




CKM-Assisted Physical-Layer Security for Resilience Against Unknown Eavesdropping Location

Ladan Khaloopour , Matthias Hollick , and Vahid Jamali 
 Technical University of Darmstadt, Darmstadt, Germany

Abstract—Channel Knowledge Map (CKM) is an emerging data-driven toolbox that captures our awareness of the wireless channel and enables efficient communication and resource allocation beyond the state of the art. In this work, we consider CKM for improving physical-layer security (PLS) in the presence of a passive eavesdropper (Eve), without making any assumptions about Eve’s location or channel state information (CSI). We employ highly directional mmWave transmissions, with the confidential message jointly encoded across multiple beams. By exploiting CKM, we derive an algorithm for time and power allocation among the beams that maximizes the absolute secrecy rate under the worst-case scenario for Eve’s location.

Index Terms—Physical layer security, channel knowledge map, secrecy capacity, eavesdropper, mmWave band.

I. INTRODUCTION

In recent years, channel knowledge map (CKM)¹ has received considerable attention as a new tool for improving communication, resource allocation, transmission robustness, and more [1, 4]. CKM includes contextual information about the wireless channel, which can be collected from a variety of sources, including real-world data from previous transmissions, artificial intelligence-based channel simulators, and various sensors. In this paper, we investigate the benefits of CKM for physical-layer security (PLS).

Most works on PLS assume that the perfect or imperfect CSI of Eve, its location area, or the direction toward Eve are available [5, 6, 7]. However, these assumptions might not be feasible in practice for a passive uncooperative eavesdropper. PLS can be enhanced by using higher frequency bands, such as millimeter wave (mmWave) frequencies, where the leakage probability is reduced due to the highly directional beams. However, the line-of-sight (LoS) link remains insecure to passive eavesdropping.

In this paper, we exploit CKM to enable PLS at mmWave bands, even in scenarios where no knowledge of Eve’s CSI or location is available. The confidential message is jointly encoded across multiple beams, which makes it impossible for the eavesdropper to recover the message unless it can decode all beams. This is physically unlikely, as the eavesdropper is present at only one (unknown) location. By leveraging CKM, we derive an algorithm for time and power allocation among the beams, that maximizes the absolute secrecy rate under

This work has been funded by the LOEWE Initiative, Hesse, Germany, within the emergenCITY Centre under Grant LOEWE/1/12/519/03/05.001(0016)/72.

¹CKM is also known by other names, e.g., radio frequency (RF) map, channel charting, time-domain channel prediction, etc. [1, 2, 3].

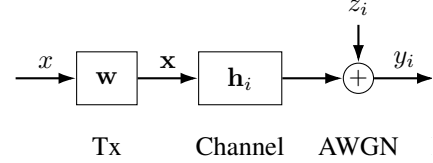


Fig. 1. General block diagram of the system model ($i \in \{r, e\}$).

the worst-case scenario for Eve’s location, i.e., the strongest attack location of Eve. Unlike our previous works [8, 9], which considered only time allocation and provided no analytical solution, here we derive analytical solutions for both time and power allocation.

II. SYSTEM MODEL AND PRELIMINARY

A. System Model

We consider a wireless communication system including a transmitter (Tx), a legitimate receiver (Rx), and a passive eavesdropper (Eve). Tx sends a confidential message to Rx, and Eve tries to intercept this message. Tx has N_t antennas, and for simplicity, Rx and Eve have a single antenna, and Eve’s location is unknown. The confidential message is denoted by $x \in \mathbb{C}$, and \mathbf{w} is the beamforming vector of the transmitter. Therefore, the transmitted data symbol $\mathbf{x} \in \mathbb{C}^{N_t}$ is given by

$$\mathbf{x} = \mathbf{w}x. \quad (1)$$

We assume $\mathbb{E}\{|x|^2\} \leq P_{\text{Tx}}$, where $\mathbb{E}\{\cdot\}$ is the expectation operator. The received signal is shown as

$$y_i = \mathbf{h}_i^H \mathbf{x} + z_i, \quad i \in \{r, e\}, \quad (2)$$

where subscripts r and e denote Rx and Eve, respectively. $y_i \in \mathbb{C}$, and $z_i \sim \mathcal{CN}(0, \sigma_i^2) \in \mathbb{C}$ is the additive white Gaussian noise (AWGN), $\mathbf{h}_i \in \mathbb{C}^{N_t}$ is the channel matrix that models the multi-path propagation of the transmitted signal in the channel between Tx and node i . The system model is shown in Fig. 1. The received signal to noise ratio (SNR) is

$$\gamma_i = \frac{P_{\text{Tx}}}{\sigma_i^2} |\mathbf{h}_i^H \mathbf{w}|^2, \quad i \in \{r, e\}. \quad (3)$$

We assume that Tx knows the CSI of Rx, i.e., \mathbf{h}_r , but does not know Eve’s location \mathbf{p}_e , its SNR γ_e , or channel \mathbf{h}_e .

