

Enhancing Secret Key Generation in Low-Mobility Scenarios by Locally Generated Pilots

Thuy M. Pham^{*}, Arsenia Chorti[‡], Gerhard P. Fettweis^{*,†}, Rafael F. Schaefer^{*,†}

^{*} Barkhausen Institut, Dresden, Germany

[†] Technische Universität Dresden, Germany & BMFTR Research Hub 6G-life & Cluster of Excellence CeTI

[‡] ETIS UMR 8051, CYU, ENSEA, CNRS, Cergy, France

{minhthuy.pham, rafael.schaefer, gerhard.fettweis}@barkhauseninstitut.org, arsenia.chorti@ensea.fr

Abstract—In this paper, we study the performance of a practical secret key generation method under low-mobility scenarios. Instead of relying on traditional cryptographic methods or leveraging spatial diversity and reconfigurable intelligent surfaces to increase channel variations, we utilize locally generated pilots to add randomness to the system, thus in turn helping to increase the secret key rate. The results demonstrate significant improvements over the original channels, whose entropy source mainly relies on mobility and channel variations. More importantly, this scheme works well without extra helpers or multiple antennas, thus providing a potential for developing reliable, lightweight security solutions for resource-constrained devices in practice.

Index Terms—Secret key generation, static, mobility, pilots, randomness.

I. INTRODUCTION

Wireless Internet of Things (IoT) devices are expected to be integrated massively into 5G networks and beyond, thus introducing significant security challenges due to the open nature of wireless communication channels. The traditional cryptographic methods relying on computational security are unsuitable for these resource-constrained devices. Therefore, physical layer security (PLS) exploits wireless channels' inherent randomness and unique characteristics to enhance security, providing a promising alternative [1].

PLS mechanisms can generally be categorized into keyless and key-based approaches. Keyless methods often utilize wiretap coding, where the design of codes and channel properties are exploited to secure the systems [2]–[7]. It is important to note that this approach typically relies on knowledge of the eavesdroppers' channel and noise, which is not always obtainable. In contrast, key-based methods focus on generating secret keys by utilizing the reciprocity and randomness inherent in wireless channels [8]–[13], making them a potentially lightweight security option for resource-constrained systems. The secret key generation (SKG) schemes have demonstrated superior performance in dynamic environments [14], [15], where the changes in channel coefficients are sufficient due to user mobility and environmental factors.

However, in less dynamic scenarios with no or low mobility, such as wireless sensor networks and many IoT settings, the secret key rate is very minimal or even zero due to a

lack of channel variations, posing a significant challenge for the deployment of SKG in practice. To tackle those issues, several approaches have been proposed to introduce additional randomness into the system [16]–[19]. For instance, in [16], spatial diversity through random beamforming was utilized to enhance channel variations. Similarly, in [17] the authors explored a rotation-based technique taking the random rotation of antennas into account to generate random phases. However, these multi-antenna strategies may not be feasible or efficient for low-cost sensors or IoT devices. Other investigations in the literature have studied the use of extra helpers, such as relays or reflecting intelligent surfaces (RIS), to introduce randomness [18], however their reliability is a concern. Recently, there has been interest in the pilot randomization technique, which helps to increase the secret key rate without any helpers [20], [21]. In [21], the authors also proved that this scheme can work well, even without multiple antennas. However, the performance of this scheme in practice remains an open problem. In addition, the impact of mobility on the system is also not well-studied.

In this paper, we investigate the performance of the randomization scheme proposed in [21] in a low-mobility scenario, which is a valid scenario for many IoT/robot-based systems. More specifically, the dataset recorded by Nokia is utilized to model low-mobility scenarios [22], in which each entity is equipped with a single antenna. We have also studied the impact of strong line-of-sight and non-line-of-sight scenarios on the performance. By considering different scenarios and varying combinations of randomization schemes for pilot signals, we have demonstrated a significant gain in terms of secret key rate in comparison with the original channels, where the source of entropy mainly comes from the channel variations and the mobility. Since the approach does not require multiple antennas or extra helpers, it is of practical relevance and has potential for a practical PLS.

The remainder of the paper is organized as follows: Section II presents the key concept of the pilot randomization technique. Section III models the evaluation scenario and presents the numerical results. Finally, Section IV summarizes the key findings and conclusions.

