# Harnessing Spatial Diversity for Physical Layer Security Without Adversary Channel Knowledge

Afifa Ishtiaq, *Student Member, IEEE*, Ladan Khaloopour, Vahid Jamali, *Senior Member, IEEE*, Matthias Hollick, *Member, IEEE*, and Arash Asadi, *Senior Member, IEEE*

***Abstract*—Millimeter-wave (mmWave) communication systems utilize phased-array antennas to generate highly directional beams, effectively reducing the signal footprint. Nonetheless, eavesdropping, particularly within the main-lobe, remains a significant concern. This paper introduces BeamSec, a novel beam hopping approach to maximize absolute secrecy rates with no information about the channel state information (CSI) or location of the eavesdroppers. Methodologically, BeamSec identifies diverse beam-pairs between transceivers by analyzing signal characteristics, such as angle of departure (AoD) and angle of arrival (AoA). To prevent the secure message from being eavesdropped, BeamSec splits and jointly encodes data among selected beams. Moreover, BeamSec optimizes secrecy by adapting time allocation across selected beams under different levels of channel knowledge, namely (*i*) full/-partial radio frequency (RF) maps constructed based on the empirical data of legitimate users, (*ii*) knowledge of the room floor plan, and (*iii*) only the instantaneous knowledge of the legitimate transmitter (TX)-receiver (RX) channel. Furthermore, we experimentally validate the efficiency of the proposed schemes using an 802.11ad-compatible 60 GHz phased-array testbed. Specifically, BeamSec demonstrates a non-zero absolute secrecy rate even for the simplistic uniform time allocation approach. Radio map (partial channel knowledge) and known room geometry (instantaneous TX/RX) based schemes provide further improvement of 124.8% and 58.13%, respectively, as compared to uniform time allocation.**

***Index Terms*—Physical layer security (PLS) mmWave, beamforming, 60 Ghz, testbed, eavesdropping.**

## I. Introduction

PHYSICAL layer security has been a prominent research area for over a decade, leveraging information-theoretic techniques to enhance security by exploiting the inherent randomness of wireless channels. This approach complements higher-layer cryptographic methods and is categorized into two main areas: $(i)$ Key generation, which derives secure keys from channel parameters to avoid high-layer key exchanges and authenticate users [2], [3]; and $(ii)$ Secure transmission, which reduces the Signal to Interference plus Noise Ratio (SINR) at eavesdroppers to prevent them from decoding packets. This is achieved using coding schemes that minimize information leakage [4], [5], [6] and reduce the signal footprint [7], i.e., the region where transmitted signals can be detected by unintended receivers or eavesdroppers (Eves). In millimeter-wave (mmWave) systems, which use highly directional beams, the signal footprint is minimized compared to traditional omnidirectional transmissions, reducing the area in which Eves can intercept the signal. The signal footprint size is influenced by factors like transmit power, antenna directionality, environmental elements, and receiver sensitivity. Techniques such as directional modulation (DM) can further enhance physical layer security by transmitting original symbols toward legitimate users while distorting symbols in undesired directions, minimizing interception risks [8]. Other methods include artificial noise transmission [9], tighter beamforming [10], and side-lobe reduction [6]. Nonetheless, the adversaries can still eavesdrop on the non-negligible side-lobes of *consumer-grade* antennas, which have been the subject of several studies such as [11] and [12].

Even if the side-lobes are sufficiently suppressed, the main-lobe remains exposed to adversaries. Prior work often argues that an attacker on the main-lobe can be easily detected [13]. In practice, the small size of consumer-grade wireless devices allows eavesdropping without creating (easily) detectable radio frequency (RF) signatures. Moreover, to ensure secure communication, most literature assumes full instantaneous/statistical channel state information (CSI) of the Eve [14], [15], [16] or her exact/approximate location [17] is available. While this knowledge may be possible to obtain for certain scenarios, e.g., a "cooperative" Eve within the same network, for most practical scenarios involving passive eavesdropping, it is challenging to obtain the Eve's channel knowledge. Hence, a fundamental challenge in practical physical layer security is to provide secure communication when no explicit knowledge about the Eve's channel or her location is available, which is the primary focus of this paper.

### A. Related Work

There exist only a few works addressing main-lobe security. The works in [14], [15], and [16] secure the main-lobe through rotated angular beamforming with a frequency-diverse

Received 30 December 2024; revised 18 May 2025; accepted 26 July 2025. Date of publication 8 August 2025; date of current version 22 December 2025. This work was supported in part by the State of Hesse through LOEWE emergenCITY under Grant LOEWE/1/12/519/03/05.001(0016)/72, in part by European Commission's Horizon 2020 through the Marie Skłodowska-Curie Action Millimeter-wave Networking and Sensing for Beyond 5G (MINTS) under Grant 861222, and in part by German Research Foundation through SenShield under Grant 447586980. An earlier version of this paper was presented at the IEEE CNS 2023 [DOI: 10.1109/CNS59707.2023.10289003]. The associate editor coordinating the review of this article and approving it for publication was B. Chalise. *(Corresponding author: Afifa Ishtiaq.)*

Afifa Ishtiaq and Matthias Hollick are with the Department of Computer Science, Technical University of Darmstadt, 64283 Darmstadt, Germany (e-mail: aishtiaq@seemoo.tu-darmstadt.de; mhollick@seemoo.tu-darmstadt.de).

Ladan Khaloopour and Vahid Jamali are with the Department of Electrical Engineering and Information Technology, Technical University of Darmstadt, 64283 Darmstadt, Germany (e-mail: ladan.khaloopour@tu-darmstadt.de; vahid.jamali@tu-darmstadt.de).

Arash Asadi is with Faculty of Electrical Engineering, Mathematics and Computer Science, TU Delft, 2628 CD Delft, The Netherlands (e-mail: A.Asadi@tudelft.nl).

Digital Object Identifier 10.1109/TWC.2025.3594733

array assuming the knowledge of the Eve's location. In [18], the authors exploit antenna arrays and ground reflections to achieve angle-range-dependent transmission and side-lobe randomization for location-based physical layer security in mmWave vehicular networks. In [19], the authors propose a dual-beam transmission technique that ensures the main-lobe is coherent only at the legitimate receiver's (RX) location. The work in [17] proposes an artificial-noise-aided hybrid precoder that maximizes the secrecy rate, assuming full channel knowledge of the Eve. The work in [20] proposes an optimal directional modulation with artificial noise using a frequency-diverse phased array scheme to decouple the angle-range correlation and maximize the secrecy rate of RX. In addition, learning-based methods have been investigated in the literature to enable physical layer security, see e.g. [21] for a survey of dynamic security methods, particularly based on reinforcement learning (RL).

Although a big step forward, the above-mentioned solutions: $(i)$ rely on specialized antennas (angular polarization) [19], or a large number of RF chains [20]; $(ii)$ require the exact knowledge of Eve's location [14], [15], [16] or channel [17]; or $(iii)$ introduce additional interference to the network by transmitting artificial noise [22]. These limitations pose a major obstacle in the practical applications of physical layer security in mmWave systems. In [23], [24], and [25], the authors propose to perform path/beam hopping between randomly chosen paths between the transmitter (TX) and RX. Although theoretically effective, *beam hopping without rigorous analysis of the correlation among TX-RX beams can adversely impact the security*: $(i)$ by increasing the signal footprint, $(ii)$ a random selection of paths may lead to selecting the paths with minimum angular separation or minimum diversity, which diminishes the essence of hopping.

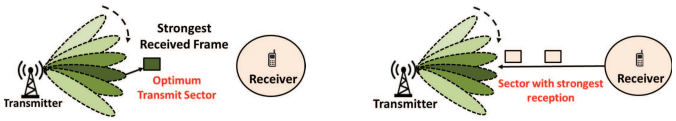
*Challenges:* Measurement campaigns have revealed mmWave channels are sparse (the number of paths between TX and RX is limited) [26], and there is a spatial correlation among these paths even in the presence of blockages [27]. This makes secure beam hopping at mmWave challenging. To enhance the physical layer security, it is crucial to identify the paths that are spatially diverse and distinct. Despite the availability of multiple paths, not all paths contribute equally to enhance secrecy as they yield different link Signal to Noise Ratio (SNR) for the legitimate RX or they may not have sufficient angular separation, making them vulnerable to interception by an Eve. For example, some beams may benefit from scattering conditions, yielding higher SNR but yet providing limited secrecy due to a larger signal footprint. These challenges underscore that there is no one-size-fits-all solution, as the information available to the system may vary. Consequently, the dynamic nature of wireless communication environments demands adaptable strategies capable of leveraging available information to enhance secrecy while maintaining system efficiency and reliability. Addressing this challenge requires optimal time allocation based on the quality of beams and available channel information. Time allocation is necessary to balance the use of high-capacity and high-security beams. Different beams have varying levels of security and capacity, and optimal time allocation ensures that the overall secrecy rate is maximized.

### B. Our Proposal: BeamSec

In this paper, we present BeamSec, a novel approach that addresses the challenging task of physical layer security, when no explicit knowledge about the Eve's channel or her location is available. This is achieved by splitting and jointly encoding data among available beams and further enhancing the secrecy by adapting time allocation across selected beams under different levels of channel knowledge. The main contributions of this paper are summarized in the following:

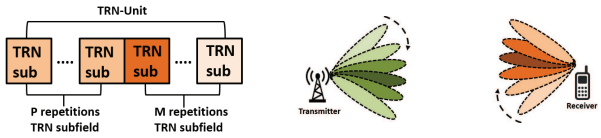
- **Low-overhead secrecy through beam pre-selection:** Including all available beams, even those with limited SNR or angular separation, would increase the overall overhead without significantly contributing to the secrecy rate. Hence, we first devise a novel beam identification strategy that pre-selects a subset of secure beam pairs, balancing secrecy and data rate. This approach relies solely on the channel knowledge obtained during standard beam training procedures at the legitimate TXs and RXs.
- **Joint coding across selected beams:** To realize main-lobe security when no explicit knowledge of the Eve's channel is available, we jointly encode information across all selected beam pairs, which allows decoding of the secure message only when all messages are successfully decoded. In particular, secrecy is achieved by exploiting the fact that although the Eve location is unknown, it is unlikely that the Eve can intercept all beams, which is necessary for decoding the secure message.
- **Maximizing secrecy rate through time allocation:** The selected beams do not equally enhance secrecy, as they produce varying link SNR for the legitimate RX or lack sufficient angular separation, increasing their susceptibility to interception by an Eve. The proposed BeamSec optimizes secrecy by adapting time allocation across selected beams under different levels of channel knowledge, namely (*i*) full/-partial RF maps constructed based on the empirical data of legitimate users, (*ii*) knowledge of the room floor plan, and (*iii*) only the instantaneous knowledge of the legitimate TX-RX channel.
- **Experimental validation for an office environment:** We implement BeamSec by creating an experimental prototype based on software-defined radio (SDR). We have conducted experiments in an office environment, evaluating BeamSec performance against various adversary models, including both single and colluding directional attackers. Our extensive experiments demonstrate that BeamSec achieves a non-zero absolute secrecy rate, even with a simplistic uniform time allocation approach. Schemes utilizing RF maps (partial channel knowledge) and known room geometry (instantaneous TX/RX knowledge) yield improvements of 124.8% and 58.13%, respectively, compared to uniform time allocation.