B. CKM

CKM provides information about how RF is distributed in the environment. This of course depends on the direction that Tx transmits, the environment itself, and the random objects. For rigorousness, we consider the following CKM.

Definition: Let $\gamma(\theta, \mathbf{p})$ be the expected power that is collected by Rx at location \mathbf{p} due to radiation by transmitter with power P_{tx} along direction θ , i.e., $\mathbf{w} = \mathbf{a}_{\text{tx}}(\theta)$, where

$$\mathbf{a}_{\text{tx}}(\theta) = \frac{1}{\sqrt{N_t}} [1, e^{-j\frac{2\pi}{\lambda} d \sin(\theta)}, \dots, e^{-j\frac{2\pi}{\lambda} (N_t-1) d \sin(\theta)}]^T.$$

Throughout this paper, CKM is referred to any (experimental or simulation-based) knowledge about random variable (RV) $\gamma(\theta, \mathbf{p})$, $\forall \theta \in \Theta \doteq \{\theta_l | l = 1, \dots, L\}$ and $\forall \mathbf{p} \in \hat{\mathcal{P}} \doteq \{\mathbf{p}_j | j = 1, \dots, J\}$, where Θ and $\hat{\mathcal{P}}$ are the set of angle of departure (AoD) and Rx location for which the CKM is constructed.

III. CKM-ASSISTED SECURITY IMPROVEMENT

In this section, first we provide a concise overview of the physical layer security conditions and then introduce the secure coding scheme considered in this work.

A. Physical Layer Security and Secure Coding

The Tx aims to transmit the confidential message \mathbf{X} of length n over the channel to the Rx in the presence of an Eve. Let us assume that Rx decodes the message as $\hat{\mathbf{X}}$ and the Eve's observations are \mathbf{Y}_e . The communication between Tx and Rx is ensured to be reliable and secure if the two following conditions are satisfied [10, 11]:

$$\lim_{n \rightarrow \infty} \Pr(\mathbf{X} \neq \hat{\mathbf{X}}) = 0, \quad (4a)$$

$$\lim_{n \rightarrow \infty} \frac{1}{n} I(\mathbf{X}; \mathbf{Y}_e) = 0, \quad (4b)$$

where $\Pr(\cdot)$ and $I(\cdot; \cdot)$ show the probability and the mutual information operators, respectively. According to [10, 11, 12], the conditions of reliable and secure communication between Tx and Rx are satisfied if the transmission rate R_r is bounded as

$$R_r \leq [C_r - C_e]^+,$$

where the right hand side of the above inequality shows the secrecy capacity. For Gaussian wiretap channel, we have

$$C_i \doteq \log_2(1 + \gamma_i), \quad i \in \{r, e\}$$

as the channel capacity of node i , where $[q]^+ \doteq \max(q, 0)$.

B. Secure Coding Over Multi-beams

We use the mmWave band for transmission, which has highly directional and narrow beams, and helps secure communication by reducing the signal footprint. However, when the LoS is used for signal transmission, the secrecy rate can be zero if Eve is located at a point on the LoS path between Tx and Rx (due to the stronger Eve channel). Here, we use multiple beams and follow the idea of jointly encoding the message over different beams proposed in [10]. Eve can intercept part of the message if it is located in the path of a

beam. But, it cannot intercept all beams to decode the entire message. Thus, the message remains secure.