II. SKG BY LOCALLY GENERATED PILOTS

In this section, we briefly introduce an approach to enhance the secret key rate [21], which does not require third-party helpers or multiple antennas. More specifically, the system consists of two legitimate users, Alice and Bob, both equipped with a single antenna, and an adversary, Eve. Both legitimate users transmit pilot signals x_A and x_B , and their estimated channels are given by:

$$y_B = hx_A + z_B, \quad (1)$$

$$y_A = x_Bh + z_A, \quad (2)$$

where h is the complex channel coefficient, and z_A, z_B denote complex Gaussian noise with zero mean and unit variance. To introduce the common randomness, we multiply the estimated channels with locally generated pilot signals, resulting in effective channels:

$$\tilde{y}_B = x_B y_B = x_B h x_A + x_B z_B, \quad (3)$$

$$\tilde{y}_A = y_A x_A = x_B h x_A + z_A x_A. \quad (4)$$

These effective channels have shared randomness, e.g., $x_B h x_A$, and are thus highly correlated and can be used as common sources for secret key generation. The pilot signals are randomized to prevent the estimated channels from being deterministic, which offers no advantage for SKG. In the following, the pilot signals are designed with zero means, which guarantees the uncorrelated properties of the signal components and offers resilience against attacks [23].

In this paper, we will evaluate the performance of this scheme under real-world scenarios and introduce different randomization schemes. Since deriving a theoretical model and secret key rate for real environments is quite involved, we, therefore, perform numerical evaluation, considering the performance of the original channel as a benchmarking scheme. In the context of secret key generation, the mutual information (MI) between Alice and Bob I_{AB} quantifies the maximum number of bits that can be extracted from their shared randomness. In addition, the SKG rate I_{SK} is determined by the MI of the effective channels in the presence of attackers, which determines the upper bound on the achievable secret key rate.

III. NUMERICAL RESULTS

In this section, we evaluate the performance of the aforementioned method using real measurement data collected at the Nokia campus in Stuttgart, Germany [22]. The measurements were performed in a location featuring multiple roads and tall buildings. An antenna array consisting of 4 rows with 16 single-polarization patch antennas each, forming a 64-element transmit array, was placed on the top of a building. The antennas were spaced with a horizontal distance of $\lambda/2$ and a vertical distance of λ . The user equipment (UE) was a single monopole antenna mounted 1.5 meters above the ground on a portable cart. During the measurement, the cart moved along different predefined tracks at a walking speed of 3.6 km/h,

resulting in a spatial channel sampling interval of less than 0.5 mm.

A. Modelling a Low-Mobility Scenario

To demonstrate the effectiveness of the aforementioned approach, we model a scenario in which each entity has a single antenna. Although the data was collected for multiple-input single-output scenarios, we can utilize it to model a scenario in which two legitimate users and an attacker have a single antenna. More specifically, Bob is considered a receiver equipped with a single monopole antenna mounted on a portable cart, moving along various tracks (shown in Fig. 1). We utilize the antennas on the top of the building to model Alice and Eve and assume that Eve can partially obtain the information to the legitimate users, for instance, to Bob. The measurement setup and tracks are depicted in Fig. 1, and other parameters and settings are detailed in [22].

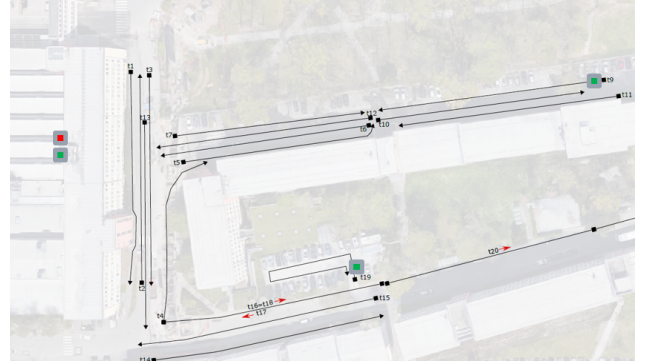


Fig. 1: Representation of the Nokia campus in Stuttgart, Germany, where the measurements were taken.