This manuscript extends its conference version [1] by including a detailed discussion on the adopted secure coding, new strategies for beam identification as well as for time allocation among the pre-selected beams relying on different levels




(a) Transmit sector sweep (b) Receive sector sweep

Fig. 1. Sector level sweep procedure of 802.11ad/ay.




(a) TRN representation (b) TX RX Sweep

Fig. 2. Beam refinement procedure of 802.11ad/ay.

of channel knowledge. These results are further accompanied by a new set of experimental measurements.

## II. Overview of IEEE 802.11Ad

In the following, we first briefly review the beam-training procedure in IEEE 802.11ad, which forms the basis for the proposed BeamSec. Commercial 802.11ad devices typically use a pre-defined codebook, providing wide coverage and high data rates via a combination of wide and narrow beams. The beam-training procedure in 802.11ad determines the appropriate beams for an access point (AP) and station (STA) through bi-directional training in two stages: sector level sweep (SLS) and beam-refinement phase (BRP), see Figs 1 and 2.

During SLS, a series of frames with multiple packets are exchanged between the AP and STA over different antenna sectors to determine the sector with the highest signal quality. The SLS consists of two types of sector sweep: the transmit sector sweep (TXSS) and the receive sector sweep (RXSS). In the TXSS, frames containing packets are transmitted over different directions in the AP's coverage using the antenna weight vectors (AWV). The STA in listening mode decodes the header and data field, associates itself with the AP, and sends feedback to ensure that the selected transmit AWV is appropriate. During RXSS, transmission on the best-known sector from TXSS allows for finding the optimal receive sector.

After identifying the optimal sector and initial configuration of AWV, the antenna settings for the AP and STA are further refined using BRP. Unlike SLS, BRP does not rely on pre-defined sector patterns but uses directional beam scanning at both AP and STA. AP is set to a specific AWV, evaluated for each AWV at STA, and repeated for all AWVs on AP. Finally, feedback is carried out to determine the optimal transmit and receive antenna configurations for AP and STA, respectively. The procedure is repeated for AP as a receiver and STA as a transmitter and exhausts every possible combination of transmit AWVs for a fixed receive AWV setting, leading to significant performance improvement over SLS-based training.

*Remark 1:* While BeamSec builds on the initial alignment and BRP procedures of IEEE 802.11ad/ay, it operates exclusively with directional beams at both transmitter and receiver, leveraging the BRP beam-pairs to perform exhaustive evaluation for secrecy rate optimization and time allocation.

## III. System and Adversary Model

Our system model consists of a transmitter (i.e., Alice) communicating with a legitimate receiver (i.e., Bob) in a multi-path environment in the presence of eavesdropper(s) (Eve). Eve is passive (i.e., she does not manipulate the communication between Alice and Bob) and her location and channel are unknown. Subsequently in the following, we provide a detailed description of the channel and eavesdropping models along with the definition of secure communication to provide physical layer security.

### A. Channel Model

We assume Alice, Bob, and Eve are multiple antenna nodes, respectively equipped with $N_a$, $N_b$, and $N_e$ antennas. The signal model is given by

$$\mathbf{y}_i = \mathbf{H}_i\mathbf{x} + \boldsymbol{\eta}_i, \quad \forall i \in \{b, e\}, \tag{1}$$

where subscripts $b$ and $e$ denote Bob and Eve, respectively. Here, $\mathbf{x} \in \mathbb{C}^{N_a}$ denotes the transmit vector satisfying the transmit power constraint $\mathsf{E}\{\mathbf{x}^H\mathbf{x}\} \leq P$, $\mathbf{H}_i \in \mathbb{C}^{N_i \times N_a}$ is the channel between Alice and node $i$, $\mathbf{y}_i \in \mathbb{C}^{N_i}$ denotes the received signal vector at node $i$, and $\boldsymbol{\eta}_i \sim \mathcal{CN}(\mathbf{0}, \sigma_\eta^2\mathbf{I}) \in \mathbb{C}^{N_i}$ denotes the zero-mean additive white Gaussian noise (AWGN) at node $i$, where $\sigma_\eta^2$ is the noise power at each antenna.

The channel matrix $\mathbf{H}_i$ is generally composed of a Line of Sight (LoS) component $\mathbf{H}_i^{LoS}$ and Non-line of Sight (nLoS) components $\mathbf{H}_i^{nLoS}$:

$$\mathbf{H}_i = \mathbf{H}_i^{LoS} + \mathbf{H}_i^{nLoS}. \tag{2}$$

The LoS channel $\mathbf{H}_i^{LoS}$ between Alice and node $i$ is:

$$\mathbf{H}_i^{LoS} = \alpha_{i,0}\mathbf{a}_i(\phi_{i,0})\mathbf{a}_a^{\mathsf{H}}(\theta_{i,0}), \quad \forall i \in \{b, e\}, \tag{3}$$

where $\alpha_{i,0} \in \mathbb{C}$ is the channel coefficient of the LoS link, $\mathbf{a}_a(\theta_{i,0}) \in \mathbb{C}^{N_a}$ denotes the transmit steering vector for Alice evaluated at angle of departure (AoD) $\theta_{i,0}$, and $\mathbf{a}_i(\phi_{i,0}) \in \mathbb{C}^{N_i}$ represents the receive steering vector at node $i$ evaluated at angle of arrival (AoA) $\phi_{i,0}$. Assuming that the nLoS channel $\mathbf{H}_i^{nLoS}$ between Alice and node $i$ comprises of $L_i$ paths, we have:

$$\mathbf{H}_i^{nLoS} = \sum_{l=1}^{L_i} \alpha_{i,l}\mathbf{a}_i(\phi_{i,l})\mathbf{a}_a^{\mathsf{H}}(\theta_{i,l}), \quad \forall i \in \{b, e\}, \tag{4}$$

where subscript $l$ denotes the path $l$ of the nLoS link, and $\alpha_{i,l}$, $\phi_{i,l}$, and $\theta_{i,l}$ are the corresponding channel coefficient, AoA, and AoD, respectively. Assuming a uniform linear array (ULA) at all nodes, the steering vectors can be written as

$$\mathbf{a}_i(\theta) = \left[1, e^{-j\kappa d\cos(\theta)}, \ldots, e^{-j\kappa(N_i-1)d\cos(\theta)}\right]^{\mathsf{T}}, \forall i \in \{a, b, e\}, \tag{5}$$

where $\kappa = \frac{2\pi}{\lambda}$ is the wave number, $\lambda$ is the wavelength, and $d$ is the element spacing.

### B. Effective Beam-Space Model

We assume that Alice transmits a single data stream via linear precoding/beamforming $\mathbf{w}_l \in \mathbb{C}^{N_a}$, i.e., $\mathbf{x} = \mathbf{w}_l x$, where $x \in \mathbb{C}$ is the data symbol that satisfies the power constraint $\mathsf{E}\{|x|^2\} \leq P$ and $\mathbf{w}_l$ is unit-norm, i.e., $\|\mathbf{w}_l\|^2 = 1$, beamforming vector for the $l$-th path. Bob adopts a linear combiner $\mathbf{f}_l \in \mathbb{C}^{N_b}$, which is a combiner vector over the $l$-th path and it is unit-norm, i.e., $\|\mathbf{f}_l\|^2 = 1$. In practice, Alice's beamformer $\mathbf{w}_l$ and Bob's combiner $\mathbf{f}_l$ are chosen from a predefined codebook (i.e., beams), denoted by $\mathcal{W}$ and $\mathcal{F}$, respectively, which account for the aforementioned beam refinement procedure. For transmission at path $l$, the signal at Bob's combiner $y_b \in \mathbb{C}$ is obtained as

$$y_b = \mathbf{f}_l^{\mathsf{H}} \mathbf{y}_b = \mathbf{f}_l^{\mathsf{H}} \big[\mathbf{H}_b \mathbf{w}_l x + \boldsymbol{\eta}_b\big]. \tag{6}$$

Hence, the achievable SNR for $l$-th transmission, $\gamma_{b,l}$, is

$$\gamma_{b,l} = \frac{P|\mathbf{f}_l^{\mathsf{H}} \mathbf{H}_b \mathbf{w}_l|^2}{\sigma_\eta^2}. \tag{7}$$

For the ideal case where Bob and Alice can respectively generate narrow beams towards the $l$-th beam-pair, i.e., $\mathbf{w}_l = \frac{1}{\sqrt{N_a}} \mathbf{a}_a(\theta_{b,l})$ and $\mathbf{f}_l = \frac{1}{\sqrt{N_b}} \mathbf{a}_b(\phi_{b,l})$, the SNR scales with the number of antennas at Alice and Bob (or, equivalently, the TX and RX antenna gains), i.e., $\gamma_{b,l} \propto N_a N_b$. We assume the Eve's channel matrix is unknown. The signal received at Eve after receive combining is

$$y_e = \mathbf{g}_l^H \mathbf{y}_e = \mathbf{g}_l^H [\mathbf{H}_e \mathbf{w}_l x + \boldsymbol{\eta}_e], \tag{8}$$

where $\mathbf{g}_l \in \mathbb{C}^{N_e}$ is the combiner used by Eve. Eve's achievable SNR, denoted by $\gamma_{e,l}$, depends on her eavesdropping capability, which is discussed in detail in Subsection III-D.

### C. Conditions for Physical Layer Security

Next, we state the conditions for achieving physical layer security. Let us assume that message $M$ is transmitted over the channel using $n$ times of transmissions, and the decoded message at Bob is $\hat{M}$. Assuming that the transmission occurs in $n$ channel uses (i.e., symbols), the two following conditions have to be satisfied to ensure a reliable and secure communication scheme between Alice and Bob [25], [28]:

$$\lim_{n\to\infty} \Pr(M \neq \hat{M}) = 0, \tag{9a}$$

$$\lim_{n\to\infty} \frac{1}{n} I(M; \mathbf{Z}^n) = 0, \tag{9b}$$

where $\Pr(\cdot)$ and $I(\cdot;\cdot)$ denote probability and mutual information, respectively, and $\mathbf{Z}^n$ is the Eve's observations during the $n$ transmissions. For a given realization of the wireless channels, the conditions in (9) are satisfied if the transmission rate, $R_{b,l}$, is bounded as [28]

$$R_{b,l} \leq [C_{b,l} - C_{e,l}]^+, \tag{10}$$

where $C_{b,l} = \log_2(1 + \gamma_{b,l})$, $C_{e,l} = \log_2(1 + \gamma_{e,l})$, and $[z]^+ \triangleq \max(0, z)$. Typically, it is assumed that Eve's CSI ($\mathbf{H}_e$ or $\gamma_{e,l}$) is known, based on which Alice can adapt the transmission rate according to (10) for ensuring a reliable and secure communication [28]. In mmWave communication systems, the channel strongly correlates to the TX's and RX's locations. Therefore, for realizing physical layer security in mmWave systems, it is helpful if Eve's location is known as assumed in [14], [15], and [16]. In this paper, we do not assume any channel knowledge regarding a particular Eve (neither the Eve's CSI nor her location). Rather, some degree of knowledge about the wireless channel itself is available i.e., radio map. This can be based on the empirical channel measurements between legitimate TXs and RXs collected over time. Moreover, we consider scenarios where the radio map is partially known, or that only room geometry is known. Finally, we also study where the channel of only legitimate TX/RX is known. In Section IV, we show that the proposed BeamSec can achieve physical layer security and adapt itself to the different degrees of channel knowledge.