We denote the fractions of time and power allocated to path (or AoD) θ_l by t_l and p_l , respectively. The node i capacity for the l -th transmission is

$$C_{i,l} = \log_2(1 + \gamma_i(\theta_l, \mathbf{p})).$$

Since Tx does not know Eve's location and channel, we consider the secrecy capacity for the worst-case location \mathbf{p}_e , and channel realization $\mathbf{h}_e(\mathbf{p}_e)$ as:

$$C_s = \min_{\mathbf{p}_e \in \mathcal{P}} \sum_{l=1}^L [C_{r,l} - \max_{\mathbf{h}_e(\mathbf{p}_e) \in \mathcal{H}(\mathbf{p}_e)} C_{e,l}]^+, \quad (5)$$

where \mathcal{P} is the set of points we would take to ensure secrecy and $\mathcal{H}(\mathbf{p}_e)$ is the set of fading realization that a potential Eve at location \mathbf{p}_e may experience. In practice, the set \mathcal{P} cannot be the entire environment since otherwise the secrecy rate will be strictly zero (e.g., at least an eavesdropper arbitrary close to the Rx can recover the message). Moreover, set $\mathcal{H}(\mathbf{p}_e)$ can be in practice unknown. In this paper, we aim at approximating C_s (and \mathcal{P}) by the use of CKM, which provides an approximation of $\mathcal{H}(\mathbf{p}_e)$ (and \mathcal{P}), denoted by $\mathcal{H}^{\text{CKM}}(\mathbf{p}_e)$ (and $\hat{\mathcal{P}}$).

C. Problem Formulation

Our objective is to maximize the secrecy capacity by jointly optimizing the time fractions t_l and power p_l allocated to beam l , $\forall l \in \{1, \dots, L\}$. We define an estimated secrecy rate \hat{C}_s , which is obtained from the available CKM, i.e., using $\mathcal{H}^{\text{CKM}}(\mathbf{p}_e)$ instead of $\mathcal{H}(\mathbf{p}_e)$ in (5). Therefore, we have

$$\begin{aligned} \mathbf{P1:} \quad & \max_{p_l \geq 0, t_l \geq 0, \forall l} \min_{\mathbf{p}_j \in \hat{\mathcal{P}}} \sum_{l=1}^L t_l \left[\log_2 \left(\frac{1 + p_l \alpha_l}{1 + p_l \beta_{l,j}} \right) \right]^+ \\ \text{s.t.} \quad & C_1 : \sum_{l=1}^L t_l \leq 1, \quad C_2 : \sum_{l=1}^L p_l t_l \leq P_{\text{tx}}, \end{aligned} \quad (6)$$

where $\alpha_l \doteq \frac{\gamma_r(\theta_l)}{P_{\text{tx}}}$ and $\beta_{l,j} \doteq \max_{\gamma(\theta_l, \mathbf{p}_j) \in \mathcal{H}^{\text{CKM}}(\mathbf{p}_j)} \frac{\gamma(\theta_l, \mathbf{p}_j)}{P_{\text{tx}}}$ are the normalized SNRs at Rx and \mathbf{p}_j , respectively, when beam l is adopted. In problem **P1**, the objective function ensures absolute secrecy regardless of Eve's location within $\mathbf{p}_j \in \hat{\mathcal{P}}$ and constraints C_1 and C_2 enforce the total time and power budgets, respectively.

D. Solution Development

The optimization problem **P1** is not convex due to the operator $[\cdot]^+$ and the argument of logarithm. However, given $p_l \geq 0$, function $\log_2 \left(\frac{1 + p_l \alpha_l}{1 + p_l \beta_{l,j}} \right)$ is only negative when $\alpha_l \leq \beta_{l,j}$. Therefore, we can drop the non-linear operator $[\cdot]^+$ by taking the sum over set $\mathcal{L}_j \doteq \{l : \alpha_l \geq \beta_{l,j}\}$. Let us define $f_j(\mathbf{p}, \mathbf{t}) \doteq \sum_{l \in \mathcal{L}_j} t_l \log_2 \left(\frac{1 + p_l \alpha_l}{1 + p_l \beta_{l,j}} \right)$, where $\mathbf{p} = [p_1, \dots, p_L]$

and $\mathbf{t} = [t_1, \dots, t_L]$. Therefore, the optimization problem in (6) will be as follows

$$\begin{aligned} \mathbf{P2}: \quad & \max_{c, p_l \geq 0, t_l \geq 0, \forall l} c \\ \text{s.t. } & \mathbf{C}_0: f_j(\mathbf{p}, \mathbf{t}) \geq c, \quad \forall \mathbf{p}_j \in \hat{\mathcal{P}} \\ & \mathbf{C}_1: \sum_{l=1}^L t_l \leq 1, \quad \mathbf{C}_2: \sum_{l=1}^L p_l t_l \leq P_{\text{tx}}, \end{aligned} \quad (7)$$

where c is an auxiliary variable. In the following, we consider the optimization problem **P2**.

