Securing Channel State Information via Fake Path Injection in SIMO Communication

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

Securing Channel State Information via Fake Path Injection in SIMO Communication

Tran Trong Duy
duytt@vnu.edu.vn
AVITECH, VNU University of Engineering and Technology
Hanoi, Vietnam

Maxime Ferreira Da Costa
maxime.ferreira@centralesupelec.fr
L2S, CNRS, CentraleSupélec, Université Paris–Saclay
Gif-sur-Yvette, France

Nguyen Linh Trung
linhtrung@vnu.edu.vn
AVITECH, VNU University of Engineering and Technology
Hanoi, Vietnam

ABSTRACT

Fake path injection is a new promising scheme for location privacy at the physical layer. Theoretical aspects of fake path injection in single-input multiple-output (SIMO) communication are studied. A novel bound on the largest eigenvalue of the Fisher information matrix for an eavesdropper to estimate the channel coefficients is derived as a function of the distance between the true and the fake paths. This result guarantees communication privacy in a statistical sense and is demonstrated by harnessing the spectral properties of Vandermonde matrices and of the Dirichlet kernel. This auspicious preliminary result encourages further investigation of the fake path injection scheme for SIMO communication in particular, and in general, MIMO communication.

KEYWORDS

Information Theory, Physical Layer Security, Array Processing

1 INTRODUCTION

With the development of technologies, the number of embedded or consumer electronic devices carried by individuals is increasing. These devices grant access to a huge number of services, many of them location-based, with an increasing risk of location data breaches. As important personal information can be inferred from location data, such as health, social relationships, and identity [2, 6], location privacy is of utmost importance. Nonetheless, location access and sharing must be tackled at different levels, namely: user devices, positioning systems, communication networks, and location-based service servers [6]. Location privacy has been studied at different layers of a communication system; however, most of them concern higher levels, such as the application or the network layers. Physical layer security remains a major challenge due to the broadcast nature of the wireless medium, calling for a surge of interest in research.

Inspired by the work of Li and Mitra [8] on *fake path injection*, we study in this work the theoretical guarantee of location privacy for single-input multiple-output (SIMO) communication using fake path injection. More precisely, we derive bounds on the estimation error of the channel coefficients by the legitimate receiver (Bob) and an eavesdropper (Eve). The proposed statistical bounds are based on recent advances in the stability of the super-resolution problem [9, 5], and on the condition number of Vandermonde matrices with nodes on the unit circle [1, 3, 7, 4]. We compare our bound with the existing bound in the literature to show a gap in theoretical performance between legitimate and illegitimate receivers. More precisely, we show fake path injection can create a gap between the spectra of Bob's and Eve's Fisher information matrices (FIM) in estimating the channel state information, demonstrating the benefits of this security scheme. Furthermore, numerical evidence of our theoretical findings is proposed.

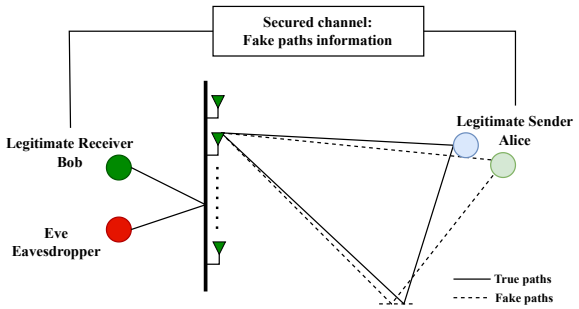

Figure 1: SIMO communication model with fake paths.