### D. Attacker Model

Two attacker models are considered: single and colluding directional attackers. The attacker is a strong adversary with directional antennas capable of aligning her RX beam toward the best direction for overhearing Alice. Let the set of combiners used by the attacker be denoted by $\mathcal{G} = \{\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_{|\mathcal{G}|}\}$ then the achievable SNR for $l$-th path at Eve is given as:

$$\gamma_{e,l} = \max_{\mathbf{g}_i \in \mathcal{G}} \frac{P|\mathbf{g}_i^{\mathsf{H}} \mathbf{H}_e \mathbf{w}_l|^2}{\sigma_\eta^2}. \tag{11}$$

The colluding attacker is an even stronger adversary model that considers directional capabilities, with each Eve scanning the channel and selecting the best combiner for eavesdropping. In particular, we assume that a set of $Q$ eavesdroppers denoted by a set $\mathcal{Q} = \{1, 2, \ldots, Q\}$ scan the channel, and for each transmission, the signal with the maximum SNR is selected for eavesdropping. Let $\mathbf{H}_l^{(q)}$ be the channel of the $q$-th Eve and $\mathcal{G}^{(q)}$ be the set of combiners used by the $q$-th Eve, i.e., $\mathbf{g}^{(q)} \in \mathcal{G}^{(q)}$. This leads to the following achievable SNR for $Q$ colluding attackers

$$\gamma_{e,l} = \max_{q\in\mathcal{Q}} \max_{\mathbf{g}_i^{(q)} \in \mathcal{G}^{(q)}} \frac{P|(\mathbf{g}_i^{(q)})^{\mathsf{H}} \mathbf{H}_e^{(q)} \mathbf{w}_l|^2}{\sigma_\eta^2}. \tag{12}$$

## IV. BeamSec

BeamSec introduces a refined algorithm focused on minimizing communication interception while considering the availability of channel knowledge. As summarized in Algorithm 1, BeamSec achieves its goal in four steps: (*i*) clustering, AoD/AoA analysis of angular channel profile (ACP) followed by pre-selection strategies to identify the best diverse and distinct beam-pairs; In Step 1: BeamSec begins by gathering key data on available paths, such as channel impulse response (CIR), AoD, and AoA between the TX and RX. The algorithm then assigns the optimal AoA for each AoD based on the maximum CIR to create beam-pairs. Beams are clustered according to their angular profiles to identify diverse and distinct paths. Two pre-selection methods refine this process: (*a*) Maximizing angular separation, which orders beams to maximize the minimum separation between them, prioritizing AoD over AoA to reduce interference; and (*b*)

**Algorithm 1** BeamSec

**Step 1: Beam identification**

Run 802.11ad beam training at Alice and Bob.
For each beam-pair $(\mathbf{w}_l, \mathbf{f}_{l'})$ from TX codebook $\mathbf{w}_l \in \mathcal{W}$ and RX codebook $\mathbf{f}_{l'} \in \mathcal{F}$, estimate the CIR $h_{l,l'}$.
For each TX beam $l$, select the RX beam $l'$ with the highest CIR: $\text{argmax}_{l'} \ |h_{l,l'}|$.
Apply K-Means for clustering potential TX-RX pairs.
Add decodable and diverse TX-RX pairs in set of beams $\mathbf{L}$.
Apply pre-selection strategies to find the best set of beams for $\mathbf{L}$.

**Step 2: Time allocation**

**switch** time allocation policy **do**
  **case** RF map knowledge: Compute $T_l, \ \forall l \triangleright$ Eq. (18)
  **case** Room geometry knowledge: Compute $T_l, \ \forall l \triangleright$ Eq. (23)
  **case** Angular profile knowledge: Compute $T_l, \ \forall l \triangleright$ Eq. (28)
  **case** Uniform (no knowledge): Set $T_l = \frac{1}{L}, \ \forall l$.

**Step 3: Rate and codebook selection**

**switch** rate selection policy **do**
  **case** zero leakage: Compute $\bar{C}_s^{\text{abs}}$ and set $R_s \leq \bar{C}_s^{\text{abs}}$. $\triangleright$ Eq. (13)
  **case** given leakage probability: Set $R_s$ that yields $P_{\text{leak}}$. $\triangleright$ Eq. (15)
For given $R_s$ and $R_{b,l} < C_{b,l}, \ \forall l$, construct codebooks for secure message $\mathcal{C}_s$, beam-pair transmissions $\mathcal{C}_l, \ \forall l$, and $\mathcal{C} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_L$. The product codebook $\mathcal{C}$ is randomly partitioned into $2^{nR_s}$ parts.

**Step 4: Secure communication over selected beam-pairs**

*% Encoding:*
For each $nR_s$ information bits, select the corresponding secure message $W_s \in \mathcal{C}_s$.
For a given $W_s$, randomly select a codeword from the $W_s$th partition in $\mathcal{C}$, which comprises $L$ codewords from codebooks $\mathcal{C}_1, \ldots, \mathcal{C}_L$.
*% Transmission/Reception:*
**for** $l = 1, \ldots, L$ **do**
  Communicate the selected codeword from $\mathcal{C}_l$ using the corresponding TX-RX beam-pair $(\mathbf{w}_l, \mathbf{f}_l)$.
**end for**
*% Decoding:*
Decode all $L$ codewords from codebooks $\mathcal{C}_1, \ldots, \mathcal{C}_L$, respectively.
From codebook $\mathcal{C}$, identify the message $W_s$ and the corresponding bits.

Minimizing intersection, which arranges beams to minimize overlap, considering the room's geometry. Regardless of the chosen pre-selection strategy, the subsequent steps function effectively with any set of identified beams, (*ii*) time allocation among the selected beam-pairs; Rather than relying on perfect CSI or the precise location of the Eve, BeamSec leverages channel knowledge maps (CKMs) to allocate time among the selected beam-pairs. CKM, often referred to as radio maps in the literature, are typically constructed using estimated or modeled channel parameters associated with specific geographic locations or environmental layouts [29], [30], [31]. In our paper, we construct the CKM directly from empirical channel measurements, collected over time during beam training by different legitimate receivers located at different locations. In other words, the adopted CKM captures spatial variations in channel quality across the environment. While the Eve's exact location is unknown, we assume the CKM provides estimates of channel quality for any given location. Accordingly, BeamSec uses the empirical CKM to optimize beam selection and time allocation against the worst-case scenario for Eve's location. The CKM can be constructed using different types of channel information. In the RF map-based approach, they are created from empirical channel measurements gathered by the legitimate receiver at various points, as shown in Fig. 7. These measurements develop a spatial map of signal strengths to estimate the potential vulnerabilities and strengths of different beam-pairs. The CKM can also be constructed using a floor plan-based approach, where room dimensions and instantaneous CSI are combined with raytracing to identify potential beam intersection points and their corresponding secrecy capacities. Alternatively, the angular profile analysis constructs the CKM by defining regions based on AoD and AoA to represent the directional distribution of received power. Each of these CKMs provides a spatial representation that helps assess where beam-pairs might be more secure or vulnerable. Based on these, BeamSec intelligently allocates more time to secure paths and less time to potentially vulnerable ones. In scenarios where historical channel measurements are unavailable, instantaneous channel knowledge at the receiver is utilized, either through angular profile analysis or intersecting paths approaches, to maximize the overall secrecy rate. This enables informed decisions on beam selection and optimal time allocation without requiring the Eve's CSI or her location. In scenarios without any optimization, time allocation is uniform. However, in scenarios with partial channel knowledge or limited knowledge at the RX, time allocation is adjusted to enhance security; $(iii)$ rate and codebook selection; and finally $(iv)$ secure communication over the beam-pairs. The description of Steps 2 and 3 depends on the specific secure communication strategy adopted in Step 4. Therefore, in contrast to their logical implementation order 1-4, we explain Step 4 before Steps 2 and 3.

*Remark 2:* The cost of the proposed beam identification strategy is primarily tied to standard beam training and CSI feedback. Overhead is reduced by pre-selecting beam-pairs based on spatial diversity, and updates are only needed when legitimate TX or RX significantly move, minimizing the overall communication time and feedback frequency.

### A. Secure Coding Over Refined Beam-Pairs

BeamSec develops a refined codebook with a set of beam-pairs agreed upon between Alice and Bob. We index these beam-pairs by $l = 1, \ldots, L$, where $L$ is the total number of refined beam-pairs by BeamSec. The selected beam-pairs provide high channel capacity between Alice and Bob and

have minimal information leakage to potential Eves. Nonetheless, we consider a general setting where the fraction of time allocated to each beam-pair can be different and subject to optimization (see Section V for the proposed time allocation scheme). Let $T_l$ denote the fraction of time assigned to communication over path $l$, where $\sum_{l=1}^{L} T_l = 1$ and $T_l \geq 0$, $\forall l$, have to hold. Moreover, the transmitted data is split among the total number of beam-pairs, i.e., each beam-pair is assigned to transmit and receive its specific data part, with overhead comparable to standard beam training and resource allocation protocols. The secrecy is ensured by encoding information, not into the individual data segments sent over different beams, but rather by *jointly* encoding information across all $L$ beam-pairs. The code construction, encoding, and decoding adopted for BeamSec follow similar techniques as those for the general physical layer security schemes with partial channel knowledge; see, e.g., [25] for details. In the following, we describe an example of such joint coding from an information-theoretic perspective. Nonetheless, we emphasize that BeamSec is expected to improve secrecy regardless of the specific strategy adopted for joint coding across the beam-pairs. From an information-theoretical perspective, the code construction, encoding, and decoding employed in BeamSec align with techniques used in general physical layer security schemes with partial CSI (see, for instance, [32]). However, it is essential to note that BeamSec differs in that it does not presuppose any knowledge regarding Eve's location. Additionally, joint coding across transmissions along $L$ beam-pairs is necessary, as elaborated in [25]. For clarity, we provide a concise overview of the secure coding utilized herein and direct interested readers to [25] and [32] for comprehensive explanations. Let $n$ denote the number of symbols (channel uses) transmitted across all $L$ transmissions. We assume that Alice possesses the CSI of Bob's channel, while information regarding Eve's channel and her location remains unknown. *Code construction:* For the $l$-th beam-pair, codebook $\mathcal{C}_l$ comprising $2^{nT_l R_{b,l}}$ randomly generated codewords is adopted, where $R_{b,l} < C_{b,l} \triangleq \log_2(1+\gamma_{b,l})$[1] is the code rate in [bits/channel use] for the $l$-th beam-pair. The product codebook of all transmissions $\mathcal{C} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_L$ with size $|\mathcal{C}| = 2^{n\sum_{l=1}^{L} T_l R_{b,l}}$ is randomly partitioned into $2^{nR_s}$ disjoint partitions, where $R_s$ is the secrecy rate [bits/channel use]. The indices of partitions, denoted by $W_s \in \mathcal{C}_s \triangleq \{1, \ldots, 2^{nR_s}\}$, represent the secure messages. We assume that the knowledge of the adopted rates $R_{b,l}$ and $R_s$ and the corresponding codebooks $\mathcal{C}_1, \ldots, \mathcal{C}_L$ and $\mathcal{C}$ are shared between Alice and Bob. *Encoding:* For a given secure message $W_s \in \mathcal{C}_s$, a codeword is *randomly* selected from the $W_s$-th partition in product codebook $\mathcal{C}$. By construction, this product codeword comprises $L$ codewords of appropriate lengths sent consecutively along the $L$ beam-pairs. *Decoding:* Since $R_{b,l} < C_{b,l}$ holds for $\forall l$, Bob can reliably decode all codewords and recover message $W_s$ from the product codebook $\mathcal{C}$. Let $C_s$ denote the maximum achievable secrecy rate of BeamSec. Then, for $R_s \leq C_s$, the *random* partitioning of the product codebook $\mathcal{C}$ ensures that while Eve may be able to determine for some beam-pairs $l$ which codeword is sent from the codebook $\mathcal{C}_l$, she will be still unable to say which message $W_s$ is sent from $\mathcal{C}_s$, i.e., message $W_s$ remains secure.