We introduce variables $\nu_j \geq 0$, $\lambda \geq 0$, and $\mu \geq 0$, which are the Lagrange multipliers associated with constraints \mathbf{C}_0 , \mathbf{C}_1 , and \mathbf{C}_2 , respectively. Now, we adopt a Lagrange dual formulation for **P2** in (7)

$$\begin{aligned} \mathcal{L}(\mathbf{p}, \mathbf{t}, c; \nu, \lambda, \mu) = & c + \sum_{j=1}^J \nu_j \left(\sum_{l \in \mathcal{L}_j} t_l \log \left(\frac{1 + p_l \alpha_l}{1 + p_l \beta_{l,j}} \right) - c \right) \\ & + \lambda \left(1 - \sum_{l=1}^L t_l \right) + \mu \left(P_{\text{tx}} - \sum_{l=1}^L p_l t_l \right), \end{aligned} \quad (8)$$

where $\nu = [\nu_1, \dots, \nu_J]$. Note that we have changed $\log_2(\cdot)$ into the natural logarithm to simplify the following derivations. One can consider that the variables ν_j and c are changed into $\nu_j / \log(2)$ and $c \log(2)$, respectively. Therefore, we can change $\log_2(\cdot)$ in $f_j(p, t)$ into $\log(\cdot)$. By applying the Karush–Kuhn–Tucker (KKT) conditions, we derive analytical solutions for the primal variables p_l and t_l , $\forall l$, as a function of the dual variables λ and μ . These conditions are given below.

Stationarity conditions:

$$\frac{\partial \mathcal{L}}{\partial c} = 1 - \sum_{j=1}^J \nu_j = 0 \quad (9a)$$

$$\frac{\partial \mathcal{L}}{\partial t_l} = -\lambda - \mu p_l + \sum_{j: l \in \mathcal{L}_j} \nu_j \log \left(\frac{1 + p_l \alpha_l}{1 + p_l \beta_{l,j}} \right) = 0 \quad (9b)$$

$$\frac{\partial \mathcal{L}}{\partial p_l} = -\mu t_l + t_l \sum_{j: l \in \mathcal{L}_j} \nu_j \left(\frac{\alpha_l}{1 + p_l \alpha_l} - \frac{\beta_{l,j}}{1 + p_l \beta_{l,j}} \right) = 0. \quad (9c)$$

Primal feasibility conditions:

$$\begin{cases} t_l \geq 0, \forall l \\ p_l \geq 0, \forall l \\ f_j(\mathbf{p}, \mathbf{t}) \geq c, \forall j \\ \sum_{l=1}^L t_l \leq 1 \\ \sum_{l=1}^L p_l t_l \leq P_{\text{tx}}. \end{cases} \quad (10)$$

Dual feasibility conditions: $\nu_j \geq 0, \forall j$, $\lambda \geq 0$, $\mu \geq 0$.

Complementary slackness conditions:

$$\begin{cases} \nu_j \left(\sum_{l \in \mathcal{L}_j} t_l \log \left(\frac{1 + p_l \alpha_l}{1 + p_l \beta_{l,j}} \right) - c \right) = 0, \forall j \\ \lambda \left(\sum_{l=1}^L t_l - 1 \right) = 0 \\ \mu \left(\sum_{l=1}^L p_l t_l - P_{\text{tx}} \right) = 0. \end{cases} \quad (11)$$

Algorithm 1 Proposed power and time allocation algorithm

Initialization

1: Initialize feasible primal variables p_l , t_l , dual variables λ , $\mu \geq 0$, step sizes η_t , η_p , η_λ , η_μ , and solution tolerance ϵ .

Iteration Steps

2: Compute active constraint: $j^* = \arg \min_j f_j(\mathbf{p}, \mathbf{t})$.
3: Update primal variables p_l from (12a) and t_l from (12b).
4: Update dual variables λ from (13a) and μ from (13b).
5: Stop if improvement in $c = \min_j f_j(\mathbf{p}, \mathbf{t})$ is below ϵ .

Output

6: Optimal p_l^* , t_l^* , λ^* , μ^* , and $c^* = f_{j^*}(\mathbf{p}^*, \mathbf{t}^*)$.