2 PROBLEM FORMULATION

We consider localization in SIMO communication as depicted in Figure 1, in which Alice sends pilot signals over a wireless medium to Bob while Eve attempts to estimate the channel state information to infer Alice's location illegally. To protect her location, Alice injects fake paths into the channel in such a way that their angles of arrival (AoAs) are close to those of the true paths under Eve's perspective. We write $\boldsymbol{c} = [c_1, \ldots, c_L]^\top \in \mathbb{C}^L$, and $\widetilde{\boldsymbol{c}}$ the channel is the channel coefficients associated to the true and fake paths, respectively, while $\boldsymbol{\tau}, \widetilde{\boldsymbol{\tau}} \subset [0, 1)$ encodes the angles of arrival of the true and fake paths. After removing the effect of the pilot, assuming Eve's linear array as N antennas, the received signal is

$$\bar{\boldsymbol{y}} = \mathbf{V}_0(\boldsymbol{\tau})\boldsymbol{c} + \mathbf{V}_0(\widetilde{\boldsymbol{\tau}})\widetilde{\boldsymbol{c}} + \boldsymbol{w}, \tag{1}$$

where $\boldsymbol{w} \sim \mathcal{CN}(\mathbf{0}, \eta^2\mathbf{I}_N)$ is circularly symmetric complex Gaussian noise, and $\boldsymbol{V}_0(\boldsymbol{\tau})$ is a Vandermonde matrix whose i-th column is $\boldsymbol{v}_0(\tau_i) = \frac{1}{\sqrt{N}}\left[e^{-i2\pi(-n)\tau_i}, \ldots, e^{i2\pi n\tau_i}\right]^\top$. Additionally, we denote $\Delta(\boldsymbol{\tau}) \triangleq \min_{\ell\neq\ell'} \inf_{j\in\mathbb{Z}} |\tau_\ell - \tau_{\ell'} + j|$ to smallest distance between distinct elements in $\boldsymbol{\tau}$, and $\delta = \max_{\ell,\ell'} \inf_{j\in\mathbb{Z}} |\tau_\ell - \widetilde{\tau}_{\ell'} + j|$ the largest distance between the elements of $\boldsymbol{\tau}$ and $\widetilde{\boldsymbol{\tau}}$.

In this work, we discuss Bob's and Eve's capability of estimating the true channel coefficients $\boldsymbol{c}$, as they contain valuable information on Alice's location. We assess communication privacy in terms of the hardness of this estimation problem. Our model assumes that Bob gets full knowledge of the fake path parameters $\widetilde{\boldsymbol{c}}$ and $\widetilde{\boldsymbol{\tau}}$ via a separate secure channel. In this setup, we say that the communication is *secure in the statistical sense* when

$$\lambda_{\max}(\mathbf{J}_{Eve}(\boldsymbol{c})) < \lambda_{\min}(\mathbf{J}_{Bob}(\boldsymbol{c})) \tag{2}$$

where $\mathbf{J}_{Bob}(\boldsymbol{c})$ and $\mathbf{J}_{Eve}(\boldsymbol{c})$ are Bob's and Eve's FIM on $\boldsymbol{c}$.

3 ESTIMATION BOUNDS ON THE CHANNEL

In Bob's perspective, the FIM writes $\mathbf{J}_{Bob}(\boldsymbol{c}) = \eta^{-2}\boldsymbol{V}_0(\boldsymbol{\tau})\mathrm{H}\boldsymbol{V}_0(\boldsymbol{\tau})$ [11, Chapter 5], and one has a bound on its smallest eigenvalue as [1, 5]

$$\lambda_{\min}(\mathbf{J}_{Bob}(\boldsymbol{c})) \geq \eta^{-2}\left(1 - \frac{1}{N\Delta(\boldsymbol{\tau})}\right). \tag{3}$$