[1]This bound relies on optimal coding (e.g., Gaussian signaling) and constitutes an upper bound on the achievable rate in practice.

### B. Secrecy Capacity

For the secure communication described above, Alice does not need to necessarily know the exact channel or location of Eve as long as she chooses a secure rate that meets $R_s \leq C_s$. In the following, we introduce a deterministic and a statistical measure to enforce the secrecy condition $R_s \leq C_s$ without knowing Eve's location/channel.

*1) Absolute Secrecy Rate:* Eve's SNR $\gamma_{e,l}$ depends on the channel matrix $\mathbf{H}_e$, which is unknown and depends on her location. Let $\mathbf{p}_e \in \mathcal{P}_e$ denote Eve's location where $\mathcal{P}_e$ denotes all possible Eve locations. A given hypothesis on $\mathbf{p}_e$ gives us certain knowledge about $\mathbf{H}_e$. For example, if $\mathbf{p}_e$ is close to Alice's location or is along the direction that the beamformer $\mathbf{w}_l$ targets, then we expect a stronger Eve's channel $\mathbf{H}_e$ and hence a larger $\gamma_{e,l}$. To formalize this concept, we assume that $\mathbf{H}_e \in \mathcal{H}_e(\mathbf{p}_e)$, where $\mathcal{H}_e(\mathbf{p}_e)$ denotes the set of all possible Eve's channel matrices $\mathbf{H}_e$ with structure in (2)–(4) given that Eve's location is $\mathbf{p}_e$. Based on this notation, the achievable absolute secrecy rate (i.e., zero information leakage) across all $L$ transmissions can be obtained as

$$\bar{C}_s^{\text{abs}} = \min_{\mathbf{p}_e \in \mathcal{P}_e} \sum_{l=1}^{L} T_l C_{s,l}(\mathbf{p}_e), \tag{13}$$

where

$$C_{s,l}(\mathbf{p}_e) = \left[C_{b,l} - \max_{\mathbf{H}_e \in \mathcal{H}_e(\mathbf{p}_e)} C_{e,l}(\mathbf{H}_e)\right]^+. \tag{14}$$

The operator $\max_{\mathbf{H}_e \in \mathcal{H}_e(\mathbf{p}_e)}$ corresponds to the worst-case channel realization given that Eve is at position $\mathbf{p}_e$ and the operator $\min_{\mathbf{p}_e \in \mathcal{P}_e}$ accounts for the worst-case location of Eve (in terms of secrecy rate). Thus, the secrecy rate in (13) accounts for all possible Eve's locations and *does not rely on the knowledge of actual Eve's location*. Hence, $R_s \leq \bar{C}_s^{\text{abs}}$ guarantees that no information is leaked to Eve, regardless of her location and the instantaneous channel quality.

*2) Information Leakage Probability:* The secrecy rate in (13) requires the quantification of worst-case Eve's rate for each Eve's location $\mathbf{p}_e$, i.e., $\max_{\mathbf{H}_e \in \mathcal{H}_e(\mathbf{p}_e)} C_{e,l}(\mathbf{H}_e)$. This quantity relies on the wireless channel, i.e., $\mathcal{H}_e(\mathbf{p}_e)$ which in practice can be obtained based on empirical measurements if sufficient measurements on different environment locations $\mathbf{p}$ have been collected by the *legitimate receiver*, which can be used as an approximation for Eve's channel, too, and is adopted in this paper. Note that, the value of the absolute secrecy rate in (13) can be quite small due to some worst-case Eve's channel conditions that occur extremely rarely. Hence, the absolute secrecy rate is a pessimistic measure of secrecy. Next, we introduce a general statistical secrecy measure, which includes the absolute secrecy rate as a special case. In particular, we quantify the *probability* that information is leaked to Eve when the transmitter transmits with a fixed rate $R_s$ [bits/s/Hz]. Therefore, the absolute secrecy rate corresponds to

the special case when the probability of information leakage is zero.

For a given rate $R_s$, information leakage probability, denoted by $P_{\text{leak}}$, can be formally defined as

$$P_{\text{leak}} = \Pr\left\{C_s(\mathbf{H}_e) \leq R_s\right\}, \tag{15}$$

where $C_s(\mathbf{H}_e)$ is the instantaneous achievable secrecy rate which is given by

$$C_s(\mathbf{H}_e) = \min_{\mathbf{p}_e \in \mathcal{P}_e} \sum_{l=1}^{L} T_l \left[C_{b,l} - C_{e,l}(\mathbf{H}_e)\right]^+, \tag{16}$$

where $\mathbf{H}_e \in \mathcal{H}_e(\mathbf{p}_e)$. Note that the key difference between the achievable absolute secrecy rate $\bar{C}_s^{\text{abs}}$ in (13) and the instantaneous achievable secrecy rate $C_s(\mathbf{H}_e)$ in (16) is that in (13), the worst-case realization is assumed for $\mathbf{H}_e$, whereas in (16), the actual (unknown) realization is assumed.

*Remark 3:* Note that the absolute secrecy rate in (13) and the information leakage probability in (15) are formulated for a single Eve. However, this formulation can be extended to account for colluding Eves. For example, for two colluding Eves, they are formulated respectively as follows:

$$\bar{C}_s^{\text{abs}} = \min_{\{\mathbf{p}_{e,i}, \mathbf{p}_{e,j}\} \subset \mathcal{P}_e} \sum_{l=1}^{L} T_l \, \min(C_{s,l}(\mathbf{p}_{e,i}), C_{s,l}(\mathbf{p}_{e,j}))$$

and

$$P_{\text{leak}} = \Pr\left\{C_s(\underline{\mathbf{H}}_e) \leq R_s\right\},$$

where $\underline{\mathbf{H}}_e = [\mathbf{H}_e(\mathbf{p}_{e,i}), \mathbf{H}_e(\mathbf{p}_{e,j})], \{\mathbf{p}_{e,i}, \mathbf{p}_{e,j}\} \subset \mathcal{P}_e$, $\mathbf{H}_e(\mathbf{p}_{e,i}) \in \mathcal{H}_e(\mathbf{p}_{e,i}), \ \forall \mathbf{p}_{e,i} \in \mathcal{P}_e$, and

$$C_s(\underline{\mathbf{H}}_e) = \min_{\{\mathbf{p}_{e,i}, \mathbf{p}_{e,j}\} \subset \mathcal{P}_e} \sum_{l=1}^{L} T_l \min_{k \in \{i,j\}} C_{s,l}(\mathbf{H}_e(\mathbf{p}_{e,k})),$$

where $C_{s,l}(\mathbf{H}_e(\mathbf{p}_{e,i})) = \left[C_{b,l} - C_{e,l}(\mathbf{H}_e(\mathbf{p}_{e,i}))\right]^+$. This formulation can be generalized to $Q$ colluding eavesdroppers too.

In the next section, we propose three different time allocation approaches for the refined beam-pairs based on the available channel knowledge.

## V. Time Allocation

To ensure reliable decoding at Bob, BeamSec requires that the quality of the legitimate link, i.e., $\gamma_{b,l}, \ \forall l$, to be known at Alice for choosing $R_{b,l} < C_{b,l}, \ \forall l$. This information is obtained through beam training. BeamSec does not require any instantaneous or statistical knowledge of the Eve's channel or her location. In fact, in principle, BeamSec works for any choices of the time assignments $T_l, \ \forall l$, and the transmission rate $R_s < \sum_{l=1}^{L} T_l C_{b,l} \triangleq C_b$. However, to ensure security, condition $R_s < C_s \leq C_b$ should be also met, either deterministically (i.e., $R_s < \bar{C}_s^{\text{abs}}$) or statistically (i.e., as in (15)). Here, we show that the values of $T_l, \ \forall l$ can be optimized depending on the knowledge that is available about the wireless channel (not any particular Eve). We consider the following scenarios:

- **RF map knowledge.** Since the Eve(s) and the legitimate RX access the same wireless channel, the empirical channel measurements collected by the legitimate RX over time (known as RF map [33], [34]) provide useful knowledge that can be exploited for optimizing the values of $T_l, \ \forall l$. Here, we study two cases: $(i)$ Full knowledge of RF map, where we assume empirical measurements of all points (in practice, sufficiently large) in $\mathcal{P}_e$ are available, and $(ii)$ Partial knowledge of RF map in which empirical measurements of only a subset of points $\hat{\mathcal{P}}_e \subset \mathcal{P}_e$ is known so far.
- **Instantaneous channel knowledge of the TX/RX.** In this case, we assume only the instantaneous channel between TX and RX is known, which is obtained via beam training. Using this knowledge, we aim to identify the most vulnerable locations for eavesdropping and then optimize $T_l, \ \forall l$, for these points. Here, we again consider two cases, where only the angular profile is known, where the room geometry (floor plan) is known in addition to the angular profile.

In the following, we propose our time allocation policies for the above scenarios.