In the following, we will investigate two scenarios in which Bob is placed at track 9 and track 19, which corresponds to a strong line-of-sight, and a non-line-of-sight scenario, respectively. In Fig. 1, Bob on track 9 is marked by the green square at the top right, while the same icon at the bottom marks that of track 19. On the left, the red and green squares represent Eve and Alice, respectively.

B. Random Pilot Schemes

In the following, we will consider three distributions for the pilot signals. More specifically, we will evaluate the performance of common distributions, e.g., Gaussian, Uniform, and Rademacher distributions studied in [21].

- The Gaussian distribution is defined as follows:

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) \quad (5)$$

where x is the random variable, μ and σ^2 are the mean and the variance, respectively. In this experiment, we consider a standard normal Gaussian distribution where $\mu = 0$ and $\sigma = 1$, e.g., $X \sim \mathcal{N}(0, 1)$.

- A uniform distribution on the interval $[a, b]$, where $a < b$, has the probability density function given by:

$$f(x) = \begin{cases} \frac{1}{b-a}, & \text{if } x \in [a, b] \\ 0, & \text{elsewhere} \end{cases} \quad (6)$$

Herein, we consider uniform distribution on the interval $[-1, 1]$, e.g., $X \sim \mathcal{U}(-1, 1)$.

- A Rademacher distribution which takes a value of ± 1 with equal probability, i.e., $P(X = 1) = P(X = -1) = \frac{1}{2}$.

Note that at each value of signal-to-noise ratio (SNR), we will take 2000 samples recorded in the dataset, which already takes the impact of the mobility into account and varies with 500 noise samples, which requires an average of over one million scenarios per SNR.

C. Results and Discussion

As can be seen in Fig. 2, due to the impact of mobility and non-line-of-sight components, which provide certain variations, the secret key rate of the original channels is much higher than zero. Despite the improvements over static scenarios whose secret key rate is zero or close to zero (c.f. [21]), the gap between the maximum mutual information and the secret key rate is still high in both scenarios. By randomizing the pilots generated locally at Alice and Bob, we can notice significant gains in terms of both I_{AB} and I_{SK} , with an increase of up to 30%, and 50% in comparison with the original channels at high SNR, respectively. More importantly, the performance of the added random signals is also more stable across the scenarios, which shows that the randomness can be controllable at both ends and has more impact than that of low mobility and other channel variations. This outcome has huge implications for practical applications.

In Fig. 3, we increase the distance between Alice and Eve, which is assumed to make the effective channels between the legitimate and that of the adversary highly uncorrelated. As can be seen from Fig. 3, the secret key rate of the original channels relies mainly on the multipath, mobility, and/or fading in the environment. For the strong-line-of-sight scenarios, the LoS component dominates, and thus the performance is relatively stable. In case of NLoS, we, however, observe the variation, with some improvement over the case of $d_{AE} = \lambda/2$, possibly due to the uncorrelated properties of larger distance and the multipath effects. Noticeably, we see a significant improvement over purely relying on channels and/or mobility when utilizing the randomized locally generated pilots. Since we can control the distribution of the pilots, the performance in both cases in Fig. 3 is relatively stable but with significantly higher secret key rate.

IV. CONCLUSIONS AND FUTURE WORKS

We have studied the performance of a practical scheme for secret key generation in a low-mobility scenario. Specifically, to increase the secret key rate, we have randomized the locally generated pilots to introduce additional randomness to