Next, we develop an iterative algorithm, where at each iteration, we update the solution towards meeting the above KKT conditions. Let us assume first that the worst-case Eve's location is unique, i.e., $j^* = \arg \min_j f_j(\mathbf{p}, \mathbf{t})$. Therefore, constraint \mathbf{C}_0 is active only for $j = j^*$, which from the complementary slackness conditions, we obtain $\nu_j = 0, \forall j \neq j^*$ and from the stationarity conditions, we get $\nu_{j^*} = 1$. Now, given the worst-case Eve's location, we adopt a gradient update for power and time variables at each iteration in order to move in the direction of satisfying the stationarity conditions:

$$p_l \leftarrow [p_l + \eta_p (g_l - \mu) t_l]^+, \quad \forall l \quad (12a)$$

$$t_l \leftarrow [t_l + \eta_t (q_l - \lambda - \mu p_l)]^+, \quad \forall l, \quad (12b)$$

where $g_l \doteq \frac{\alpha_l}{1 + p_l \alpha_l} - \frac{\beta_{l,j^*}}{1 + p_l \beta_{l,j^*}}$, $q_l \doteq \log \left(\frac{1 + p_l \alpha_l}{1 + p_l \beta_{l,j^*}} \right)$, and η_t and η_p are step sizes. Note that the stationarity condition in (9c) can be solved analytically for a known j^* ; however, a gradual update as in (12a) is preferred since a significant variation in the variables introduces numerical instability due to the underlying change in j^* from one iteration to the next.

Finally, dual variables μ and λ are updated as follows to meet the dual feasibility and complementary slackness conditions:

$$\lambda \leftarrow [\lambda + \eta_\lambda r_1]^+, \quad (13a)$$

$$\mu \leftarrow [\mu + \eta_\mu r_2]^+, \quad (13b)$$

where $r_1 = \sum_{l=1}^L t_l - 1$ and $r_2 = \sum_{l=1}^L p_l t_l - P_{\text{tx}}$ are constraint residuals and η_λ and η_μ are step sizes.

The proposed iterative solution for **P2** is summarized in Algorithm 1.

IV. SIMULATION RESULTS

As an initial investigation and to draw some insight, we consider a system with two ideal narrow beams ($L = 2$, an LoS path and a 10 dB weaker non-LoS path), where the leakage from one beam to another is negligible, which is valid for large N_t at mmWave bands. We consider the following normalized parameter values: $\alpha_1 = \beta_{1,1} = 2 \text{ W}^{-1}$, $\alpha_2 = \beta_{2,2} = 0.2 \text{ W}^{-1}$, $\beta_{1,2} = \beta_{2,1} = 0 \text{ W}^{-1}$, $P_{\text{tx}} = 10 \text{ W}$.

The secrecy capacity versus the power of the LoS path is plotted in Fig. 2. As observed, using only the LoS path for transmission is not secure, whereas joint coding even with uniform time and power allocation would consistently

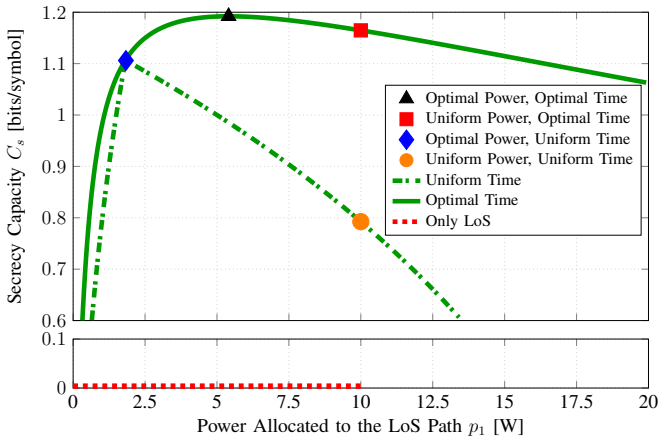


Fig. 2. Absolute secrecy capacity vs. the power allocated to the LoS path with the average transmit power $P_{tx} = 10$ W.

provide secrecy. Performance improves when only the powers are optimized, and improves even more when only the times are optimized [8, 9]. As shown, the scheme of joint power and time allocation outperforms the algorithms which only optimize either time or power. Moreover, Fig. 2 shows that allocating less power to the LoS link than to the weaker non-LoS link maximizes secrecy rate.

The secrecy capacity versus the total transmitted power P_{tx} (for both LoS and non-LoS paths) is plotted in Fig. 3. As observed, using only the LoS path does not provide secrecy. When both LoS and non-LoS paths are employed, the secrecy capacity is positive even with the simple scheme of uniform time and uniform power allocation. As shown, the scheme of joint power and time allocation outperforms the algorithms which only optimize either time (e.g., proposed in [8, 9]) or power. Note that Fig. 2 is a special case of Fig. 3 where $P_{tx} = 10$ W, and confirms the secrecy capacities in Fig. 3. Moreover, Fig. 3 shows that the secrecy rate is an increasing function of the total transmitted power P_{tx} .

