Physical Layer Location Privacy in SIMO Communication Using Fake Path Injection

Duy Tran Trong, Maxime Ferreira Da Costa, Trung Nguyen Linh

Physical Layer Location Privacy in SIMO Communication Using Fake Path Injection

Tran Trong Duy*†, Maxime Ferreira Da Costa†, and Nguyen Linh Trung*
*AVITECH, VNU University of Engineering & Technology, Hanoi, Vietnam
†CentraleSupélec, Université Paris–Saclay, CNRS, Laboratory of Signals and Systems, Gif-sur-Yvette, France

***Abstract*—Fake path injection is an emerging paradigm for inducing privacy over wireless networks. In this paper, fake paths are injected by the transmitter into a SIMO multipath communication channel to preserve her physical location from an eavesdropper. A novel statistical privacy metric is defined as the ratio between the largest (resp. smallest) eigenvalues of Bob's (resp. Eve's) Cramér-Rao lower bound on the SIMO multipath channel parameters to assess the privacy enhancements. Leveraging the spectral properties of generalized Vandermonde matrices, bounds on the privacy margin of the proposed scheme are derived. Specifically, it is shown that the privacy margin increases quadratically in the inverse of the separation between the true and the fake paths under Eve's perspective. Numerical simulations further showcase the approach's benefit.**

I. Introduction

Electronic devices and software services requesting, storing, and sharing user's physical location are more ubiquitous than ever, posing significant privacy issues for both individuals and governments. While novel approaches to protect users' location are to be developed, most are software or network-based and operate on the upper layer of the communication stack, see [1], [2] and references therein. They are, however, ineffective in securing the radio transmissions.

On the other hand, the main physical layer security methods protect users' physical location from real-time localization systems. Those systems typically consist of beacons with multiple antennas that collect the user's channel state information and then fuse their samples to estimate the target's location collaboratively. To circumvent localisation systems, protocols adding artificial pseudo-random noise to the transmitted signal or to spatially discriminate the physical space via beamforming [3]–[8] are proposed. In particular, Goel et. al [3] achieves a secrecy capacity by introducing artificial noise in the null space of the legitimate receiver's channel either with or without the help of amplifying relays, while [4] relies on synchronized transmissions from cooperative agents to distort the measured received signal strength at illegitimate receivers. Artificial noise and beamforming are combined in [7] to minimize the power of the signal at unwanted stations. However, those approaches hide the transmitter's location from all receiving parties and exclude the option to disclose the location to legitimate ones. Additionally, noise injection and beamforming leverage implicit assumptions on the eavesdropper channel to operate, which might be hardly verified in practice.

More recently, a novel beamforming scheme for location privacy via fake path injection was proposed by Li. and al. in [9], [10] in the context of multiple-input single-output orthogonal frequency division multiplexing (MISO-OFDM) communication. Unlike the previous, this method does not require channel information and allows the disclosure of the transmitter's location to legitimate parties. A key in the privacy analysis of this scheme is the stability of the *line spectral estimation* problem (*a.k.a* super-resolution), which consists of recovering the frequencies of complex exponentials from finite samples of their linear combination [11]. In particular, the author's analysis leverages recent progress made in understanding the fundamental limit of line spectral estimation and its relationship with the condition number of Vandermonde matrices [12]–[15].

A. Contributions and Organization of the Paper

Inspired by [9], [10], we consider the problem of protecting the location of a transmitter (Alice) from an eavesdropper (Eve) in her communication with a legitimate receiver (Bob). We focus on the unchartered case where the communication medium is a single-input multiple-output (SIMO) geometric multi-path channel. If Bob and Eve dispose of linear antenna arrays, both parties can attempt to estimate the angle-of-arrivals (AoAs) of the impinging paths, leaking information on Alice's physical location. We focus on the case of Alice transmitting a known pilot sequence. We establish that fake paths injection can prevent Eve from accurately estimation the channel coefficients and the AoA's, inducing privacy. To ease Bob's channel estimate, the existence of a side-channel is supposed, where Alice and Bob exchange at a low-information rate the parameters of the fake paths, so they can be resolved at the receiver side.

To assess the privacy benefit of the communication paradigm, a novel *statistical privacy metric* is introduced in Definition 1 as the quotient between the smallest eigenvalue of Eve's Cramér-Rao lower bound (CRB) on the channel parameters based with the largest eigenvalue of Bob's one. This statistical metric is more stringent than the metric adopted in [10], as it uniformly controls the error estimate of *any linear combination* of the channel parameters. It is built on recent advances in controlling the condition number of *generalized Vandermonde matrices* [16].

Tran Trong Duy's work is funded by the Master, PhD Scholarship Programme of Vingroup Innovation Foundation (VINIF): VINIF.2022.ThS.018.
M. Ferreira Da Costa's work is supported by ANR: ANR-20-IDEES-0002.

The rest of this paper is organized as follows. The SIMO communication model with side-information channel and the secrecy metric conducting our analysis are presented in Section II, where their relevance is discussed. Section III presents our main privacy results. Two specific cases are considered:

1) Eve knows the channel coefficients and only infers Alice's AoAs;
2) Eve infers both the channel coefficients and Alice AoAs.

In both cases, explicit bounds on the secrecy margin are provided. In particular, the importance of small angular separations between the true and the fake paths in Eve's perspective in inducing secrecy is highlighted. Section IV presents the proof of the preceding results. Numerical simulations validating the theoretical secrecy bounds are provided in Section V, and a conclusion is drawn in Section VI.