### A. RF Map Knowledge

In this case, we assume that the Eve experiences the same channel statistics at location $\mathbf{p}_e$ as those measured empirically by the legitimate RX at location $\mathbf{p}_e$. Therefore, despite the unavailability of the current location of the Eve, an estimate of $\bar{C}_s^{\text{abs}}$, denoted by $\hat{\bar{C}}_s^{\text{abs}}$, can be computed from (13) based on the past empirical channel measurements (which can be available only for a subset of locations $\hat{\mathcal{P}}_e \subset \mathcal{P}_e$). The received power for all beams is measured at selected locations, i.e., $\hat{\mathcal{P}}_e$. With the above partial knowledge of the wireless channel, one can optimize $T_l, \forall l$, to maximize the secrecy rate. In particular, the optimization problem for maximizing the estimated achievable absolute secrecy rate $\hat{\bar{C}}_s^{\text{abs}}$ in terms of time variable $T_l$ can be formulated for single and the case of two colluding eavesdroppers as follows:

*1) Single eavesdropper:* The optimization problem for maximizing the absolute secrecy rate in case of a single Eve with unknown CSI and location information is formulated as

$$\begin{aligned} \max_{T_l, \forall l} \quad & \hat{\bar{C}}_s^{\text{abs}} = \min_{\mathbf{p}_e \in \hat{\mathcal{P}}_e} \sum_{l=1}^{L} T_l C_{s,l}(\mathbf{p}_e) \\ \text{s.t.} \quad & 0 \leq T_l \leq 1, \ \forall l, \ \text{and} \ \sum_{l=1}^{L} T_l = 1. \end{aligned} \tag{17}$$

Defining auxiliary optimization variable $t$ for the epigraph of the cost function, we can transform the above problem into

$$\begin{aligned} \max_{T_l, \forall l} \quad & t \\ \text{s.t.} \quad & \sum_{l=1}^{L} T_l C_{s,l}(\mathbf{p}_e) \geq t, \quad \forall \mathbf{p}_e \in \hat{\mathcal{P}}_e \\ & 0 \leq T_l \leq 1, \ \forall l, \ \text{and} \ \sum_{l=1}^{L} T_l = 1. \end{aligned} \tag{18}$$

*2) Colluding eavesdroppers ($Q = 2$):* Since the locations of eavesdroppers are unknown, all possible combinations of their locations must be considered for maximizing absolute secrecy rate, leading to the following optimization problem

$$\max_{T_l,\forall l} \quad \hat{\hat{C}}_s^{\text{abs}} = \min_{\{\mathbf{p}_{e,i},\mathbf{p}_{e,j}\}\subset\mathcal{P}_e} \sum_{l=1}^{L} T_l \, \min(C_{s,l}(\mathbf{p}_{e,i}), C_{s,l}(\mathbf{p}_{e,j}))$$
$$\text{s.t.} \quad 0 \le T_l \le 1, \ \forall l, \ \text{and} \ \sum_{l=1}^{L} T_l = 1, \tag{19}$$

which can be transformed into

$$\max_{T_l,\forall l} \quad t$$
$$\text{s.t.} \quad \sum_{l=1}^{L} T_l \, \min(C_{s,l}(\mathbf{p}_{e,i}), C_{s,l}(\mathbf{p}_{e,j})) \ge t,$$
$$\forall \{\mathbf{p}_{e,i}, \mathbf{p}_{e,j}\} \subset \hat{\mathcal{P}}_e,$$
$$0 \le T_l \le 1, \ \forall l, \ \text{and} \ \sum_{l=1}^{L} T_l = 1. \tag{20}$$

The above optimization problems become linear programming respectively with $|\hat{\mathcal{P}}_e| + L + 1$ and $\binom{|\hat{\mathcal{P}}_e|}{2} + L + 1$ linear constraints for single and two colluding eavesdroppers, which can be solved using standard numerical solvers for convex optimization, e.g., CVX [35]. The time optimization problem with colluding eavesdroppers in (20) is more complex compared to that with single Eve in (18). However, it is obvious that the maximum absolute secrecy capacity with colluding eavesdroppers is less than that with a single Eve, and as the number of colluding eavesdroppers increases the maximum absolute secrecy capacity decreases.

### B. Instantaneous Channel Knowledge of TX/RX

In this subsection, we focus on the problem of time allocation only for the case of single Eve. Next, we assume that only the knowledge of SNRs ($\gamma_{b,l}$), AoDs, and AoAs for $L$ beams between TX and RX is available. Although compared to the RF map, less information is available in this scenario, it can still be exploited as a basis for optimizing $T_l$, $\forall l$. For instance, if two beams are very close in the angular profile, it is more likely that both can be simultaneously intercepted by one Eve and, hence, should not be activated simultaneously. Next, we consider two cases depending on whether the floor plan is known or not.

*1) Room Geometry Knowledge (Floor Plan):* The knowledge of the floor plan helps us identify if two beams are intersected. The intersection constitutes a worst-case location for secure communication since Eve can simultaneously intercept the intersecting beams at this location. To formally state the proposed time-allocation policy, we make the following assumptions:

A1: We assume that the beams are modeled with ideal rays.

A2: We assume that Eve can fully intercept the link if she is located on the beam path, but there is no information leakage from a beam to Eve when she is not located along the path of that beam.

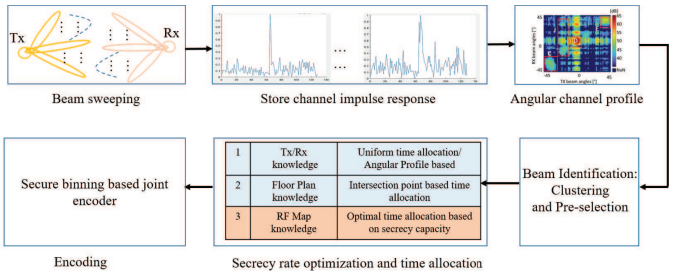



Fig. 3. An overview of BeamSec procedure.

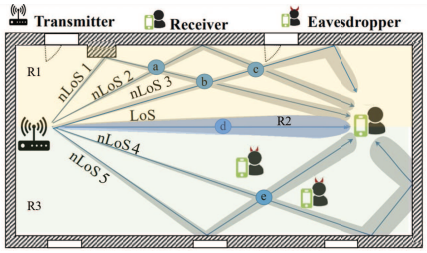



Fig. 4. Beam trajectories and their sub-regions: $R_1$–$R_3$.

A3: We assume the dominant channel effects are path loss and reflection (i.e., we neglect scattering, diffraction, etc.).

Note that assumptions A1-A3 are reasonable in mmWave communication systems, where the channel is sparse and highly directional beams are adopted.

Let us define $\mathcal{L}(\mathbf{p}_e)$ as a set of beams whose trajectories pass through point $\mathbf{p}_e$. Under assumptions A1-A3, the secrecy capacity for beam $l$ at position $\mathbf{p}_e$ is approximated as

$$C_{s,l}(\mathbf{p}_e) = \begin{cases} 0, & \text{if } l \in \mathcal{L}(\mathbf{p}_e) \\ C_{b,l}, & \text{otherwise.} \end{cases} \tag{21}$$

Note that having the floor plan, $C_{s,l}(\mathbf{p}_e)$ can be computed for all relevant points $\mathbf{p}_e \in \mathcal{P}_e$ based on standard raytracing algorithm [36]. Substituting $C_{s,l}(\mathbf{p}_e)$ from (21) for all $\mathbf{p}_e \in \mathcal{P}_e$ into (17), we can readily obtain the optimized $T_l$, $\forall l$. However, it is possible to significantly reduce the complexity of solving (17) if we identify only the most vulnerable points for eavesdropping. As discussed before, these are the points where multiple beams intersect. To illustrate how these points can be identified, we focus on first-order reflections, which, in mmWave channels, are often the dominant paths after the LoS path. Let us assume a rectangular floor plan, see Fig. 4. Focusing on the first-order reflections, the trajectories of the beams divide the area into three distinct sub-regions, as depicted in Fig. 4. The upper sub-area, i.e., R1, is traversed by the paths of certain targeted beams (beams characterized by negative AoDs and positive AoAs). The second sub-area, i.e., R2, represents the LoS, through which a single beam's path is established (beams defined by zero AoD and zero AoA). The lower sub-area, i.e., R3, accommodates the paths of other targeted beams (beams with positive AoDs and negative AoAs). *It is important to note that although sub-regions R1 and R3 are both classified as nLoS, they represent distinct spatial clusters. Beyond mere differences in AoA and AoD, these clusters exhibit unique multi-path characteristics–such as different delay profiles and power distributions–stemming from variations in the scattering*

*environment, which justify their separate treatment in our beam selection and optimization process.* As observed in Fig. 4, every combination of beams within the upper (or lower) sub-area has one intersection point. Let us define set $\hat{\mathcal{P}}'_e$, which contains only the intersection points for the interesting beams and one point on the beams that have no intersection with other beams. In the following lemma, we introduce a subset of $\hat{\mathcal{P}}^*_e$, which contains the bottleneck points.

*Lemma 1:* For scenario floor plan, where $C_{s,l}(\mathbf{p}_e)$ is obtained from (21), without loss of generality the set $\hat{\mathcal{P}}'_e$ can be reduced into a subset $\hat{\mathcal{P}}^*_e \subseteq \hat{\mathcal{P}}'_e$ where

$$\hat{\mathcal{P}}^*_e = \{\mathbf{p}^i_e \in \hat{\mathcal{P}}'_e | \nexists \mathbf{p}^j_e \in \hat{\mathcal{P}}^*_e : \mathcal{L}(\mathbf{p}^i_e) \subseteq \mathcal{L}(\mathbf{p}^j_e)\}. \tag{22}$$

*Proof:* Let us define $\mathbf{p}^{\min}_e = \operatorname{argmin}_{\mathbf{p}_e \in \hat{\mathcal{P}}'_e} \bar{C}_s(\mathbf{p}_e, \mathbf{T}^*)$, where $\bar{C}_s(\mathbf{p}_e, \mathbf{T}^*) = \sum_{l=1}^{L} T^*_l C_{s,l}(\mathbf{p}_e)$ and $\mathbf{T}^* = [T^*_1, \ldots, T^*_L]$. To prove this lemma, we use contradiction. Thus, we assume that $\hat{\mathcal{P}}^*_e$ is not a comprehensive subset of $\hat{\mathcal{P}}'_e$. Therefore, $\mathbf{p}^{\min}_e \notin \hat{\mathcal{P}}^*_e$ and $\forall \mathbf{p}_e \in \hat{\mathcal{P}}^*_e : \bar{C}_s(\mathbf{p}_e, \mathbf{T}^*) > \bar{C}_s(\mathbf{p}^{\min}_e, \mathbf{T}^*)$. Since, $\mathbf{p}^{\min}_e \in \hat{\mathcal{P}}'_e - \hat{\mathcal{P}}^*_e$, we have $\exists \mathbf{p}^j_e \in \hat{\mathcal{P}}^*_e : \mathcal{L}(\mathbf{p}^{\min}_e) \subseteq \mathcal{L}(\mathbf{p}^j_e)$. If $\mathcal{L}(\mathbf{p}^{\min}_e) = \mathcal{L}(\mathbf{p}^j_e)$, $\bar{C}_s(\mathbf{p}^{\min}_e, \mathbf{T}^*) - \bar{C}_s(\mathbf{p}^j_e, \mathbf{T}^*) = 0$. Otherwise, we have $\mathcal{L}(\mathbf{p}^{\min}_e) \subset \mathcal{L}(\mathbf{p}^j_e)$. From (22), we conclude that $\mathbf{p}^j_e \in \hat{\mathcal{P}}^*_e$. Therefore, there exists at least one beam $l_j \in \mathcal{L}(\mathbf{p}^j_e)$, where $l_j \notin \mathcal{L}(\mathbf{p}^{\min}_e)$. Thus, we have

$$\begin{aligned}
&\bar{C}_s(\mathbf{p}^{\min}_e, \mathbf{T}^*) - \bar{C}_s(\mathbf{p}^j_e, \mathbf{T}^*) \\
&= \sum_{l \notin \mathcal{L}(\mathbf{p}^{\min}_e)} T^*_l C_{s,l}(\mathbf{p}^{\min}_e) - \sum_{l \notin \mathcal{L}(\mathbf{p}^j_e)} T^*_l C_{s,l}(\mathbf{p}^j_e) \\
&\overset{(a)}{\geq} T^*_{l_j} C_{b,l_j} \geq 0,
\end{aligned} \tag{23}$$

where (a) follows from (21). If $\bar{C}_s(\mathbf{p}^{\min}_e, \mathbf{T}^*) - \bar{C}_s(\mathbf{p}^j_e, \mathbf{T}^*) > 0$, it means that $\mathbf{p}^{\min}_e$ is not the worst case point, and if $\bar{C}_s(\mathbf{p}^{\min}_e, \mathbf{T}^*) - \bar{C}_s(\mathbf{p}^j_e, \mathbf{T}^*) = 0$, the minimum secrecy capacity is still achievable on point $\mathbf{p}^j_e \in \hat{\mathcal{P}}^*_e$. This completes the proof. ■

According to Lemma 1, the maximum cardinality of $\hat{\mathcal{P}}^*_e$ is equal to the maximum number of non-subset subsets. Thus, we have $|\hat{\mathcal{P}}^*_e| \leq \binom{L}{\lfloor L/2 \rfloor}$.