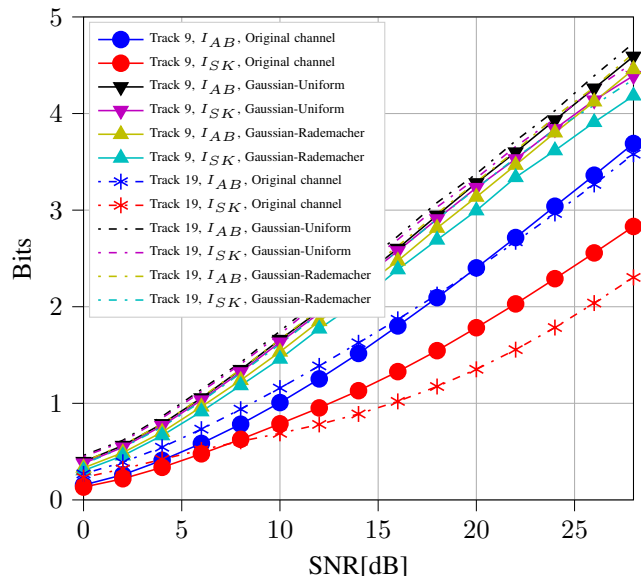
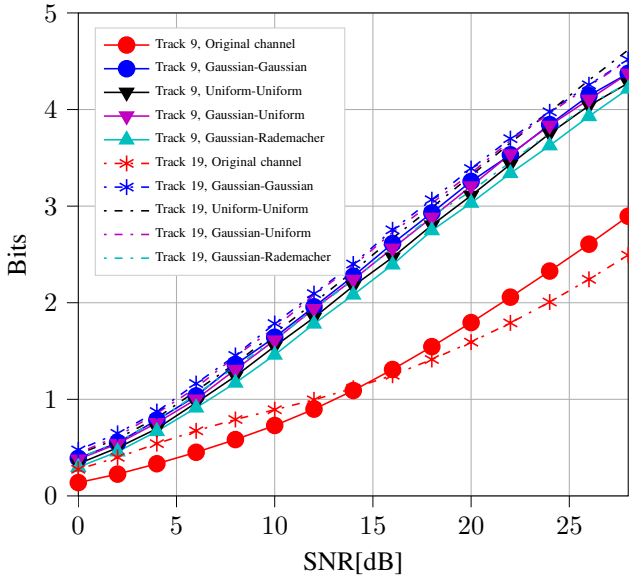


Fig. 2: Mutual information evaluation of the impact of mobility and randomization schemes on a scenario where Eve is fixed next to Alice at a distance $d_{AE} = \lambda/2$ and Bob moves at the speed of 3.6 km/h.

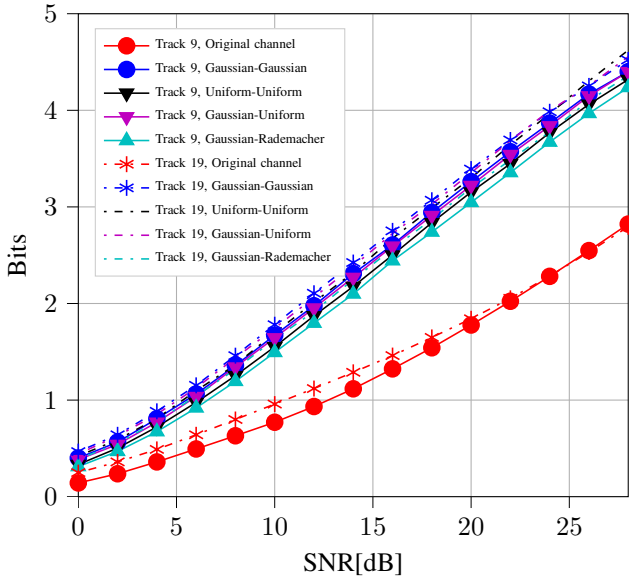
the system, without employing third-party helpers or multiple antennas. Taking advantage of an experimental dataset, we have modelled a typical scenario consisting of two legitimate users and an attacker. The results demonstrated significant improvements over the original channels, providing a potential for lightweight, practical, and reliable solutions for resource-constrained devices. As for future work, we can implement a new testbed to evaluate the performance of this scheme with fewer restrictions posed by the existing measurement, for example, in terms of the knowledge of the links to the legitimate users and/or the mobility. Furthermore, we can also investigate the case in which Eve knows full or partial distributions generated by both legitimate users.

ACKNOWLEDGEMENT

This work is financed by the Saxon State government out of the State budget approved by the Saxon State Parliament. This work has further been supported in part by the German Federal Ministry of Research, Technology and Space (BMFTR) through the research hub *6G-life* under Grant 16KISK001K and in part by the German Research Foundation (DFG) as part of Germany's Excellence Strategy – EXC 2050/1 - Project ID 390696704 - Cluster of Excellence “*Centre for Tactile Internet with Human-in-the-Loop*” (*CeTI*). This publication is also based upon work from COST Action 6G-PHYSEC (CA22168), supported by COST (European Cooperation in Science and Technology). The authors would also like to thank S. Wesemann, G. Kaltbeitzel, D. Wiegner, M. Kinzler, S. Merk and S. Woerner from Nokia for realizing the channel measurements and sharing the data.