B. Mathematical Notation and Definitions

Let $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ be the unidimensional torus. For any $\tau \in \mathbb{T}$, we define $\boldsymbol{v}_0(\tau) \in \mathbb{C}^N$ and $\boldsymbol{v}_1(\tau) = \frac{\mathrm{d}\boldsymbol{v}_0(\tau)}{\mathrm{d}\tau} \in \mathbb{C}^N$ as,

$$\boldsymbol{v}_0(\tau) = \frac{1}{\sqrt{N}}\left[e^{-i2\pi(-n)\tau}, \dots, e^{i2\pi n\tau}\right]^\top \tag{1a}$$

$$\boldsymbol{v}_1(\tau) = \frac{1}{\sqrt{N}}\left[i2\pi(-n)e^{i2\pi(-n)\tau}, \dots, i2\pi n e^{i2\pi n\tau}\right]^\top, \tag{1b}$$

where $2n+1 = N$. For any set $\boldsymbol{\tau} = \{\tau_1, \dots, \tau_L\} \subset \mathbb{T}$ of L elements, we define by $\boldsymbol{V}_0(\boldsymbol{\tau}), \boldsymbol{V}_1(\boldsymbol{\tau}) \in \mathbb{C}^{N\times L}$, the *generalized Vandermonde matrices*

$$\boldsymbol{V}_p(\boldsymbol{\tau}) = \left[\boldsymbol{v}_p(\tau_1), \dots, \boldsymbol{v}_p(\tau_L)\right], \quad p \in \{0, 1\}. \tag{2}$$

The normalized Dirichlet kernel of order $N = 2n+1$, written D_N, is given for any $t \in \mathbb{R}$ by $D_N(t) = \frac{1}{N}\sum_{k=-n}^{n} e^{-i2\pi kt}$, which an infinitely derivable, periodic function with period 1. Of particular interest are the identities $D_N(0) = 1$, $D_N''(0) = -\frac{\pi^2}{3}(N-1)(N+1)$, $D_N^{(4)}(0) = \frac{\pi^4}{5}N^4(1+o(1))$.

II. Problem Statement

A. SIMO Model with Fake Path Injection

We consider localization in SIMO communication, in which the transmission between a transmitter (Alice) and a receiver (Bob) is overheard by an eavesdropper (Eve). We assume both Bob and Eve to know the pilot sequence transmitted by Alice, and to dispose of a uniform linear array of N antennas, which we assume of half-wavelength spacing $d = \frac{\lambda}{2}$, where λ is the carrier wavelength. Additionally, we assume both Alice–Bob and Alice–Eve channels to be as linear with L-multipath, and write $\boldsymbol{c} = \{c_1, \dots, c_L\} \subset \mathbb{C}$ the channel coefficients, while $\boldsymbol{\tau} = \{\tau_1, \dots, \tau_L\} \subset \mathbb{T}$ encode the AoAs $\phi_\ell \in [-\frac{\pi}{2}, \frac{\pi}{2})$ through the relationship with $\tau_\ell = \frac{d\sin(\phi_\ell)}{\lambda} \in \mathbb{T}$.

To protect her physical location, we assume Alice to transmit fake signals—carrying no relevant information—, which are modeled on the receiver side as spurious paths parameterized by coefficients $\widetilde{\boldsymbol{c}}$ and angular mapping $\widetilde{\boldsymbol{\tau}}$. On either Bob or Eve's side, the received signal writes

$$\boldsymbol{y} = \mathbf{V}_0(\boldsymbol{\tau})\boldsymbol{c} + \mathbf{V}_0(\widetilde{\boldsymbol{\tau}})\widetilde{\boldsymbol{c}} + \boldsymbol{w}, \tag{3}$$

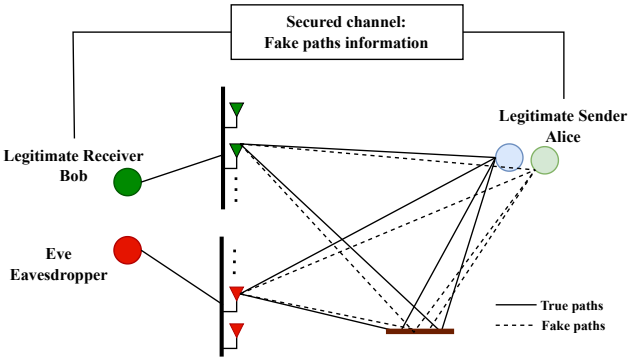

Figure 1. SIMO communication model with fake path injection

where $\boldsymbol{w} \sim \mathcal{CN}(\mathbf{0}, \eta^2\mathbf{I}_N)$ is noise which is assumed circularly symmetric complex Gaussian with covariance $\eta^2\mathbf{I}_N$. The SIMO parameters $\{\boldsymbol{c}, \boldsymbol{\tau}, \widetilde{\boldsymbol{c}}, \widetilde{\boldsymbol{\tau}}\}$ and the noise power η^2 in Equation (3) can be different for Bob and Eve. In the sequel, we discriminate Bob's and Eve's parameters with the subscripts "B" or "E", respectively, only when disambiguation is needed. In practice, fake paths can emerge from Alice's beamforming design [10], or from a third-party jammer cooperating with Alice.

To resolve the ambiguities introduced by faking the signal, we assume Alice and Bob can privately exchange securely at a low communication rate in a side channel that is not overheard by Eve. The studied setup assumes the transmission of the artificial fake paths' parameters $\{\widetilde{\boldsymbol{c}}, \widetilde{\boldsymbol{\tau}}\}$. Hence, Bob can remove the faked component from its received signal before estimating the true signal parameters, while Eve has to estimate both fake and true channel components, which is statistically harder. The system model is depicted in Figure 1.

Let us assume there is a secure channel so that Alice and Bob can share the artificial fake paths information $\{\widetilde{\boldsymbol{c}}, \widetilde{\boldsymbol{\tau}}\}$, then for Bob, the unknown parameters are the true channel coefficient $\boldsymbol{c}$ and the true AoAs $\boldsymbol{\tau}$.

