where c is the speed of light. The true and mismatched PDFs of the delay estimation $\hat{\boldsymbol{\tau}}_\mathrm{E}$, conditioned on Alice's position, are expressed as

$$f_\mathrm{T}\left(\hat{\boldsymbol{\tau}}_\mathrm{E}|\mathbf{p}_\mathrm{A}\right) \propto \exp\left(-\frac{1}{2}\left(\hat{\boldsymbol{\tau}}_\mathrm{E} - \overline{\boldsymbol{\tau}}_\mathrm{E}\right)^\top \boldsymbol{\Xi}_\mathrm{T}^{-1}\left(\hat{\boldsymbol{\tau}}_\mathrm{E} - \overline{\boldsymbol{\tau}}_\mathrm{E}\right)\right) \quad (15)$$

and

$$f_\mathrm{M}\left(\hat{\boldsymbol{\tau}}_\mathrm{E}|\mathbf{p}_\mathrm{A}\right) \propto \exp\left(-\frac{1}{2}\left(\hat{\boldsymbol{\tau}}_\mathrm{E} - \boldsymbol{\tau}_\mathrm{E}\right)^\top \boldsymbol{\Xi}_\mathrm{M}^{-1}\left(\hat{\boldsymbol{\tau}}_\mathrm{E} - \boldsymbol{\tau}_\mathrm{E}\right)\right) \quad (16)$$

respectively. Here, $\boldsymbol{\Xi}_\mathrm{T} \in \mathbb{R}^{K_\mathrm{E}\times K_\mathrm{E}}$ and $\boldsymbol{\Xi}_\mathrm{M} \in \mathbb{R}^{K_\mathrm{E}\times K_\mathrm{E}}$ are diagonal variance matrices with their i-th diagonal elements being MCRB$(\overline{\tau}_{\mathrm{E},i})$ and CRB$(\tau_{\mathrm{E},i})$, respectively. In addition, CRB$(\tau_{\mathrm{E},i})$ denotes the CRB for delay estimation at the i-th Eve without model mismatch (i.e., in (1)), derived as

$$\mathrm{CRB}(\tau_{\mathrm{E},i}) = \frac{3N_0}{4\pi^2\Delta f\left(M+1\right)\left(2M+1\right)\left|\alpha_{\mathrm{E},i}\right|^2 P}, \quad (17)$$

where $\alpha_{\mathrm{E},i}$ is the complex channel gain at the i-th Eve.

We now proceed by deriving the pseudo-true location $\overline{\mathbf{p}}_\mathrm{A}$, the MCRB, and the LB.

- *Pseudo-True Location:* By substituting (15) and (16) into (7), the pseudo-true position of Alice can be obtained by

$$\begin{aligned}\overline{\mathbf{p}}_\mathrm{A} &= \arg\min_{\tilde{\mathbf{p}}_\mathrm{A}} \mathcal{D}\left(f_\mathrm{T}\left(\hat{\boldsymbol{\tau}}_\mathrm{E}|\mathbf{p}_\mathrm{A}\right) \| f_\mathrm{M}\left(\hat{\boldsymbol{\tau}}_\mathrm{E}|\tilde{\mathbf{p}}_\mathrm{A}\right)\right)\\ &= \arg\min_{\tilde{\mathbf{p}}_\mathrm{A}} \left(\tilde{\boldsymbol{\tau}}_\mathrm{E}(\tilde{\mathbf{p}}_\mathrm{A}) - \overline{\boldsymbol{\tau}}_\mathrm{E}\right)^\top \boldsymbol{\Xi}_\mathrm{M}^{-1}\left(\tilde{\boldsymbol{\tau}}_\mathrm{E}(\tilde{\mathbf{p}}_\mathrm{A}) - \overline{\boldsymbol{\tau}}_\mathrm{E}\right)\\ &= \arg\min_{\tilde{\mathbf{p}}_\mathrm{A}} \sum_{i=1}^{K_\mathrm{E}} \frac{\left(\|\tilde{\mathbf{p}}_\mathrm{A} - \mathbf{p}_{\mathrm{E},i}\| - c\overline{\tau}_{\mathrm{E},i}\right)^2}{\mathrm{MCRB}\left(\overline{\tau}_{\mathrm{E},i}\right)}, \end{aligned} \quad (18)$$