In Eve's perspective, assuming she knows the AoA's $\{\boldsymbol{\tau}, \widetilde{\boldsymbol{\tau}}\}$— which is favorable to the eavesdropper—, the unknowns are $\{\boldsymbol{c}, \widetilde{\boldsymbol{c}}\}$, yielding the FIM

$$\mathbf{J}_{Eve}(\boldsymbol{c}, \widetilde{\boldsymbol{c}}) = \eta^{-2}\begin{bmatrix} \boldsymbol{V}_0(\boldsymbol{\tau})^{\mathrm{H}}\boldsymbol{V}_0(\boldsymbol{\tau}) & \boldsymbol{V}_0(\boldsymbol{\tau})^{\mathrm{H}}\boldsymbol{V}_0(\widetilde{\boldsymbol{\tau}}) \\ \boldsymbol{V}_0(\widetilde{\boldsymbol{\tau}})^{\mathrm{H}}\boldsymbol{V}_0(\boldsymbol{\tau}) & \boldsymbol{V}_0(\widetilde{\boldsymbol{\tau}})^{\mathrm{H}}\boldsymbol{V}_0(\widetilde{\boldsymbol{\tau}}) \end{bmatrix}, \tag{4}$$

As $\widetilde{\boldsymbol{c}}$ caries to relevant information, Eve's restricts her estimation on $\boldsymbol{c}$, and the restricted FIM on $\boldsymbol{c}$ is given by [10]

$$\mathbf{J}'_{Eve}(\boldsymbol{c}) = \eta^{-2}\boldsymbol{V}_0(\boldsymbol{\tau})^{\mathrm{H}}(\boldsymbol{I} - \boldsymbol{P}_{\widetilde{\boldsymbol{V}}_0})\boldsymbol{V}_0(\boldsymbol{\tau}), \tag{5}$$

where $\boldsymbol{P}_{\widetilde{\boldsymbol{V}}_0} = \widetilde{\boldsymbol{V}}_0\left(\widetilde{\boldsymbol{V}}_0^{\mathrm{H}}\widetilde{\boldsymbol{V}}_0\right)^{-1}\widetilde{\boldsymbol{V}}_0^{\mathrm{H}}$ is the orthogonal projection on the column space of $\widetilde{\boldsymbol{V}}_0$.

Theorem 1 provides an upper bound on the largest eigenvalues of Eve's restricted FIM (5). The bound increases quadratically in the distance between the true and fake paths δ, and is hyperbolic in Δ. This highlights the need for small path separation δ of the effectiveness of fake path injection methods and corroborates with the findings in [8].

Theorem 1 (Upper bound on Eve for estimation of channel coefficients). *Assume $\Delta > \frac{1}{N}$ and $4\delta < \Delta$, then there exist $C > 0$ such that*

$$\lambda_{\max}(\mathbf{J}'_{Eve}(\boldsymbol{c})) \leq 4\,(N\delta)^2\left(\frac{\pi^2}{3} + \frac{\pi^2\ln(L) + C}{N\Delta}\right), \tag{6}$$

A sketch proof of Theorem 1 is provided in the rest of this section.

Proof: Let $\boldsymbol{E} = \boldsymbol{V}_0(\boldsymbol{\tau}) - \boldsymbol{V}_0(\widetilde{\boldsymbol{\tau}})$ and $\boldsymbol{F} = \boldsymbol{E}^{\mathrm{H}}\boldsymbol{E}$. We can write $\mathbf{J}'_{Eve}(\boldsymbol{c}) = \eta^{-2}\boldsymbol{E}^{\mathrm{H}}(\boldsymbol{I} - \boldsymbol{P}_{\widetilde{\boldsymbol{V}}_0})\boldsymbol{E}$. As $\lambda_{max}(\boldsymbol{E}^{\mathrm{H}}\boldsymbol{E})$ is contractive, it yields

$$\lambda_{\max}(\mathbf{J}'_{Eve}(\boldsymbol{c})) = \eta^{-2}\lambda_{\max}(\boldsymbol{E}^{\mathrm{H}}(\boldsymbol{I}-\boldsymbol{P}_{\widetilde{\boldsymbol{V}}_0})\boldsymbol{E}) \leq \eta^{-2}\lambda_{\max}(\boldsymbol{F}) \leq \eta^{-2}\,\|\boldsymbol{F}\|_\infty\,. \tag{7}$$