V. CONCLUSION

In this paper, we have employed CKM to enhance PLS in the presence of a passive Eve, without making any assumptions about Eve's location or CSI. The confidential message was transmitted using the highly directional mmWave band and was jointly encoded across multiple beams. We derived an algorithm for time and power allocation among the beams that maximizes the absolute secrecy rate under the worst-case scenario for Eve's location. The simulation results validate the performance of our scheme compared to previous methods, where either time or power is uniformly allocated, while the other is optimized. Furthermore, our results show that the secrecy capacity increases with the total transmitted power.

REFERENCES

[1] C. Studer, S. Medjkouh, E. Gonultaş, T. Goldstein, and O. Tirkkonen, "Channel charting: Locating users within the radio environment using channel state information," *IEEE Access*, vol. 6, pp. 47682–47698, 2018.

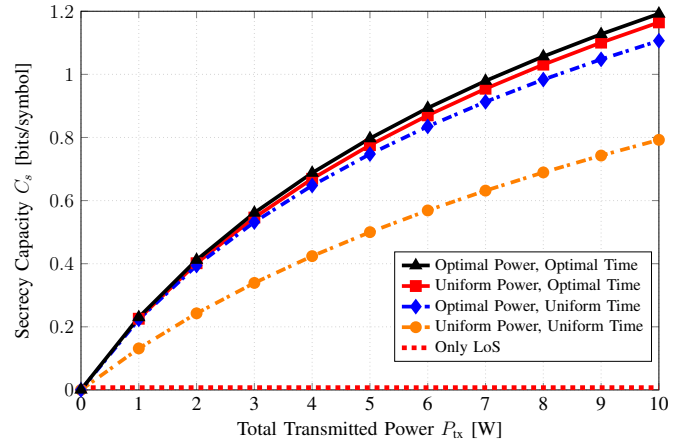


Fig. 3. Absolute secrecy capacity vs. the total transmitted power along the LoS and non-LoS paths.

- [2] W. Jiang and H. D. Schotten, "Neural network-based fading channel prediction: A comprehensive overview," *IEEE Access*, vol. 7, pp. 118 112–118 124, 2019.
- [3] A. Duel-Hallen, "Fading channel prediction for mobile radio adaptive transmission systems," *Proceedings of the IEEE*, vol. 95, no. 12, pp. 2299–2313, 2007.
- [4] Y. Zeng, J. Chen, J. Xu, D. Wu, X. Xu, S. Jin, X. Gao, D. Gesbert, S. Cui, and R. Zhang, "A tutorial on environment-aware communications via channel knowledge map for 6G," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 3, pp. 1478–1519, 2024.
- [5] J. Lin, Q. Li, J. Yang, H. Shao, and W.-Q. Wang, "Physical-layer security for proximal legitimate user and eavesdropper: A frequency diverse array beamforming approach," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 671–684, 2017.
- [6] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3231–3245, 2013.
- [7] D. Xu, X. Yu, D. W. K. Ng, A. Schmeink, and R. Schober, "Robust and secure resource allocation for ISAC systems: A novel optimization framework for variable-length snapshots," *IEEE Transactions on Communications*, vol. 70, no. 12, pp. 8196–8214, 2022.
- [8] A. Ishtiaq, A. Asadi, L. Khalooupour, W. Ahmed, V. Jamali, and M. Hollick, "Beamsec: A practical mmwave physical layer security scheme against strong adversaries," in *2023 IEEE Conference on Communications and Network Security (CNS)*, 2023, pp. 1–9.
- [9] A. Ishtiaq, L. Khalooupour, V. Jamali, M. Hollick, and A. Asadi, "Harnessing spatial diversity for physical layer security without adversary channel knowledge," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2025, Accepted for publication.
- [10] C.-Y. Yeh, A. Cohen, R. G. D'Oliveira, M. Médard, D. M. Mittleman, and E. W. Knightly, "Angularly dispersive terahertz links with secure coding: From theoretical foundations to experiments," in *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2022, pp. 268–273.
- [11] R. F. Schaefer, H. Boche, and H. V. Poor, "Secure communication under channel uncertainty and adversarial attacks," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1796–1813, 2015.
- [12] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proceedings of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, 2017.