  where $\tilde{\boldsymbol{\tau}}_\mathrm{E} = [\tilde{\tau}_{\mathrm{E},1}, \ldots, \tilde{\tau}_{\mathrm{E},K_\mathrm{E}}]^\top$ with $\tilde{\tau}_{\mathrm{E},i} = \|\tilde{\mathbf{p}}_\mathrm{A} - \mathbf{p}_{\mathrm{E},i}\|/c$. The above problem can be solved using gradient descent with backtracking line search, wherein an initial point can be obtained via a coarse grid search [16].
- *MCRB:* To compute the MCRB of location estimation, we need to determine the components therein. Specifically, for the first-order partial derivatives, we have

$$\frac{\partial \boldsymbol{\tau}_\mathrm{E}}{\partial\left[\mathbf{p}_\mathrm{A}\right]_k} = \left[\frac{\left[\mathbf{p}_\mathrm{A}\right]_k - \left[\mathbf{p}_{\mathrm{E},1}\right]_k}{c\left\|\mathbf{p}_\mathrm{A} - \mathbf{p}_{\mathrm{E},1}\right\|}, \ldots, \frac{\left[\mathbf{p}_\mathrm{A}\right]_k - \left[\mathbf{p}_{\mathrm{E},K_\mathrm{E}}\right]_k}{c\left\|\mathbf{p}_\mathrm{A} - \mathbf{p}_{\mathrm{E},K_\mathrm{E}}\right\|}\right]^\top. \quad (19)$$

  For the second-order partial derivatives, we have

$$\frac{\partial^2 \boldsymbol{\tau}_\mathrm{E}}{\partial\left[\mathbf{p}_\mathrm{A}\right]_k \partial\left[\mathbf{p}_\mathrm{A}\right]_n} = \begin{cases} \boldsymbol{\psi}\left(\mathbf{p}_\mathrm{A}\right), & k = n,\\ \mathbf{0}_{K_\mathrm{E}}, & k \neq n, \end{cases} \quad (20)$$

  where

$$\boldsymbol{\psi}\left(\mathbf{p}_\mathrm{A}\right) = \left[\frac{1}{c\left\|\mathbf{p}_\mathrm{A} - \mathbf{p}_{\mathrm{E},1}\right\|}, \ldots, \frac{1}{c\left\|\mathbf{p}_\mathrm{A} - \mathbf{p}_{\mathrm{E},K_\mathrm{E}}\right\|}\right]^\top. \quad (21)$$

  Then, MCRB $\left(\overline{\mathbf{p}}_\mathrm{A}\right)$ is obtained by substituting (19) and (20), along with $\boldsymbol{\Xi}_\mathrm{M}$ and $\boldsymbol{\epsilon}(\tilde{\mathbf{p}}_\mathrm{A}) = \tilde{\boldsymbol{\tau}}_\mathrm{E} - \overline{\boldsymbol{\tau}}_\mathrm{E}$, into (8) and (9).
- *LB:* The LB matrix is expressed as

$$\mathrm{LB}\left(\mathbf{p}_\mathrm{A}, \overline{\mathbf{p}}_\mathrm{A}\right) = \mathrm{MCRB}\left(\overline{\mathbf{p}}_\mathrm{A}\right) + \left(\mathbf{p}_\mathrm{A} - \overline{\mathbf{p}}_\mathrm{A}\right)\left(\mathbf{p}_\mathrm{A} - \overline{\mathbf{p}}_\mathrm{A}\right)^\top. \quad (22)$$

[1]To maintain the generality, we do not explicitly specify the dimension of the location, as the derivations can be applied to both 2D and 3D cases.