For $N = 2n+1$, we let $D_N(\cdot)$ the Dirichlet kernel of order N defined by $D_N(t) = \frac{1}{N}\sum_{k=-n}^{n} e^{i2\pi kt}$, which is an infinitely differentiable function, with second derivative bounded by [7]

$$|D''_N(t)| \leq N^2\left(\frac{\pi^2}{2N|t|} + \frac{\pi}{N^2|t|^2} + \frac{1}{N^3|t|^3}\right) \text{ for } -\frac{1}{2} \leq t \leq \frac{1}{2}. \tag{8}$$

We control $\|\boldsymbol{F}\|_\infty$ from the expression of its generic term, Taylor's polynomial approximation, and (8) as follows

$$\begin{aligned}
\left|F_{i,j}\right| &= \left|D_N(\tau_i - \tau_j) - D_N(\widetilde{\tau}_i - \tau_j) + D_N(\widetilde{\tau}_i - \widetilde{\tau}_j) - D_N(\tau_i - \widetilde{\tau}_j)\right| \\
&\leq 4\delta^2\left[\sup_{|\varepsilon|\leq 2\delta}|D''_N(\tau_i - \tau_j + \varepsilon)|\right] \\
&\leq 4(N\delta)^2\left(\frac{\pi^2}{2N(|\tau_i - \tau_j| - 2\delta)} + \frac{\pi}{N^2(|\tau_i - \tau_j| - 2\delta)^2}\right. \\
&\qquad \left. + \frac{1}{N^3(|\tau_i - \tau_j| - 2\delta)^3}\right), \qquad \forall i \neq j.
\end{aligned} \tag{9}$$

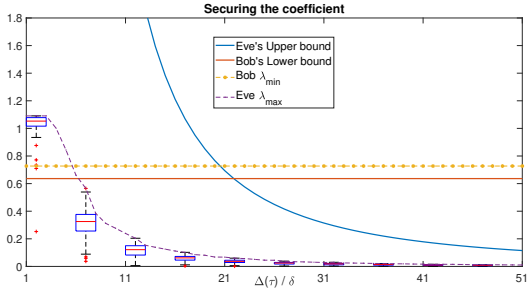

Figure 2: Theoretical and empirical realizations of extremal eigenvalues of Alice's and Bob's FIM, $L = 4$, $\Delta(\boldsymbol{\tau}) = 1/L$

Consider i is fixed. Up to a reordering to the j's indices, since the derivatives of Dirichlet kernel are 1-periodic, one may assume $|\tau_i - \tau_j| \geq |j-i|\Delta(\boldsymbol{\tau})$. Exploiting the decreasing of the majorant in (9), $|D''_N(0)| \leq \frac{\pi^2}{3}N^2$ and the harmonic progression bound yields

$$\begin{aligned}
\|\boldsymbol{F}\|_\infty &= \max_i\left\{|F_{i,i}| + \sum_{j\neq i}|F_{i,j}|\right\} \leq 4\delta^2\left(|D''_N(0)| + \sum_{j\neq i}|D''_N(\tau_i - \tau_j)|\right) \\
&\leq 4\,(N\delta)^2\left(\frac{\pi^2}{3} + \frac{\pi^2\ln(L) + 2\pi^2 + 2\pi s_2 + 2s_3}{N\Delta}\right),
\end{aligned} \tag{10}$$

where $s_p = \sum_{j=1}^{\infty}(j - \frac{1}{2})^{-p} < \infty$ for $p = 2, 3$. One concludes by substituting (10) on (7) on the result with $C = 2\pi^2 + 2\pi s_2 + 2s_3$ □.