(a) $d_{AE} = \lambda$



(b) $d_{AE} = 2\lambda$

Fig. 3: Secret key rate I_{SK} under highly uncorrelated scenarios, and different combinations of random distributions.

REFERENCES

- [1] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Natl. Acad. Sci. U.S.A.*, vol. 114, no. 1, pp. 19–26, Jan. 2017.
- [2] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [3] A. Carleial and M. Hellman, "A note on Wyner's wiretap channel (corresp.)," *IEEE Trans. Inf. Theory*, vol. 23, no. 3, pp. 387–390, May 1977.
- [4] C. Mitrpant, A. J. H. Vinck, and Yuan Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2181–2190, May 2006.
- [5] M. Bloch and J. Barros, *Physical-Layer Security: From Information*

- Theory to Security Engineering*. Cambridge, UK: Cambridge University Press, 2011.
- [6] R. F. Schaefer, H. Boche, A. Khisti, and H. V. Poor, Eds., *Information Theoretic Security and Privacy of Information Systems*. Cambridge, UK: Cambridge University Press, 2017.
- [7] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 5–22, 2021.
- [8] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.
- [9] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
- [10] J. Hershey, A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6, Jan. 1995.
- [11] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.
- [12] M. Mitev, A. Chorti, M. Reed, and L. Musavian, "Authenticated secret key generation in delay-constrained wireless systems," *Eurasip J. Wirel. Commun. Netw.*, 2020.
- [13] Y. Xu and D. Cao, "Secret key generation from vector Gaussian sources with public and private communications," *IEEE Trans. Inf. Theory*, vol. 67, no. 8, pp. 5420–5431, Aug. 2021.
- [14] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. IEEE ISIT*, 2006, pp. 2593–2597.
- [15] E. A. Jorswieck, A. Wolf, and S. Engelmann, "Secret key generation from reciprocal spatially correlated MIMO channels," in *Proc. IEEE Globecom Workshops*, 2013, pp. 1245–1250.
- [16] H. Taha and E. Alsusa, "Secret key exchange using private random precoding in MIMO FDD and TDD systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 4823–4833, 2017.
- [17] T. M. Pham, A. N. Barreto, M. Mitev, M. Matthé, and G. Fettweis, "Secure communications in line-of-sight scenarios by rotation-based secret key generation," in *Proc. IEEE ICC Workshops*, 2022, pp. 1101–1105.
- [18] Z. Ji, P. L. Yeoh, G. Chen, C. Pan, Y. Zhang, Z. He, H. Yin, and Y. Li, "Random shifting intelligent reflecting surface for otp encrypted data transmission," *IEEE Wireless Commun. Lett.*, vol. 10, no. 6, pp. 1192–1196, 2021.
- [19] N. Aldaghri and H. Mahdaviyar, "Physical layer secret key generation in static environments," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2692–2705, 2020.
- [20] S. Kojima and S. Sugiura, "User-independent randomized pilot activation for secure key generation," *IEEE Trans. Wirel. Commun.*, vol. 23, no. 9, pp. 11 624–11 635, 2024.
- [21] T. M. Pham, R. F. Schaefer, G. P. Fettweis, and A. Chorti, "Pilot randomization-based secret key generation for static scenarios," in *Proc. IEEE GLOBECOM*, 2024, pp. 37–42.
- [22] M. K. Shehzad, L. Rose, S. Wesemann, and M. Assaad, "ML-based massive MIMO channel prediction: Does it work on real-world data?" *IEEE Wireless Commun. Lett.*, vol. 11, no. 4, pp. 811–815, 2022.
- [23] T. M. Pham, M. Mitev, A. Chorti, and G. P. Fettweis, "Pilot randomization to protect MIMO secret key generation systems against injection attacks," *IEEE Wirel. Commun. Lett.*, vol. 12, no. 7, pp. 1234–1238, 2023.