B. Statistical Privacy Metric

Alice's physical location can be inferred by estimating the AoA's $\{\phi_\ell\}$, or equivalently the τ_ℓ's from the observation $\boldsymbol{y}$ given by Equation (3). As the columns of $\boldsymbol{V}_0(\boldsymbol{\tau})$ in (2) are complex exponential vectors, estimating the model parameters amounts to solving a *line spectral estimation* problem [17], [18], which is a fundamental signal processing primitive. The privacy of Alice's location can be assessed by the statistical accuracy Eve reaches in estimating the parameters $\{\boldsymbol{c}, \boldsymbol{\tau}\}$.

In this work, we measure privacy in terms of the eigenvalue gap between Bob's and Eve's Fisher information matrices (FIMs), and it is formally defined as follows.

Definition 1 (Statistical privacy)**.** *Assume a legitimate party Bob and an illegitimate party Eve attempt to estimate unknown parameters $\boldsymbol{\theta}$ under an observation $\boldsymbol{y}$, and write* $\mathbf{CRB}$ *the CRB matrix on $\boldsymbol{\theta}$ under observation $\boldsymbol{y}$. Given $\gamma \geq 1$, is it said*

that statistical privacy *is achieved with margin* γ *if*

$$\frac{\lambda_{\min}(\mathbf{CRB}_{\mathrm{E}}(\boldsymbol{\theta}_E))}{\lambda_{\max}(\mathbf{CRB}_{\mathrm{B}}(\boldsymbol{\theta}_B))} \geq \gamma. \tag{4}$$

Through the Cramér-Rao theorem, Definition 1 is met if the quadratic error achieved by an unbiased estimator in Eve's attempt to estimate *any linear form of the parameters* $\boldsymbol{\theta}_E$ is γ-times greater than Bob's error on *any other linear form of the parameters* $\boldsymbol{\theta}_B$. Hence, Definition 1 of statistical privacy is more stringent than requesting control of the quadratic error on one single parameter. Furthermore, larger values of the privacy margin γ imply greater privacy in the estimation task.

III. Main Results

This section presents results on the statistical privacy of fake path injection in the SIMO model presented in Section II. We start by introducing the *wrap-around distance* Δ, defined as the minimal distance over the torus between two distinct elements in $\boldsymbol{\tau}$, and the *inter-separation* δ, defined as Hausdorff distance between the true and the paths *i.e.*

$$\Delta = \Delta(\boldsymbol{\tau}) \triangleq \min_{\ell \neq \ell'} \inf_{j \in \mathbb{Z}} |\tau_\ell - \tau_{\ell'} + j| \tag{5a}$$

$$\delta = \delta(\boldsymbol{\tau}, \widetilde{\boldsymbol{\tau}}) \triangleq \max_{\ell, \ell'} \inf_{j \in \mathbb{Z}} |\tau_\ell - \widetilde{\tau}_{\ell'} + j| \,. \tag{5b}$$

The above metrics play a critical role in the stability of line spectrum estimation, and the convergence of numerical methods [19], [20].

In the sequel, statistical privacy is studied for two distinct scenarios. First, we study the CRB on $\boldsymbol{\tau}$ under the assumption that Bob and Eve know the channel coefficients $\{\boldsymbol{c}, \widetilde{\boldsymbol{c}}\}$. Second, we study the CRB on $\{\boldsymbol{\tau}, \boldsymbol{c}\}$ under the hypothesis that Bob Eve's is agnostic of any channel parameters.

A. Privacy on the Angle of Arrivals

We assume a simplified scenario where the channel coefficients $\{\boldsymbol{c}, \widetilde{\boldsymbol{c}}\}$ are known to both Bob and Eve. Hence Bob's only remaining unknown is $\{\boldsymbol{\tau}\}$, while Eve's unknowns are $\{\boldsymbol{\tau}, \widetilde{\boldsymbol{\tau}}\}$. We highlight assuming knowledge on the channel coefficients is *favorable* to Eve, and hence the current modeling is conservative for a privacy study. Theorem 2 presents desirable bounds on the extremal eigenvalue of Bob and Eve's CRB on the parameter $\boldsymbol{\tau}$ given measurement $\boldsymbol{y}$ of the form (3).

Theorem 2. *Assume* $\Delta_B \geq \frac{\pi^2}{N}$*, and* $\delta_E < \frac{\Delta_E}{2}$*. Then there exists a constant* $C > 0$ *such that*

$$\lambda_{\max}(\mathbf{CRB}_{\mathrm{B}}(\boldsymbol{\tau}_B)) \leq \frac{\pi^2}{3} \eta_B^2 N^2 \Big(1 - \pi^2 \left(N\Delta_B\right)^{-1}\Big)^{-1} \tag{6a}$$

$$\lambda_{\min}(\mathbf{CRB}_{\mathrm{E}}(\boldsymbol{\tau}_E)) \geq \frac{\eta_E^2}{4\delta_E^2} \left(\left| D_N^{(4)}(0) \right| + \frac{CN^4 \log\left(\frac{L}{2}\right)}{N\Delta_E \left(1 - \frac{2\delta}{\Delta_E}\right)} \right)^{-1}. \tag{6b}$$

Taking the quotient between the two quantities (6b) and (6a) immediately yield Corollary 3.

Corollary 3. *Under the assumption of Theorem 2 the SIMO communication model described in Section II is statistically private in the sense of Definition 1 with secrecy margin*

$$\gamma \geq \frac{3}{4\pi^2} \frac{\eta_E^2}{\eta_B^2} \left(N\delta_E\right)^{-2} \frac{\left| D_N^{(4)}(0) \right| + \frac{CN^4}{N\Delta_E \left(1 - \frac{2\delta_E}{\Delta_E}\right)} \log\left(\frac{L}{2}\right)}{1 - \pi^2 \left(N\Delta_B\right)^{-1}}. \tag{7}$$

where $C > 0$ *is the numerical constant of Theorem 2.*

Corollary 3 indicates that provided Bob perceives well-separated paths, the secrecy margin increases with the ratio between Eve's and Bob's noise levels and decreases as the distance between the true and the fake paths increases. Additionally, increasing the number of antennas N while maintaining $N\delta_E$ to a constant yields a polynomial increment in the privacy margin $\gamma = \mathcal{O}(N^4)$.