Based on (22), the lower bound for the expected root mean squared error of position estimation in the presence of model mismatch is expressed as

$$\sqrt{\mathbb{E}\left[\|\hat{\mathbf{p}}_\mathrm{A} - \mathbf{p}_\mathrm{A}\|^2\right]} \geq \sqrt{\mathrm{tr}\left(\mathrm{LB}\left(\mathbf{p}_\mathrm{A}, \overline{\mathbf{p}}_\mathrm{A}\right)\right)}, \quad (23)$$

where $\hat{\mathbf{p}}_\mathrm{A}$ denotes a misspecified-unbiased estimator, with its mean under the true model being $\overline{\mathbf{p}}_\mathrm{A}$.

C. Qualitative Analysis

Based on the MCRB analysis, we perform a qualitative performance prediction in 2D on the impact of both AM and AN as a function of the number of Eves. When there is only 1 Eve, AM and AN will constrain Eve's estimate of Alice on a circle around Eve, the radius of which depends on AM and AN. When there are 2 Eves, they will determine Alice on the intersection of two circles. This means that they will determine a location estimate (up to an ambiguity), with an error that depends on the LB. When there are 3 or more Eves, the localization problem becomes over-determined, which implies that methods such as TDOA can be applied. Given the observations in Remark 1, this implies that neither AM nor AN can protect Alice from the Eves determining her location.

In the next section, we will use the derived bounds to quantitatively evaluate the impact of AM and AN on localization considering 2 Eves.

IV. Numerical Results

A. Scenario

Unless otherwise specified, the simulation parameters are presented as follows: A 2D localization scenario is considered where Alice is located at $[80\text{ m}, 80\text{ m}]^\top$, three Bobs (legitimate BSs) are located at $[0\text{ m}, 0\text{ m}]^\top$, $[90\text{ m}, 0\text{ m}]^\top$, and $[80\text{ m}, 160\text{ m}]^\top$, respectively, while two Eves (unauthorized BSs) are located at $[0\text{ m}, 0\text{ m}]^\top$ and $[80\text{ m}, 160\text{ m}]^\top$, respectively. The transmit power $P = 10$ dBm, carrier frequency $f_c = 28$ GHz, bandwidth $W = 100$ MHz, number of subcarriers $M = 1024$, and noise PSD is -173.855 dBm/Hz. In addition, the differential delays of AM follow $\delta_l = l/(LW)$ $(l = 0, 1, \ldots, L)$, with the maximum injected delay being the time resolution[2], i.e., $1/W$.

B. Results and Discussion

We will first analyze the AM approach in detail, as it has more tunable parameters than the AN approach. Then, the impact of both AN and AM on localization will be evaluated under different scenarios.

1) Impact of the Number of AMs: Fig. 2 illustrates the effects of varying AM numbers L on the LB of unauthorized localization. To demonstrate the impact of the relative strength of the pilot's components, we consider $\beta_l = (l+1)^t$ $(l = 0, 1, \ldots, L)$ with t as the decay factor. Specifically, for $t < 0$, more power is allocated to the component with a smaller delay,

[2]If the maximum injected delay exceeds the time resolution, Eve can distinguish it as an additional path. Consequently, the mismatched model would not solely comprise a LOS path, which is a case left for our future work.

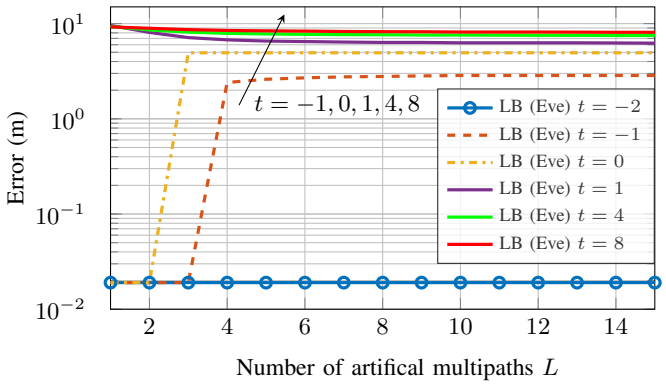

Fig. 2. Location LB versus number of AMs for various power allocation coefficients.