The following lemma reveals an interesting property of the optimal solution to (17) when the approximate secrecy capacities in (21) are adopted and without loss of generality, $\hat{\mathcal{P}}^*_e$ is the reduced subset of $\hat{\mathcal{P}}'_e$ defined in (22).

*Lemma 2:* Let us define $\mathbf{p}^{\min}_e = \operatorname{argmin}_{\mathbf{p}_e \in \hat{\mathcal{P}}^*_e} \bar{C}_s(\mathbf{p}_e, \mathbf{T}^*)$, where $\bar{C}_s(\mathbf{p}_e, \mathbf{T}^*) = \sum_{l=1}^{L} T^*_l C_{s,l}(\mathbf{p}_e)$ and $\mathbf{T}^* = [T^*_1, \ldots, T^*_L]$. For scenario floor plan, where $C_{s,l}(\mathbf{p}_e)$ is obtained from (21), $\mathbf{p}^{\min}_e \in \hat{\mathcal{P}}^*_e$ is not a unique point (if $|\hat{\mathcal{P}}^*_e| \geq 2$).

*Proof:* We use contradiction to prove this lemma. So, we assume that $\mathbf{p}^{\min}_e \in \hat{\mathcal{P}}^*_e$ is a unique point. Therefore, $\forall\ \mathbf{p}'_e \in \hat{\mathcal{P}}^*_e$ where $\mathbf{p}'_e \neq \mathbf{p}^{\min}_e$, we have

$$\bar{C}_s(\mathbf{p}'_e, \mathbf{T}^*) > \bar{C}_s(\mathbf{p}^{\min}_e, \mathbf{T}^*). \tag{24}$$

According to (21), we have $\bar{C}_s(\mathbf{p}_e, \mathbf{T}^*) = \sum_{l \in \mathcal{L}^c(\mathbf{p}_e)} T^*_l C_{b,l}$, where $\mathcal{L}^c(\mathbf{p}_e) = \{1, \cdots, L\} - \mathcal{L}(\mathbf{p}_e)$. As a result,

$$\begin{aligned}
&\bar{C}_s(\mathbf{p}'_e, \mathbf{T}^*) - \bar{C}_s(\mathbf{p}^{\min}_e, \mathbf{T}^*) \\
&\quad = \sum_{l \in \mathcal{L}^c(\mathbf{p}'_e)} T^*_l C_{b,l} - \sum_{l \in \mathcal{L}^c(\mathbf{p}^{\min}_e)} T^*_l C_{b,l}
\end{aligned} \tag{25}$$


(a) Corollary 1 (b) Corollary 2

Fig. 5. Two examples.

If $\mathcal{L}^c(\mathbf{p}'_e) = \mathcal{L}^c(\mathbf{p}^{\min}_e)$, (25) results in

$$\bar{C}_s(\mathbf{p}'_e, \mathbf{T}^*) - \bar{C}_s(\mathbf{p}^{\min}_e, \mathbf{T}^*) = 0,$$

which contradicts (24). Otherwise, $\mathcal{L}^c(\mathbf{p}'_e) \neq \mathcal{L}^c(\mathbf{p}^{\min}_e)$, and three cases are possible:

I) $\mathcal{L}^c(\mathbf{p}'_e) \subseteq \mathcal{L}^c(\mathbf{p}^{\min}_e)$. Thus, $\mathcal{L}(\mathbf{p}^{\min}_e) \subseteq \mathcal{L}(\mathbf{p}'_e)$. Based on (22), $\mathbf{p}^{\min}_e \notin \hat{\mathcal{P}}^*_e$, which contradicts our assumption.

II) $\mathcal{L}^c(\mathbf{p}^{\min}_e) \subseteq \mathcal{L}^c(\mathbf{p}'_e)$. Thus, $\mathcal{L}(\mathbf{p}'_e) \subseteq \mathcal{L}(\mathbf{p}^{\min}_e)$. Based on (22), $\mathbf{p}'_e \notin \hat{\mathcal{P}}^*_e$, which contradicts our assumption.

III) $\mathcal{L}^c(\mathbf{p}'_e) \nsubseteq \mathcal{L}^c(\mathbf{p}^{\min}_e)$ and $\mathcal{L}^c(\mathbf{p}^{\min}_e) \nsubseteq \mathcal{L}^c(\mathbf{p}'_e)$. If $\forall l_1 \in \mathcal{L}^c(\mathbf{p}'_e) - \mathcal{L}^c(\mathbf{p}^{\min}_e) : T^*_{l_1} = 0$, from (25) we have

$$\bar{C}_s(\mathbf{p}'_e, \mathbf{T}^*) - \bar{C}_s(\mathbf{p}^{\min}_e, \mathbf{T}^*) \leq \sum_{l \in \mathcal{L}^c(\mathbf{p}'_e) - \mathcal{L}^c(\mathbf{p}^{\min}_e)} T^*_l C_{b,l} \leq 0, \tag{26}$$

which contradicts the definition of $\mathbf{p}^{\min}_e$. Therefore, $\exists l_1 \in \mathcal{L}^c(\mathbf{p}'_e) - \mathcal{L}^c(\mathbf{p}^{\min}_e) : T^*_{l_1} > 0$. Since $\mathcal{L}^c(\mathbf{p}^{\min}_e)$ is non-empty, $\exists l_2 \in \mathcal{L}^c(\mathbf{p}^{\min}_e)$. Let us define $\mathbf{T}^{\text{new}}$, where $T^{\text{new}}_{l_1} \doteq T^*_{l_1} - \epsilon$, where $\epsilon > 0, \epsilon \to 0$, $T^{\text{new}}_{l_2} \doteq T^*_{l_2} + \epsilon$, and $T^{\text{new}}_l \doteq T^*_l$, $\forall l \neq l_1, l_2$. We have

$$\begin{aligned}
&\bar{C}_s(\mathbf{p}^{\min}_e, \mathbf{T}^{\text{new}}) - \bar{C}_s(\mathbf{p}^{\min}_e, \mathbf{T}^*) \\
&\quad = \sum_{l \in \mathcal{L}^c(\mathbf{p}^{\min}_e)} T^{\text{new}}_l C_{b,l} - \sum_{l \in \mathcal{L}^c(\mathbf{p}^{\min}_e)} T^*_l C_{b,l} \\
&\quad = (T^{\text{new}}_{l_2} - T^*_{l_2}) C_{b,l_2} > 0.
\end{aligned} \tag{27}$$

So, $\mathbf{T}^*$ cannot be the optimal time allocation. ■

In the following, we present two corollaries to provide some analytical insights into the optimal time allocation.

*Corollary 1:* Consider two available beams, denoted as $l_1$ and $l_2$, which do not intersect (see Fig. 5-(a)). Without loss of generality, we assume $C_{b,l_1} > C_{b,l_2}$. According to Lemma 2, the allocated times are given by $T^*_{l_1} = \frac{C_{b,l_2}}{C_{b,l_1} + C_{b,l_2}}$ and $T^*_{l_2} = \frac{C_{b,l_1}}{C_{b,l_1} + C_{b,l_2}}$.

*Proof:* Let us consider non-intersecting beams $l_1$ and $l_2$ as mentioned in Corollary 1, we need to consider at least two points: $\mathbf{p}^1_e$ on $l_1$ and $\mathbf{p}^2_e$ on $l_2$. Therefore, $\mathcal{L}(\mathbf{p}^1_e) = \{l_1\}$, $\mathcal{L}(\mathbf{p}^2_e) = \{l_2\}$, and $\hat{\mathcal{P}}^*_e = \{\mathbf{p}^1_e, \mathbf{p}^2_e\}$. Note that if we select another point $\mathbf{p}^j_e$ on $l_i, i \in \{1, 2\}$, then, according to Lemma 1, we have $\mathbf{p}^j_e \notin \hat{\mathcal{P}}^*_e$. Since, $\mathcal{L}(\mathbf{p}^j_e) \in \{l_1, l_1\} \subseteq \mathcal{L}(\mathbf{p}^i_e)$. Therefore, we have only two bottleneck points $\mathbf{p}^1_e$ and $\mathbf{p}^2_e$. Now, we apply Lemma 2. From Lemma 2, we know that $\mathbf{p}^{\min}_e$ is not unique. Therefore, $\bar{C}_s(\mathbf{p}^{\min}_e, \mathbf{T}^*) = \bar{C}_s(\mathbf{p}^1_e, \mathbf{T}^*) = \bar{C}_s(\mathbf{p}^2_e, \mathbf{T}^*)$. As a result, $T^*_2 C_{b,l_2} = T^*_1 C_{b,l_1}$. From this equation and $T^*_1 + T^*_2 = 1$, we conclude that $T^*_1 = \frac{C_{b,l_2}}{C_{b,l_1} + C_{b,l_2}}$ and $T^*_2 = \frac{C_{b,l_1}}{C_{b,l_1} + C_{b,l_2}}$. ■

*Corollary 2:* Consider three available beams, denoted as $l_1$, $l_2$, and $l_3$, where only $l_2$ and $l_3$ intersect (see Fig. 5-(b)).

Without loss of generality, we assume $C_{b,l_2} > C_{b,l_3}$. According to Lemma 2, the allocated times are determined as follows: $T^*_{l_1} = \frac{C_{b,l_2}}{C_{b,l_1}+C_{b,l_2}}$, $T^*_{l_2} = \frac{C_{b,l_1}}{C_{b,l_1}+C_{b,l_2}}$, and $T^*_{l_3} = 0$.