B. Channel Coefficients–AoAs Privacy

Herein is considered the generic case where both AoA and channel parameters are unknown. Since the vectors $\boldsymbol{c}$ and $\boldsymbol{\tau}$ are of different units, and since the statistical error of an estimator of $\boldsymbol{\tau}$ scales inversely proportional to N [15], we apply the normalization $u_\ell = \sqrt{-D_N''(0)}\tau_\ell$ and control the CRB on the set of parameter $\boldsymbol{\theta} = \{\boldsymbol{c}, \boldsymbol{u}\}$ instead. Bounds on the CRBs and the privacy margin are given in Theorem 4 and Corollary 5.

Theorem 4. *Assume* $\Delta_B \geq \frac{\pi^2}{N}$*, and* $\delta_E < \frac{\Delta_E}{2}$*. Then there exists two constants* $C, C' > 0$ *such that*

$$\lambda_{\max}(\mathbf{CRB}_{\mathrm{B}}(\boldsymbol{\theta}_B)) \leq \eta_B^2 \Big(1 - \pi^2 \left(N\Delta_B\right)^{-1}\Big)^{-1} \tag{8a}$$

$$\lambda_{\min}(\mathbf{CRB}_{\mathrm{E}}(\boldsymbol{\theta}_E)) \geq \frac{\eta_E^2 N^2}{4\delta_E^2} \left(C + \frac{C' \log\left(\frac{L}{2}\right)}{N\Delta_E \left(1 - \frac{2\delta_E}{\Delta_E}\right)} \right)^{-1}. \tag{8b}$$

Corollary 5. *Under the assumption of Theorem 4 the SIMO communication model described in Section II is statistically private in the sense of Definition 1 with secrecy margin*

$$\gamma \geq \frac{\eta_E^2}{4\eta_B^2} \left(N\delta_E\right)^{-2} \frac{CN^4 + \frac{C'N^4}{N\Delta_E \left(1 - \frac{2\delta_E}{\Delta_E}\right)} \log\left(\frac{L}{2}\right)}{1 - \pi^2 \left(N\Delta_B\right)^{-1}}, \tag{9}$$

where $C, C' > 0$ *are the numerical constants of Theorem 4.*

The trends on γ proposed by Corollary 5 is similar to that of Corollary 3, when channel coefficients are known.

IV. Proofs of Theorem 2 and Theorem 4

We present proof of the main results. Preliminary bounds on the Dirichlet kernel are given in IV-A, then Theorems 2 and 4 are demonstrated in Sections IV-B and IV-C.

A. Numerical Bounds on the Dirichlet Kernel

The next lemma proposes bounds for the infinite norm of matrices involving the Dirichlet kernel in their generic terms.

Lemma 6. *Let $\boldsymbol{\tau} \subset \mathbb{T}$ and $\widetilde{\boldsymbol{\tau}} \subset \mathbb{T}$ two sets of cardinality L, with maximal inter-separation δ as in* (5b)*. Let $\boldsymbol{G}_p$ the matrix with generic term, for $p \in \{0,1,2\}$,*

$$\boldsymbol{G}_p(i,j) = D_N^{(p)}(\tau_i-\tau_j)-D_N^{(p)}(\widetilde{\tau}_i-\tau_j)+D_N^{(p)}(\widetilde{\tau}_i-\widetilde{\tau}_j)-D_N^{(p)}(\tau_i-\widetilde{\tau}_j). \tag{10}$$

If $\delta < \frac{\Delta(\boldsymbol{\tau})}{2}$, then there exists constants $C_p \geq 0$ such that

$$\|\boldsymbol{G}_p\|_\infty \leq 4\delta^2 \left(\sup_{|\varepsilon|\leq 2\delta} \left| D_N^{(p+2)}(\varepsilon) \right| + \frac{C_p N^{p+2} \log\left(\frac{L}{2}\right)}{N\Delta(\boldsymbol{\tau})\left(1-\frac{2\delta}{\Delta(\boldsymbol{\tau})}\right)} \right). \tag{11}$$

Proof: First of all, applying Taylor's polynomial approximation with the assumption $|\tau_\ell - \widetilde{\tau}_\ell| \leq \delta$ yields

$$|\boldsymbol{G}_p(i,j)| \leq 4\delta^2 \sup_{|\varepsilon|\leq 2\delta} \left| D_N^{(p+2)}\left(\tau_i - \tau_j + \varepsilon\right) \right|. \tag{12}$$

Next, we claim the existence of constants $C_p \geq 0$ such that

$$\left| D_N^{(p+2)}(t) \right| \leq C_p N^{p+1} |t|^{-1}, \quad \forall t \in [-\frac{1}{2}, \frac{1}{2}),\ p \in \{0,1,2\}. \tag{13}$$

Similar bounds are studied in [14] for the derivatives up to the second order. Numerical experiments justify the following values of the constants, $C_0 = 5, C_1 = 16, C_2 = 50$. We fix the value of i. From the separation condition (5a), one can reorder the indexes without loss of generality, so that $0 \leq |j-i|\Delta(\boldsymbol{\tau}) \leq |\tau_i - \tau_j| \leq 1$ for all j. Therefore, Equations (12) and (13), and the decreasing of $|t|^{-1}$ over $[0, \frac{1}{2})$ induce