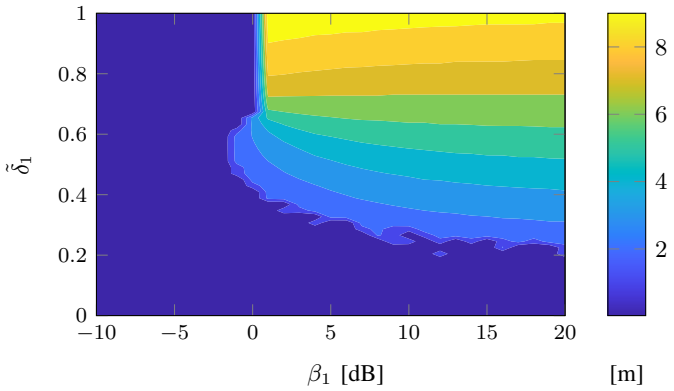

Fig. 3. Heat map for localization LB versus β_1 and $\tilde{\delta}_1$.

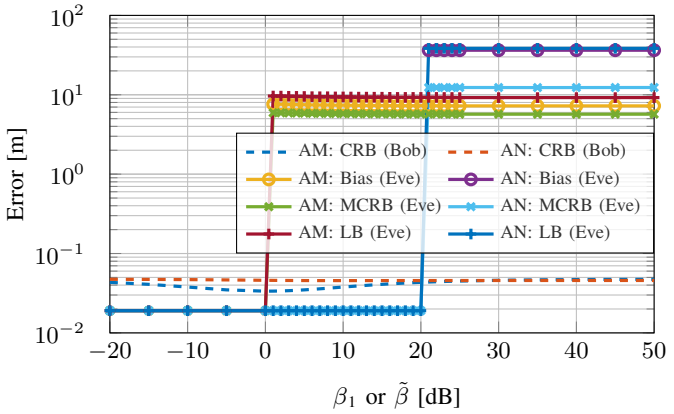

Fig. 4. Localization error bounds (CRB, MCRB, and LB) and bias under AM and AN, versus β_1 or $\tilde{\beta}$, for $\delta_1 = 1/W$.

for $t = 0$, equal power is allocated to each component, and for $t > 0$, less power is allocated to the component with a smaller delay. As can be concluded, for different L, allocating more power to the component with a larger delay, results in a larger LB for unauthorized localization. Furthermore, keeping a minimal number of components intended for generating AMs ($L = 1$) is the most effective choice. The key insight here is that injecting more than one AM is not beneficial. Therefore, we set $L = 1$ in the following simulations.

2) Impact of AMs Gain and Delay: Fig. 3 examines how different selections of β_1 and $\tilde{\delta}_1 = \delta_1 W$ influence the LB of unauthorized localization on a heat map. In this figure, when β_1 is sufficiently large, setting a larger $\tilde{\delta}_1$ (closer to 1) is more helpful in mitigating location leakage. This is because it increases the chance that Eve takes the generated AM with artificial delay as a LoS path, resulting in a larger bias in delay estimation and LB of position estimation. An interesting phenomenon worth noting is that when β_1 is slightly less than 0 dB, i.e., the component in the pilot intended for generating the AM has almost the same power as the original component, the LB of location estimation undergoes an up-then-down process as the injected delay becomes larger. This stems from the initial increase in injected delay, causing a larger bias in delay estimation and consequently larger LB in position estimation due to insufficient separation between the two paths. As the injected delay gets close to the time resolution, the relatively stronger LOS path is more distinguishable, resulting in reduced bias and LB in position estimation. On the contrary, the NLOS dominates when $\beta_1 > 0$ dB.