*Proof:* We select two points: $\mathbf{p}_e^1$ on $l_1$ and $\mathbf{p}_e^2$ on the intersection of $l_2$ and $l_3$. Therefore, $\mathcal{L}(\mathbf{p}_e^1) = \{l_1\}$, $\mathcal{L}(\mathbf{p}_e^2) = \{l_2, l_3\}$, and $\hat{\mathcal{P}}^*_e = \{\mathbf{p}_e^1, \mathbf{p}_e^2\}$. Note that if we select another point $\mathbf{p}_e^j$ on $l_i, i \in \{1,2,3\}$, then, according to Lemma 1, we have $\mathbf{p}_e^j \notin \hat{\mathcal{P}}^*_e$. Since $\mathcal{L}(\mathbf{p}_e^j) \in \{l_1, l_2, l_3\} \subseteq \mathcal{L}(\mathbf{p}_e^i), i \in \{1,2\}$. Therefore, we have only two bottleneck points $\mathbf{p}_e^1$ and $\mathbf{p}_e^2$. Now we apply Lemma 2. From Lemma 2, we know that $\mathbf{p}_e^{\min}$ is not unique. Therefore, $\bar{C}_s(\mathbf{p}_e^{\min}, \mathbf{T}^*) \doteq \bar{C}_s(\mathbf{p}_e^1, \mathbf{T}^*) = \bar{C}_s(\mathbf{p}_e^2, \mathbf{T}^*)$. As a result, $T_2^* C_{b,l_2} + T_3^* C_{b,l_3} = T_1^* C_{b,l_1}$. The times are allocated to maximize the total capacity. Since $C_{b,l_2} > C_{b,l_3}$, we have $T^*_{l_3} = 0$, $T_1^* = \frac{C_{b,l_2}}{C_{b,l_1}+C_{b,l_2}}$, and $T_2^* = \frac{C_{b,l_1}}{C_{b,l_1}+C_{b,l_2}}$. Note that $T^*_{l_2}$ and $T^*_{l_3}$ have an equal shared budget in the condition $T_1^* + T_2^* + T_3^* = 1$, with different contributions to the total capacity $C_{b,l_2} > C_{b,l_3}$. Thus, the maximum capacity is obtained when $T_3^* = 0$. Therefore, we obtain $T^*_{l_1} = \frac{C_{b,l_2}}{C_{b,l_1}+C_{b,l_2}}$, $T^*_{l_2} = \frac{C_{b,l_1}}{C_{b,l_1}+C_{b,l_2}}$, and $T^*_{l_3} = 0$. ■

*Remark 4:* Corollary 1 shows that for non-intersecting beams, more time is allocated to the weaker beam in order to exploit the diversity of the two beams for secure communication. While Corollary 2 reveals that among intersecting beams, only the stronger beam is allocated a non-zero time.

*2) Angular Profile Knowledge:* Here, we assume the floor plan is unknown, and we only have access to the angular profile of the link between TX and the legitimate RX. Based on this limited knowledge, we cannot guarantee an absolute secrecy rate; nonetheless, we can use this information to optimize the time allocation variable $T_l$, $\forall l$. In fact, considering that the transmitter beams have side lobes and even the main lobe has a certain beam width, it is reasonable to choose beams that are well separated. Otherwise, it is more likely that an Eve can simultaneously intercept multiple beams.

Let us show the AoD by $\theta$ and the AoA by $\phi$. For each beam $l$ in the angular profile, we can define a rectangular region $\theta \in [\theta_l^-, \theta_l^+]$ and $\phi \in [\phi_l^-, \phi_l^+]$, representing the angular intervals that surround the total received power of that specific beam. In fact, the beam's transmitted power is never received at AoA $\phi \notin [\phi_l^-, \phi_l^+]$, and the received power from this beam was not transmitted from AoD $\theta \notin [\theta_l^-, \theta_l^+]$.

In this method, we do not have any knowledge about the channel, but the angular profile at TX and RX is available. For example, the AoD of a beam specifies the first points on the path of that beam. Thus, as a metric for optimizing $T_l, \forall l$, we define the maximum achievable secrecy capacity at the beginning and ending points of a beam's path, denoted by $C_{s,\text{AoD}}$ and $C_{s,\text{AoA}}$, respectively. Then, we consider the worst case, i.e., $\min(C_{s,\text{AoD}}, C_{s,\text{AoA}})$, as an approximation for the secrecy capacity of the system.

We know that if beam $l$ is transmitted, the Eve can intercept it when she is located along $\theta \in [\theta_l^-, \theta_l^+]$ or $\phi \in [\phi_l^-, \phi_l^+]$. As a result, the secrecy capacity of beam $l$ based on TX knowledge is defined as

$$\tilde{C}_{s,\text{AoD},l}(\theta) \doteq \begin{cases} 0, & \text{if } \theta \in [\theta_l^-, \theta_l^+] \\ C_{b,l}, & \text{otherwise.} \end{cases}$$

The secrecy capacity across all beams based on TX knowledge is defined as

$$C_{s,\text{AoD}} = \min_{\theta} \sum_{l=1}^{L} T_l \tilde{C}_{s,\text{AoD},l}(\theta).$$

Similarly, based on RX knowledge, the secrecy capacity of beam $l$ is defined as

$$\tilde{C}_{s,\text{AoA},l}(\phi) \doteq \begin{cases} 0, & \text{if } \phi \in [\phi_l^-, \phi_l^+] \\ C_{b,l}, & \text{otherwise.} \end{cases}$$

The secrecy capacity across all beams based on RX knowledge is defined as

$$C_{s,\text{AoA}} = \min_{\phi} \sum_{l=1}^{L} T_l \tilde{C}_{s,\text{AoA},l}(\phi).$$

Therefore, the total secrecy capacity for angular profile based on the TX and RX knowledge is $C_s = \min(C_{s,\text{AoD}}, C_{s,\text{AoA}})$, and the optimal time allocation for this scheme is obtained as

$$\max_{T_l, \forall l} \; C_s = \min(C_{s,\text{AoD}}, C_{s,\text{AoA}})$$
$$\text{s.t.} \;\; 0 \le T_l \le 1, \;\; \forall l, \text{and} \sum_{l=1}^{L} T_l = 1. \tag{28}$$

The above optimization approach is linear in $T_l, \forall l$ and hence can be efficiently solved using the standard numeric solvers such as CVX [35].

## VI. Experimental Evaluation

We implemented BeamSec on an SDR-based testbed using the Xilinx RFSoC ZCU111 for baseband processing and a SiversIMA transceiver for the 60 GHz RF front-end with 2 GHz bandwidth (see Fig. 6). The RF front-end has a 16-element phased-array antenna with analog beamforming, using an open-source 802.11ad/ay implementation [37]. Each TX and RX beamformer used a codebook size of 64 provided by SIVERS [38]. Due to space limitations, we do not refer codebook; however, we would like to highlight that our approach is generalizable and not tied to the specific codebook adopted in our paper. Alice and Bob, the legitimate parties, synchronize using the 802.11ad protocol and agree on beam-switching intervals post-optimization. Eve, the adversary, is synchronized

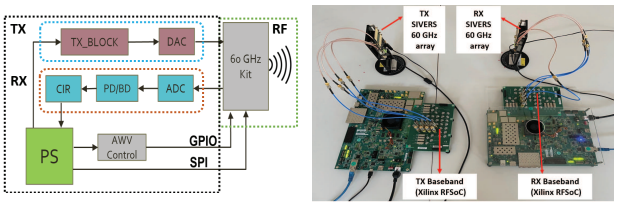



Fig. 6. An overview of our 60GHz testbed including Baseband (Xilinx RFSoC) and RF transceiver (60GHz phased arrays).

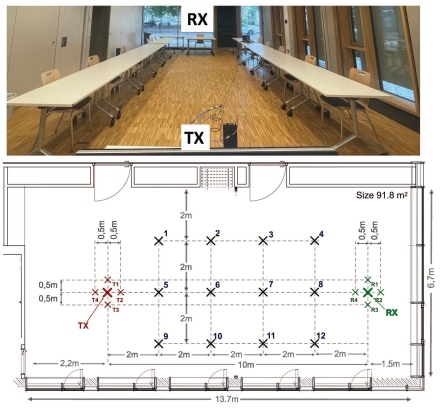



Fig. 7. Overview and layout of the seminar room and the exact location of measurement points.

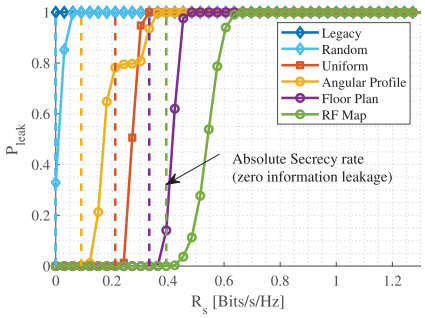



Fig. 8. Information leakage probabilities for $L = 7$, highlighting differences between schemes with a moderate path count.

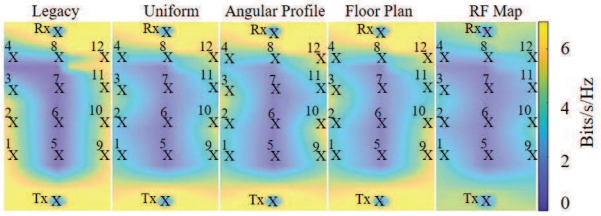



Fig. 9. Absolute secrecy rate ($\bar{C}_s^{\text{abs}}$) heatmap. BeamSec achieves a 58.13% increase using floor plan-based instantaneous RX channel knowledge and a 124.86% increase with partial RF map knowledge, compared to naive uniform allocation for $L = 7$.

with Alice to model a realistic attack scenario. The setup was tested in a 91.8 $m^2$ seminar room with typical indoor furnishings, with the antenna placed 75 cm above the floor and experiments conducted during office hours without human presence. The phased array covered $\pm 45°$ and was extended to $\pm 135°$ by rotating the antenna. The room layout and Eve's positions are depicted in Fig. 7. We validated BeamSec against two attack models: $(i)$ Single attacker and $(ii)$ Colluding attackers. We conducted real-time data collection with offline processing of 100 packets per beam pair, adhering to the standard 802.11ad synchronization process and predefined beam switching intervals. Each measurement was repeated 100 times per path, yielding $L \times 100$ packets per location, with the total transmission period (T) limited to 100 packets[2] and allocated across paths. Due to SDR hardware limitations, time allocation optimization was performed offline in MATLAB to validate BeamSec principles. The BeamSec algorithm requires feedback from the RX (Bob) to the TX (Alice) regarding SNR values $\gamma_{b,l}$ for this optimization. Empirical channel measurements were collected at various seminar room points (see Fig. 7), and used to create channel knowledge map. This data, collected over time by the legitimate RX, can aid in channel knowledge map reconstruction. Comprehensive experiments were conducted BeamSec in indoor settings against single and colluding eavesdroppers, focusing on information leakage and absolute secrecy. Evaluation considered: $(i)$ *Legacy scheme:* Uses only LoS to benchmark the need for multiple paths. $(ii)$ *Uniform time allocation:* Serves as a baseline for different time allocation schemes with varying channel knowledge. $(iii)$ *Random beam selection [24]:* Highlights the necessity of diverse beams over random selection. These schemes do not require specific wireless channel knowledge or changes in codeword length. Given that $\bar{C}_s^{\text{abs}}$ is unknown, ensuring zero information leakage (i.e., valid when $R_s < \bar{C}_s^{\text{abs}}$) is infeasible; thus, information leakage probability is used as a performance metric. While this study focuses on time allocation for maximizing $\bar{C}_s^{\text{abs}}$, optimizing $T_l$ for a fixed rate $R_s$ to minimize $P_{\text{leak}}$ is a potential future research direction. We demonstrate in Section VI that time allocations $T_l$ for maximizing $\bar{C}_s^{\text{abs}}$ significantly improve $P_{\text{leak}}$ compared to the uniform time allocation baseline.