$$\begin{aligned}
\sum_{j=1}^{L} |\boldsymbol{G}_p(i,j)| &= |\boldsymbol{G}_p(i,i)| + \sum_{\substack{1\leq j\leq L \\ j\neq i}} |\boldsymbol{G}_p(i,j)| \\
&\leq 4\delta^2 \left(\sup_{|\varepsilon|\leq 2\delta} \left| D_N^{(p+2)}(\varepsilon) \right| + \sum_{\substack{1\leq j\leq L \\ j\neq i}} \sup_{|\varepsilon|\leq 2\delta} \left| D_N^{(p+2)}\left(\tau_i - \tau_j + \varepsilon\right) \right| \right) \\
&\leq 4\delta^2 \left(\sup_{|\varepsilon|\leq 2\delta} \left| D_N^{(p+2)}(\varepsilon) \right| + \sum_{\substack{1\leq j\leq L \\ j\neq i}} \sup_{|\varepsilon|\leq 2\delta} \frac{C_p N^{p+1}}{|\tau_i - \tau_j + \varepsilon|} \right) \\
&\leq 4\delta^2 \left(\sup_{|\varepsilon|\leq 2\delta} \left| D_N^{(p+2)}(\varepsilon) \right| + 2C_p N^{p+1} \sum_{k=1}^{\lceil \frac{L-1}{2} \rceil} \frac{1}{k\Delta - 2\delta} \right)
\end{aligned} \tag{14}$$

As the bound (14) holds independently of i, one may conclude on the desired result with the identity $\sum_{k=1}^{\lceil \frac{L-1}{2} \rceil} \frac{1}{k\Delta-2\delta} \leq \frac{1}{2\Delta(\boldsymbol{\tau})\left(1-\frac{2\delta}{\Delta(\boldsymbol{\tau})}\right)} \log\left(\frac{L}{2}\right) \leq$ for $\delta < \frac{\Delta(\boldsymbol{\tau})}{2}$. ∎

B. Proof of Theorem 2

We start by proving the bound (6a) for Bob's estimation of $\boldsymbol{\tau}$. As the fake paths parameters $\{\widetilde{\boldsymbol{c}}, \widetilde{\boldsymbol{\tau}}\}$ are communicated by Alice to Bob, and the channel coefficients $\boldsymbol{c}$ are assumed to be known, only $\boldsymbol{\tau}$ is left to be estimated to Bob. The FIM writes

$$\mathbf{J}_B(\boldsymbol{\tau}) = \eta^{-2} \operatorname{diag}(\boldsymbol{c})^{\mathsf{H}} \boldsymbol{V}_1(\boldsymbol{\tau})^{\mathsf{H}} \boldsymbol{V}_1(\boldsymbol{\tau}) \operatorname{diag}(\boldsymbol{c}), \tag{15}$$

which immediately implies through the relation $\mathbf{CRB}_{\mathrm{B}}(\boldsymbol{\tau}) = \boldsymbol{J}_B(\boldsymbol{\tau})^{-1}$, and with [16, Thm. 4], [21]

$$\begin{aligned}
\lambda_{\max}(\mathbf{CRB}_{\mathrm{B}}(\boldsymbol{\tau})) &= \lambda_{\min}(\boldsymbol{J}_B(\boldsymbol{\tau}))^{-1} \\
&\leq \eta^2 |c_{\min}|^{-2} \lambda_{\min}\left(\boldsymbol{V}_1(\boldsymbol{\tau})^{\mathsf{H}} \boldsymbol{V}_1(\boldsymbol{\tau})\right)^{-1} \\
&\leq \eta^2 |c_{\min}|^{-2} \frac{\pi^2}{3} N^2 \left(1 - \pi^2 (N\Delta)^{-1}\right)^{-1}.
\end{aligned} \tag{16}$$

Next, we demonstrate Eve's estimation bound (6b). As Eve is assumed to know the channel coefficients, her unknowns in the observation model (3) reduces to $\boldsymbol{\theta} = \{\boldsymbol{\tau}, \widetilde{\boldsymbol{\tau}}\}$, and her FIM on $\boldsymbol{\theta}$ under the observation $\boldsymbol{y}$ writes [22, Chapter 5]

$$\mathbf{J}_E(\boldsymbol{\theta}) = \eta^{-2} \operatorname{diag}(\boldsymbol{c}, \widetilde{\boldsymbol{c}})^{\mathsf{H}} \begin{bmatrix} \boldsymbol{V}_1(\boldsymbol{\tau})^{\mathsf{H}} \boldsymbol{V}_1(\boldsymbol{\tau}) & \boldsymbol{V}_1(\boldsymbol{\tau})^{\mathsf{H}} \boldsymbol{V}_1(\widetilde{\boldsymbol{\tau}}) \\ \boldsymbol{V}_1(\widetilde{\boldsymbol{\tau}})^{\mathsf{H}} \boldsymbol{V}_1(\boldsymbol{\tau}) & \boldsymbol{V}_1(\widetilde{\boldsymbol{\tau}})^{\mathsf{H}} \boldsymbol{V}_1(\widetilde{\boldsymbol{\tau}}) \end{bmatrix} \operatorname{diag}(\boldsymbol{c}, \widetilde{\boldsymbol{c}}). \tag{17}$$

The CRB matrix is given by inverse of (17). Schur's inversion formula yields [23]

$$\mathbf{CRB}_E(\boldsymbol{\theta}) = \eta^2 \operatorname{diag}(\boldsymbol{c}, \widetilde{\boldsymbol{c}})^{-1} \begin{bmatrix} \boldsymbol{M}^{-1} & * \\ * & \widetilde{\boldsymbol{M}}^{-1} \end{bmatrix} \operatorname{diag}(\boldsymbol{c}, \widetilde{\boldsymbol{c}})^{-\mathsf{H}} \tag{18}$$