3) Comparison of the Impact of the Injected Component: In Fig. 4, we compare the LB of both the legitimate localization at Bobs and the unauthorized localization at Eves under AM and AN. Specifically, we evaluate the impacts of the relative strength of injected components (indicated by β_1 under AM and $\tilde{\beta}$ under AN) on the localization performance. Note that the AN realization is fixed among different $\tilde{\beta}$ to remain consistence, and the position of sudden jump (i.e., 0 dB) may change with other realizations. As seen, when the strength of the injected component is moderately larger than the original component, AM significantly outperforms AN in mitigating location leakage. However, when the injected component becomes more dominant, i.e., almost all power is allocated to it when formulating the pilot, AN exhibits superiority over AM. This results from the fact that the delay bias incurred by AM is limited by the maximum injected differential delay, which falls within the time resolution, while AN leads to a delay bias larger than this threshold. In the injected-component-dominant regime, the increased bias in delay estimation translates into a boost in LB in position estimation.

It is noteworthy that both AM and AN have an insignificant impact on legitimate localization in terms of CRB. This is because Bobs, as cooperative nodes, are aware of manipulation in the pilot without suffering from model mismatch. As long as the power of the pilot remains invariant, localization performance would not be severely impacted. However, it is observed that the CRB under AM is usually smaller than that under AN, especially when the injected and original components have relatively balanced power (e.g., $\beta_1 = 0$), demonstrating AM's advantage in imposing less performance degradation towards legitimate localization.

4) Comparison of the Impact of the Transmit Power: Figs. 5(a) and (b) depict the localization error bounds and bias versus transmit power for β_1 or $\tilde{\beta} = 10$ dB and β_1 or $\tilde{\beta} = 30$ dB, respectively. As observed, for unauthorized localiza-

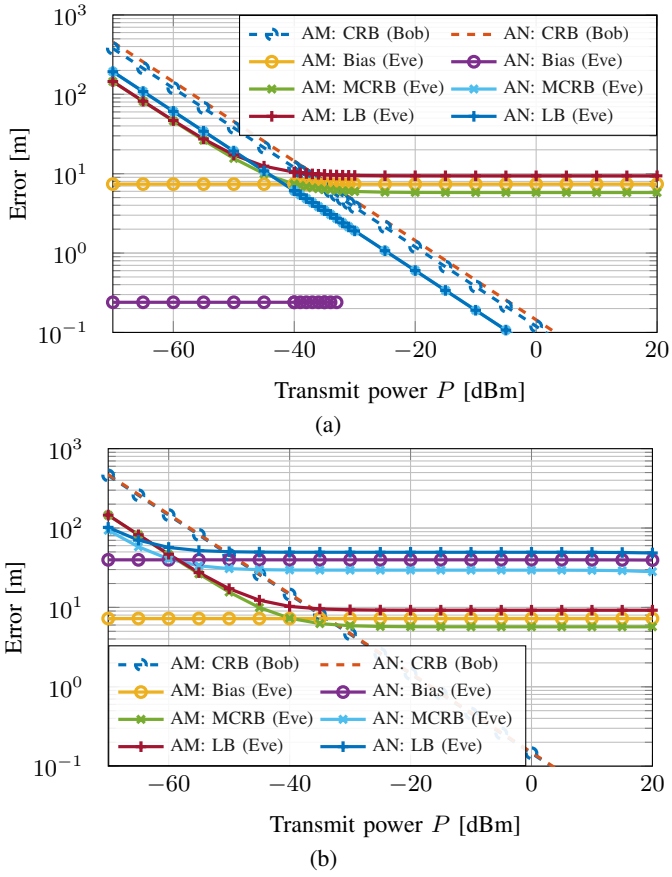

Fig. 5. Localization error bounds (CRB, MCRB, and LB) and bias under AM and AN for $\delta_1 = 1/W$, versus (a) Transmit power P when $\beta_1 = 10$ dB. (b) Transmit power P when $\beta_1 = 30$ dB.

tion, the CRB decreases in the low-power regime and saturates as the power increases, demonstrating the mitigation of location leakage (i.e., the localization error is above a certain level). For legitimate localization without model mismatch, the CRB constantly decreases with increasing power. Note that we are analyzing the worst case where Even knows the clock offset and channel gain, and hence the LB is lower than CRB in the low-power regime where bias is not dominated. Additionally, when the transmit power is high (i.e., the noise power level is relatively low when $P > -30$ dBm), as shown in 5(a), AN will not introduce any bias term (only MCRB). Finally, as coincided with Fig. 4, AM is superior to AN with a moderately strong injected component (as shown in Fig. 5(a)), AN fails to introduce a large bias or enlarge variance) but less effective than AN when the injected component becomes more dominant (as shown in 5(b)).