4 EXPERIMENTS

We set the number of antennas for Bob and Eve $N = 11$, the number of paths $L = 4$, and the AoAs to be maximally separated, *i.e.* $\Delta(\boldsymbol{\tau}) = 1/L$. A visualization of the theoretical bounds (3) and (6) for Bob and Eve is shown in Figure 2, and compared with the empirical realization of the extremal eigenvalues of Bob's and Eve's FIMs. Eve's empirical realizations are computed by randomizing the fake paths such that $|\boldsymbol{\tau}_i - \widetilde{\boldsymbol{\tau}}_i| \leq \delta$. For clarity, we only show the maximum among all realizations of the largest eigenvalue of Eve and their distribution at certain ratios. One can see that the empirical upper bound on Eve's largest eigenvalue goes to zero at a quadratic rate as the ratio increases, corroborating with the trend predicted by Theorem 1. In this setup, when $\Delta(\boldsymbol{\tau})/\delta > 22$, one can theoretically guarantee the privacy of the communication in a statistical sense.

5 CONCLUSION

In this paper, we proved fake path injection could secure the channel coefficients in a statistical sense in SIMO communication when the fake paths perceived by Eve are close enough to the true ones. To that end, we provided novel bounds for Bob's smallest eigenvalue and Eve's largest eigenvalue of their respective FIM on the channel coefficients when a pilot sequence is sent.

For future work, we would like to extend our results for the privacy of the AoAs, as they also convey information on Alice's location. Furthermore, extending the privacy guarantees of fake path injection in the more generic context of MIMO communication would be a significant leap in the scheme's applicability to modern communication systems.

REFERENCES

[1] Céline Aubel and Helmut Bölcskei. "Vandermonde matrices with nodes in the unit disk and the large sieve". In: *Applied and Computational Harmonic Analysis* 47.1 (2019), pp. 53–86.

[2] Roshan Ayyalasomayajula et al. "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*. HotMobile '23. Newport Beach, California: Association for Computing Machinery, 2023, pp. 124–130. DOI: 10.1145/3572864.3580345.

[3] Dmitry Batenkov et al. "Conditioning of Partial Nonuniform Fourier Matrices with Clustered Nodes". In: *SIAM Journal on Matrix Analysis and Applications* 41.1 (2020), pp. 199–220. DOI: 10.1137/18M1212197.

[4] Maxime Ferreira Da Costa. *The condition number of weighted non-harmonic Fourier matrices with applications to super-resolution*. Oct. 2023. hal: hal-04261330. URL: https://hal.science/hal-04261330. preprint.

[5] Maxime Ferreira Da Costa and Urbashi 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. DOI: 10.1109/ISIT50566.2022.9834831.

[6] Hongbo Jiang et al. "Location Privacy-Preserving Mechanisms in Location-Based Services: A Comprehensive Survey". In: *ACM Comput. Surv.* 54.1 (Jan. 2021). ISSN: 0360-0300. DOI: 10.1145/3423165. URL: https://doi.org/10.1145/3423165.

[7] Stefan Kunis and Dominik Nagel. "On the condition number of Vandermonde matrices with pairs of nearly-colliding nodes". In: *Numerical Algorithms* 87.1 (May 2021), pp. 473–496. ISSN: 1572-9265. DOI: 10.1007/s11075-020-00974-x. URL: https://doi.org/10.1007/s11075-020-00974-x.

[8] Jianxiu Li and Urbashi Mitra. *Channel State Information-Free Location-Privacy Enhancement: Fake Path Injection*. July 11, 2023. arXiv: 2307.05442 [eess.SP]. URL: https://arxiv.org/abs/2307.05442. preprint.

[9] Ankur 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*. STOC '15. Portland, Oregon, USA: Association for Computing Machinery, 2015, pp. 821–830. ISBN: 9781450335362. DOI: 10.1145/2746539.2746561.

[10] Louis L. Scharf and L. Todd McWhorter. "Geometry of the Cramer-Rao bound". In: *Signal Processing* 31.3 (1993), pp. 301–311.

[11] Harry L. Van Trees, Kristine L. Bell, and Zhi Tian. *Detection Estimation and Modulation Theory, Part I: Detection, Estimation, and Filtering Theory, 2nd Edition*. John Wiley & Sons, 2013.