with $\boldsymbol{M} = \boldsymbol{V}_1(\boldsymbol{\tau})^{\mathsf{H}} \boldsymbol{P}_1^{\perp}(\widetilde{\boldsymbol{\tau}}) \boldsymbol{V}_1(\boldsymbol{\tau})$, $\widetilde{\boldsymbol{M}} = \boldsymbol{V}_1(\widetilde{\boldsymbol{\tau}})^{\mathsf{H}} \boldsymbol{P}_1^{\perp}(\boldsymbol{\tau}) \boldsymbol{V}_1(\widetilde{\boldsymbol{\tau}})$, where $\boldsymbol{P}_1^{\perp}(\boldsymbol{\tau})$ and $\boldsymbol{P}_1^{\perp}(\widetilde{\boldsymbol{\tau}})$ are the projection matrices onto the orthogonal complement of the column space of $\boldsymbol{V}_1(\boldsymbol{\tau})$ and $\boldsymbol{V}_1(\widetilde{\boldsymbol{\tau}})$, respectively. Hence, Eve's CRB matrix on the AoA relevant parameters $\boldsymbol{\tau}$ satisfies

$$\begin{aligned}
\lambda_{\min}\left(\mathbf{CRB}_{\mathrm{E}}(\boldsymbol{\tau})\right) &= \lambda_{\min}\left(\eta^2 \operatorname{diag}(\boldsymbol{c})^{-\mathsf{H}} \boldsymbol{M}^{-1} \operatorname{diag}(\boldsymbol{c})^{-1}\right) \\
&\geq \eta^2 |c_{\max}|^{-2} \lambda_{\max}\left(\boldsymbol{M}\right)^{-1}
\end{aligned} \tag{19}$$

It remains to provide an upper bound on $\lambda_{\max}(\boldsymbol{M})$ to conclude. We let $\boldsymbol{V}_0(\boldsymbol{\tau}) = \boldsymbol{V}_0(\widetilde{\boldsymbol{\tau}}) + \boldsymbol{E}$. The expression of $\boldsymbol{M}$ reduces to

$$\boldsymbol{M} = \boldsymbol{E}^{\mathsf{H}} \boldsymbol{P}_1^{\perp}(\boldsymbol{\tau}) \boldsymbol{E}. \tag{20}$$

Next, by a direct calculation of the generic term $\boldsymbol{E}^{\mathsf{H}}\boldsymbol{E}$ reveals the identify $\boldsymbol{G}_2 = \boldsymbol{E}^{\mathsf{H}}\boldsymbol{E}$, where $\boldsymbol{G}_2$ is as in (10). Hence, by the contractivity of the orthogonal projection $\boldsymbol{P}_1^{\perp}(\boldsymbol{\tau})$ one as

$$\lambda_{\max}(\boldsymbol{M}) \leq \lambda_{\max}(\boldsymbol{E}^{\mathsf{H}}\boldsymbol{E}) = \lambda_{\max}(\boldsymbol{G}_2) \leq \|\boldsymbol{G}_2\|_\infty. \tag{21}$$

Combining (19) with (21) and applying Lemma 6 concludes on Inequation (6b). ∎

C. Proof of Theorem 4

First of all, we define by $\boldsymbol{W}(\boldsymbol{\tau})$ the concatenation $\boldsymbol{W}(\boldsymbol{\tau}) = \left[\boldsymbol{V}_0(\tau), \frac{1}{\sqrt{-D_N''(0)}} \boldsymbol{V}_1(\boldsymbol{\tau})\right]$. We structure the proof analogously to that of Theorem 2.

We start by considering Bob's case, for whom the unknowns are $\boldsymbol{\theta} = \{\boldsymbol{c}, \boldsymbol{u}\}$. The FIM writes

$$\mathbf{J}_B(\boldsymbol{\theta}) = \eta^{-2} \operatorname{diag}(\mathbf{1}, \boldsymbol{c})^{\mathsf{H}} \boldsymbol{W}(\boldsymbol{\tau})^{\mathsf{H}} \boldsymbol{W}(\boldsymbol{\tau}) \operatorname{diag}(\mathbf{1}, \boldsymbol{c}), \tag{22}$$

and one establishes (8a) with [16, Theorem 4], [21] with

$$\begin{aligned}\lambda_{\max}(\mathbf{CRB}_{\mathrm{B}}(\boldsymbol{\theta})) &= \lambda_{\min}(\boldsymbol{J}_B(\boldsymbol{\tau}))^{-1} \\ &\leq \eta^2|c_{\min}|^{-2}\lambda_{\min}\left(\boldsymbol{W}(\boldsymbol{\tau})^{\mathsf{H}}\boldsymbol{W}(\boldsymbol{\tau})\right)^{-1} \\ &\leq \eta^2|c_{\min}|^{-2}\left(1-\pi^2(N\Delta)^{-1}\right)^{-1}. \quad (23)\end{aligned}$$

As for Eve, her unknowns are $\bar{\boldsymbol{\theta}} = \{\boldsymbol{c}, \boldsymbol{u}, \widetilde{\boldsymbol{c}}, \widetilde{\boldsymbol{u}}\}$, and her CRB matrix writes [22, Chapter 5]

$$\mathbf{CRB}_E(\bar{\boldsymbol{\theta}}) = \eta^2 \mathrm{diag}(\boldsymbol{c}, \widetilde{\boldsymbol{c}})^{-1} \begin{bmatrix} \boldsymbol{N}^{-1} & * \\ * & \widetilde{\boldsymbol{N}}^{-1} \end{bmatrix} \mathrm{diag}(\boldsymbol{c}, \widetilde{\boldsymbol{c}})^{-\mathsf{H}} \quad (24)$$

with $\boldsymbol{N} = \boldsymbol{W}(\boldsymbol{\tau})^{\mathsf{H}}\widetilde{\boldsymbol{Q}}^{\perp}\boldsymbol{W}(\boldsymbol{\tau})$ and $\widetilde{\boldsymbol{N}} = \boldsymbol{W}(\widetilde{\boldsymbol{\tau}})^{\mathsf{H}}\widetilde{\boldsymbol{Q}}^{\perp}\boldsymbol{W}(\widetilde{\boldsymbol{\tau}})$, and where $\boldsymbol{Q}^{\perp}$ and $\widetilde{\boldsymbol{Q}}^{\perp}$ are the projection matrices onto the orthogonal complement of the column space of $\boldsymbol{W}(\boldsymbol{\tau})$ and $\boldsymbol{W}(\widetilde{\boldsymbol{\tau}})$, respectively. Hence Eve's CRB on the partial set of relevant parameter $\boldsymbol{\theta} = \{\boldsymbol{c}, \boldsymbol{u}\}$ can be lower bounded by