V. Conclusion

This paper addressed the threat of location leakage in delay-based uplink localization systems, in which several unauthorized BSs could potentially infer the position of an end user. To protect the location privacy from being exposed to unauthorized BSs, we investigated two methods, namely AM and AN, whose key idea is manipulating the pilot by injecting an artificial component. This manipulation ensures that unauthorized BSs, without knowledge of the change in pilot, would undergo model mismatch and generate erroneous delay and location estimations. To analyze the performance of unauthorized localization, we resorted to the MCRB analysis, tailored for evaluating estimation under model mismatch. Numerical results demonstrated that the manipulation in the pilot significantly undermined the performance of unauthorized localization while imposing marginal performance degradation to legitimate localization. Furthermore, the superiority of AM over AN varied depending on the specific scenario. Future work will extend the analytical framework to angle-based and scene-aware localization.

References

[1] A. Behravan *et al.*, "Positioning and sensing in 6G: Gaps, challenges, and opportunities," *IEEE Veh. Technol. Mag.*, vol. 18, no. 1, pp. 40–48, Dec. 2022.

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

[3] "3GPP TR 38.855 V16.0.0: Study on NR positioning support (Release 16) (accessed on 10-Feb-2023)," Mar. 2019. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3501

[4] "3GPP TR 38.859 V18.0.0: Study on expanded and improved NR positioning (Release 18) (accessed on 20-Apr-2024)," Dec. 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3985

[5] Z. Deng *et al.*, "A TDOA and PDR fusion method for 5G indoor localization based on virtual base stations in unknown areas," *IEEE Access*, vol. 8, pp. 225 123–225 133, Dec. 2020.

[6] R. Shokri *et al.*, "Protecting location privacy: optimal strategy against localization attacks," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, 2012, pp. 617–627.

[7] J. J. Checa *et al.*, "Location-privacy-preserving technique for 5G mmWave devices," *IEEE Commun. Lett.*, vol. 24, no. 12, pp. 2692–2695, 2020.

[8] S. Tomasin, "Beamforming and artificial noise for cross-layer location privacy of E-health cellular devices," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Wkshps)*, 2022, pp. 568–573.

[9] P. Huang *et al.*, "Attacking and defending deep-learning-based off-device wireless positioning systems," *IEEE Trans. Wireless Commun. (Early Access)*, 2024.

[10] J. Li *et al.*, "Channel state information-free artificial noise-aided location-privacy enhancement," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, 2023.

[11] S. Fortunati *et al.*, "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.

[12] H. Chen *et al.*, "Channel model mismatch analysis for XL-MIMO systems from a localization perspective," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2022, pp. 1588–1593.

[13] ——, "Modeling and analysis of OFDM-based 5G/6G localization under hardware impairments," *IEEE Trans. Wireless Commun. (Early Access)*, Dec. 2023.

[14] 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)*, 2023.

[15] M. Levy-Israel *et al.*, "MCRB on DOA estimation for automotive MIMO radar in the presence of multipath," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 59, no. 5, pp. 4831–4843, Jun. 2023.

[16] C. Ozturk *et al.*, "RIS-aided near-field localization under phase-dependent amplitude variations," *IEEE Trans. Wireless Commun.*, vol. 22, no. 8, pp. 5550–5566, Jan. 2023.

[17] ——, "RIS-aided localization under pixel failures," *IEEE Trans. Wireless Commun. (Early Access)*, Jan. 2024.

[18] B. He *et al.*, "Artificial noise injection for securing single-antenna systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9577–9581, 2017.