$$\begin{aligned}\lambda_{\min}\left(\mathbf{CRB}_{\mathrm{E}}(\boldsymbol{\theta})\right) &= \lambda_{\min}\left(\eta^2\,\mathrm{diag}(\boldsymbol{c})^{-1}\boldsymbol{N}^{-1}\,\mathrm{diag}(\boldsymbol{c})^{-\mathsf{H}}\right) \\ &\geq \eta^2|c_{\max}|^{-2}\lambda_{\max}\left(\boldsymbol{N}\right)^{-1}. \quad (25)\end{aligned}$$

It remains to upper bounding $\lambda_{\max}(\boldsymbol{N})$ to conclude. We let $\boldsymbol{W}(\boldsymbol{\tau}) = \widetilde{\boldsymbol{W}}(\widetilde{\boldsymbol{\tau}}) + \boldsymbol{F}$. The expression of $\boldsymbol{M}$ reduces to

$$\boldsymbol{M} = \boldsymbol{F}^{\mathsf{H}}\widetilde{\boldsymbol{P}}^{\perp}\boldsymbol{F}. \quad (26)$$

A direct calculation of the generic term of $\boldsymbol{F}^{\mathsf{H}}\boldsymbol{F}$ yields the block decomposition

$$\boldsymbol{F} = \begin{bmatrix} \boldsymbol{G}_0 & \frac{1}{\sqrt{-D_N''(0)}}\boldsymbol{G}_1 \\ \frac{1}{\sqrt{-D_N''(0)}}\boldsymbol{G}_1^{\mathsf{H}} & -\frac{1}{D_N''(0)}\boldsymbol{G}_2 \end{bmatrix} \quad (27)$$

where $\boldsymbol{G}_p$ are the matrices defined in (10), $p \in \{0,1,2\}$. Furthermore, since $\boldsymbol{P}^{\perp}$ is an orthogonal projection, it is contractive.

$$\begin{aligned}\lambda_{\max}(\boldsymbol{N}) \leq \lambda_{\max}(\boldsymbol{F}^{\mathsf{H}}\boldsymbol{F}) &\leq \left\|\boldsymbol{F}^{\mathsf{H}}\boldsymbol{F}\right\|_{\infty} \\ &\leq \max\left\{\|\boldsymbol{G}_0\|_{\infty} + \frac{1}{\sqrt{-D_N''(0)}}\|\boldsymbol{G}_1\|_{\infty}, \right. \\ &\qquad \left. \frac{1}{\sqrt{-D_N''(0)}}\|\boldsymbol{G}_1\|_{\infty} - \frac{1}{D_N''(0)}\|\boldsymbol{G}_2\|_{\infty}\right\}. \quad (28)\end{aligned}$$

Combining (25) with (28) and applying Lemma 6 concludes on Inequation (6b). ∎

V. Numerical Experiments

We provide numerical insight on the results presented in Section III. We assume Bob and Eve have $N = 31$ antennas, $L = 5$ true paths with equispaced AoAs for both Bob and Eve in the parameter space, that is $\Delta_B = \Delta_E = 1/L$. The SNR is defined as $\mathsf{SNR} = \|\boldsymbol{V}_0(\boldsymbol{\tau})\|_2^2 / \|\boldsymbol{w}\|_2^2$, and we set $\mathsf{SNR}_B = \mathsf{SNR}_E = 0\mathrm{dB}$. We consider the scenario described in Section III-A, where the channel coefficients are assumed to be known to both Bob and Eve.

Figure 2 pictures the theoretical bounds on Bob's and Eve's CRBs established in Theorem 2 as a function of the ratio δ_E/Δ_E. A comparison is made with the numerical realization of the CRB for the random realization of the fake paths while ensuring $|\widetilde{\boldsymbol{\tau}}_\ell - \boldsymbol{\tau}_\ell| \leq \delta$ of all paths $\ell \in \{1,\dots,L\}$. The histogram of the empirical realization of $\lambda_{\min}(\mathbf{CRB}_{\mathrm{E}}(\boldsymbol{\theta}_E))$ as well as its extremal value is display. Also there is a gap, between the theoretical and realized bound on Eve's CRB—possibly due to the coarse majoration in Lemma 6—, the tend is captured by our theoretical predictions.

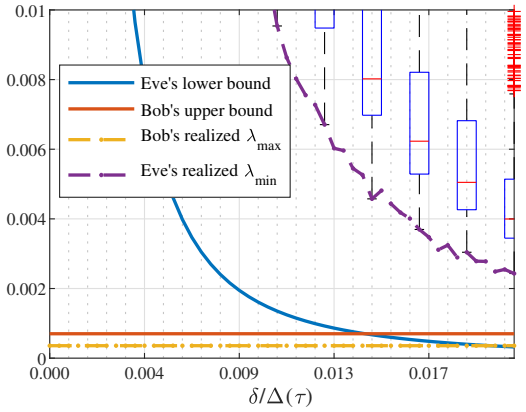

Figure 2. Theoretical and realized extremal values of Bob's and Eve's CRB, case of known channel coefficients.

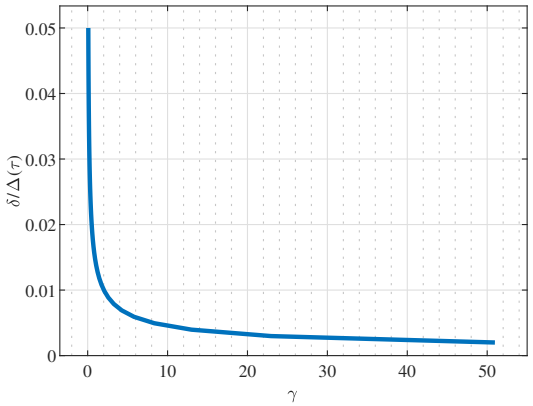

Figure 3. Fake path separation needed to achieve a target secrecy margin γ, case of known channel coefficients.

Figure 3 shows the ratio $\frac{\delta_E}{\Delta_E}$ that is requested to achieve a given secrecy margin γ, which corroborates with Corollary 3.

VI. Conclusion

In this work, we proposed a novel scheme to induce the location privacy of a transmitter in a SIMO multipath communication paradigm. Privacy is achieved through the injection of fake paths, whose parameters are secretly shared between Alice and Bob over a secure side channel. Privacy is assessed in our framework by a novel statistical metric on the extremal eigenvalues of Bob's and Eve's CRB on the true path parameters. The privacy enhancements are backed by theoretical guarantees and mainly depend on the angular distance between the true and the fake paths under Eve's perspective.

We leave for future work a sharpening of the proposed bounds, and possible extension of the framework in the more general context of MIMO communication.

References

[1] H. Jiang, J. Li, P. Zhao, F. Zeng, Z. Xiao, and A. Iyengar, "Location privacy-preserving mechanisms in location-based services: A comprehensive survey", *ACM Comput. Surv.*, vol. 54, no. 1, Jan. 2021.

[2] S. Farhang, Y. Hayel, and Q. Zhu, "Phy-layer location privacy-preserving access point selection mechanism in next-generation wireless networks", in *2015 IEEE Conference on Communications and Network Security (CNS)*, 2015, pp. 263–271.

[3] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise", *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[4] S. Oh, T. Vu, M. Gruteser, and S. Banerjee, "Phantom: Physical layer cooperation for location privacy protection", in *2012 Proceedings IEEE INFOCOM*, 2012, pp. 3061–3065.

[5] W. Wang, Y. Chen, and Q. Zhang, "Privacy-preserving location authentication in Wi-Fi networks using fine-grained physical layer signatures", *IEEE Transactions on Wireless Communications*, vol. 15, no. 2, pp. 1218–1225, 2016.

[6] J. J. Checa and S. Tomasin, "Location-privacy-preserving technique for 5G mmWave devices", *IEEE Communications Letters*, vol. 24, no. 12, pp. 2692–2695, 2020.

[7] S. Tomasin, "Beamforming and artificial noise for cross-layer location privacy of e-health cellular devices", in *2022 IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2022, pp. 568–573.

[8] R. Ayyalasomayajula, A. Arun, W. Sun, and D. Bharadia, "Users are closer than they appear: Protecting user location from WiFi APs", in *Proceedings of the 24th International Workshop on Mobile Computing Systems and Applications*, Newport Beach, California: Association for Computing Machinery, 2023, pp. 124–130.

[9] J. Li and U. Mitra, "Channel state information-free artificial noise-aided location-privacy enhancement", in *ICASSP 2023 - 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2023, pp. 1–5.

[10] J. Li and U. Mitra. "Channel state information-free location-privacy enhancement: Fake path injection". arXiv: 2307.05442 [eess]. (Jul. 11, 2023), preprint.

[11] Ø. Ryan and M. Debbah, "Asymptotic behavior of random Vandermonde matrices with entries on the unit circle", *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3115–3147, 2009.

[12] C. Aubel and H. Bölcskei, "Vandermonde matrices with nodes in the unit disk and the large sieve", *Applied and Computational Harmonic Analysis*, vol. 47, no. 1, pp. 53–86, 2019.

[13] D. Batenkov, L. Demanet, G. Goldman, and Y. Yomdin, "Conditioning of partial nonuniform Fourier matrices with clustered nodes", *SIAM Journal on Matrix Analysis and Applications*, vol. 41, no. 1, pp. 199–220, 2020.

[14] S. Kunis and D. Nagel, "On the condition number of Vandermonde matrices with pairs of nearly-colliding nodes", *Numerical Algorithms*, vol. 87, no. 1, pp. 473–496, May 2021.

[15] M. Ferreira Da Costa and U. Mitra, "On the stability of super-resolution and a Beurling–Selberg type extremal problem", in *2022 IEEE International Symposium on Information Theory (ISIT)*, 2022, pp. 1737–1742.

[16] M. Ferreira Da Costa, "Second-order Beurling approximations and super-resolution from bandlimited functions", in *2023 International Conference on Sampling Theory and Applications (SampTA)*, IEEE, 2023, pp. 1–5.

[17] S. M. Kay and S. L. Marple, "Spectrum analysis—a modern perspective", *Proceedings of the IEEE*, vol. 69, no. 11, pp. 1380–1419, 1981.

[18] H. Krim and M. Viberg, "Two decades of array signal processing research: The parametric approach", *IEEE signal processing magazine*, vol. 13, no. 4, pp. 67–94, 1996.

[19] A. Moitra, "Super-resolution, extremal functions and the condition number of Vandermonde matrices", in *Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing*, New York, NY, USA, 2015, pp. 821–830.

[20] M. Ferreira Da Costa and W. Dai, "A tight converse to the spectral resolution limit via convex programming", in *2018 IEEE International Symposium on Information Theory (ISIT)*, 2018, pp. 901–905.

[21] M. Ferreira Da Costa, "The condition number of weighted non-harmonic Fourier matrices with applications to super-resolution", working paper or preprint, Oct. 2023.

[22] H. L. Van Trees, K. L. Bell, and Z. Tian, *Detection Estimation and Modulation Theory, Part I: Detection, Estimation, and Filtering Theory, 2nd Edition*. John Wiley & Sons, 2013.

[23] L. L. Scharf and L. McWhorter, "Geometry of the Cramér-Rao bound", *Signal Processing*, vol. 31, no. 3, pp. 301–311, 1993.