*Remark 5:* We note that the effectiveness of our time allocation optimization in Section V depends on the quality of channel knowledge. Fig. 11 in [1], which is our previous work, demonstrates that increasing the number of measurement points leads to higher absolute secrecy rates. Notably, in our indoor scenario, a moderate measurement density (approximately 1–2 m spacing) is sufficient to capture the essential spatial variations; beyond this point, the secrecy rate saturates, and further increases yield only marginal gains. Hence, we use 12 observation points, see Fig. 7, throughout the experiments presented in this section.

### A. Single Eavesdropper

In the following, we present results first in terms of information leakage probability which includes the absolute secrecy rate as a special case and, subsequently, we focus on the absolute secrecy rate.

*1) Information Leakage Probability:* In Fig. 8, we demonstrate the probability of leakage, $P_{\text{leak}}$, versus the transmission rate, $R_s$, under BeamSec with instantaneous channel knowledge or RF map knowledge[3] in comparison with the legacy approach (i.e., choosing the best beam). The absolute secrecy rate, $\bar{C}_s^{\text{abs}}$, can be inferred from the leakage probability by identifying the maximum rate $R_s$ for which $P_{\text{leak}}$ is zero. First, we observe from Fig. 8 that the legacy approach leads to nearly complete leakage even for very low data rates.

[2]Constrained by ZCU111 RAM capacity.

[3]As explained in Section V, partial knowledge refers to having sparse measurement of the wireless channel in the room, see Fig. 7.

This observation is attributed to the fact that the LoS link is highly exposed to attackers, particularly those who benefit from higher directional antenna gain. While mmWave beams are highly directional, the legacy scheme focuses on a single beam, typically the LoS path. If Eve is aligned with this path, she can fully intercept the communication. This is why complete leakage is possible in the legacy scheme if Eve is on the same path as Alice and Bob. Similarly, random beam selection [24] also leads to complete leakage because it ignores the individual security properties of each path, such as their susceptibility to eavesdropping or spatial diversity. This approach increases the chance of selecting paths with low secrecy rates or those that overlap significantly with the Eve's position, maximizing their signal strength and minimizing secrecy. Without strategic use of channel knowledge, random selection frequently hits the weakest links, allowing an Eve to intercept and decode nearly all transmitted information. On the contrary, (*i*) *Uniform time allocation:* BeamSec provides a non-zero secure rate without channel knowledge of the environment by just exploiting the distinct and diverse beams. For $L = 7$ beams, it achieves zero information leakage up to $R_s \leq 0.212$ [Bits/s/Hz] (Fig. 8), (*ii*) *Partial RF map:* Utilizing sparse channel measurements, achieves zero leakage up to $R_s \leq 0.394$ [Bits/s/Hz] for $L = 7$. Improves secrecy performance by ∼85.7% compared to uniform allocation, (*iii*) *Floor plan knowledge:* Using angular profiles and room geometry, achieves zero leakage up to $R_s \leq 0.364$ [Bits/s/Hz] for $L = 7$, outperforming uniform allocation by ∼71.4%. Optimizes time allocation based on intersection points, and (*iv*) *Angular profile knowledge:* Provides $R_s \leq 0.091$ [Bits/s/Hz] for $L = 7$ beams. Performance is expected to improve with more antennas.

Partial RF map shows the strongest performance. Floor plan knowledge reduces performance by ∼7.69%, while angular profile knowledge alone decreases performance by ∼76.9% compared to partial RF map for $L = 7$.

*2) Absolute Secrecy Rate:* Fig. 8 shows the absolute secrecy rate as a heatmap across the evaluation area for all considered schemes. The values are obtained by interpolating secrecy rate measurements at discrete Eve locations, corresponding to the layout shown in Fig. 7. This spatial representation provides insight into how secrecy performance varies throughout the environment. Darker blue regions indicate areas of low secrecy, approaching zero, typically where the Eve receives strong signal power. Brighter regions represent higher secrecy performance resulting from secure beam and time allocation strategies. As illustrated, the legacy scheme exhibits zero secrecy rate along the LoS path, shown by a prominent dark blue line between the transmitter and receiver. This occurs because all transmission power is concentrated on a single beam, which an Eve can easily align with. In such a case, the Eve's channel may be stronger than the legitimate receiver's, resulting in a secrecy rate of zero. We assume that the Eve has sufficient capability to decode all intercepted messages. In contrast, BeamSec adopts multiple secure beam allocation strategies, achieving significantly higher absolute secrecy rates under different levels of channel knowledge: (*i*) *Uniform time allocation:* BeamSec pre-selects a set of candidate beams and distributes transmission time uniformly. Despite not using environment-specific information, it achieves an absolute secrecy rate of 0.269 [bits/s/Hz] by avoiding concentration of signal energy on a single path, (*ii*) *Partial RF map knowledge:* This scheme leverages historical channel measurements to estimate spatial vulnerabilities. By intelligently allocating more time to beams with lower interception risk, it achieves an absolute secrecy rate of 0.6043 [bits/s/Hz], even without real-time knowledge of the Eve's location, (*iii*) *Floor plan knowledge:* This approach incorporates knowledge of room geometry to identify intersecting beams–locations where multiple beams overlap and may increase interception risk. Using this information, the scheme selectively minimizes transmission time over vulnerable beams and yields an absolute secrecy rate of 0.425 [bits/s/Hz], and (*iv*) *Only angular profile knowledge:* By analyzing angular characteristics (i.e., AoD and AoA), this scheme identifies likely interception directions and reduces exposure by favoring safer beam directions. Although conservative, it maintains a non-zero secrecy rate of 0.202 [bits/s/Hz]. Overall, the performance ranking of these schemes reflects their ability to adapt time allocation based on available spatial information. The floor plan and RF map-based approaches outperform others due to their ability to identify and avoid high-risk regions, thereby enhancing secrecy against passive eavesdroppers.

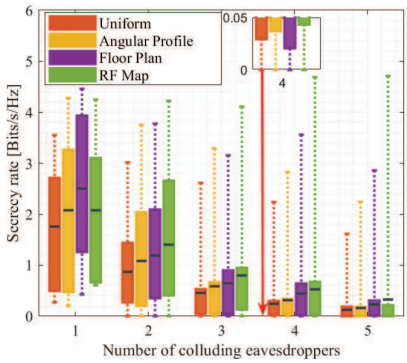



Fig. 10. Absolute secrecy rate versus number of colluding eavesdroppers for L = 7.

## B. Colluding Eavesdroppers

Next, we investigate the robustness of BeamSec in the presence of multiple colluding eavesdroppers. We have conducted an analysis of the worst channel realizations concerning secrecy rates across all possible combinations of colluding eavesdroppers, as depicted in Fig. 10. Here we show the average, 25-th, and 75-th percentile, minimum and maximum, where minimum values correspond to the absolute secrecy rate. This analysis provided valuable insights into how an increasing number of colluding eavesdroppers influences the secrecy rate. Notably, as the number of colluding eavesdroppers rises, both the absolute and average secrecy rates experience a decline. To offer a comprehensive perspective, Fig. 10 also incorporates the scenario of a single Eve, representing a non-colluding context. The box plot depicts the mean alongside the 25-th and 75-th percentiles, showcasing

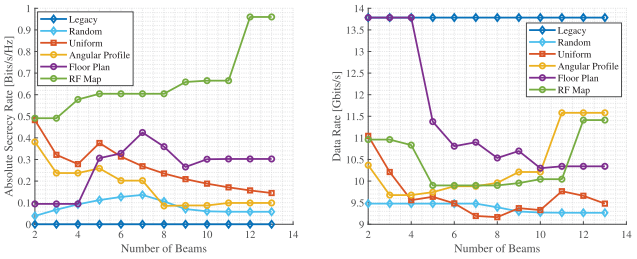
the variability in absolute secrecy rates across different Eve configurations. Despite the challenges posed, our proposed methodologies consistently uphold a non-zero absolute secrecy rate for the majority of the Eve configurations, demonstrating resilience against escalating Eve numbers. Both the RF map and floor plan exhibit robustness against colluding eavesdroppers until the presence of four colluding eavesdroppers, respectively, where less than 25% of Eve configurations exhibit an absolute secrecy rate as low as 0.043 and 0.027 [Bits/s/Hz], respectively. The uniform and angular profile schemes also show resilience up to four colluding eavesdroppers. On average (mean of all absolute secrecy rates of all configurations), the absolute secrecy rate for uniform time allocation experiences a 50.6% drop as the number of colluding eavesdroppers increases to two. This rate further declines to 0.124 [Bits/s/Hz] for five colluding eavesdroppers, marking a 92.9% decrease. The uniform scheme's lack of adaptability to the channel knowledge of the environment may result in vulnerabilities in data transmission. The angular profile scheme demonstrates slightly superior performance compared to the uniform scheme, with a 47.7% drop in absolute secrecy rate as the number of colluding eavesdroppers increases to two. This rate approaches 0.164 [Bits/s/Hz] for five colluding eavesdroppers, representing a 92.1% decrease. However, the angular profile's optimization process does not adequately consider the spatial layout of the environment or the potential clustering of eavesdroppers, leading to sub-optimal performance in scenarios involving coordinated Eve attacks.

### C. Absolute Secrecy Rate Vs Number of Beams

We examine how the number of beams affects the absolute secrecy rate, especially with a single Eve. Unlike legacy systems with potential zero leakage, BeamSec maintains a non-zero secrecy rate across all time-allocation strategies. Increasing beams enhances channel diversity but also expands the attack surface, creating a trade-off. Random beam selection [24], although better than legacy, may lead to limited diversity and minimal angular separation, increasing eavesdropping risks. Uniform time allocation, benefiting from BeamSec's diverse beams, enhances the secrecy rate by 236% ($L = 5$) without time allocation optimization. Optimized time allocation further improves secrecy by 58% and 125% with floor plan and RF map knowledge, respectively. Secrecy rate improvements depend on effective time allocation. With RF map knowledge, the secrecy rate consistently rises with more beams. However, schemes with instantaneous channel knowledge, like angular profiles and floor plans, may see fluctuations. For example, angular profiles may decrease secrecy with more beams due to reduced angular separation. Floor plan schemes initially benefit from beam diversity but may face interference and inefficiencies beyond optimal beam count.

### D. Trade-off Between Data Rate and Secrecy

Balancing data rate and secrecy is crucial in modern communication systems. Fig. 11a and Fig. 11b illustrate this trade-off for time-allocation methods. The Legacy method




(a) Absolute secrecy rate. (b) Data rate.

Fig. 11. Comparison of absolute secrecy rate and data rate versus numbers of beams.

offers the highest data rate but lacks secrecy and is unsuitable for security-sensitive applications. In contrast, uniform, angular profile, floor plan, and RF map methods provide different trade-offs. Uniform reduces data rate by 42.86% but modestly increases secrecy. Angular profile balances with a 32.14% data rate decrease and moderate secrecy increase. The floor plan offers a smaller data rate reduction (28.57%) with higher secrecy, ideal for stable performance. RF map achieves minimal data rate decrease (25%) with the highest secrecy increase, optimal for high-security applications. Each method allows tailored solutions based on specific application needs.

## VII. Conclusion

In conclusion, this paper presents BeamSec, a practical physical layer security framework for mmWave systems. By adapting to varying levels of channel knowledge, BeamSec enables secure communication ranging from uniform to RX- or RF map-based time allocation. Leveraging key wireless features such as AoD, AoA, and SNR, it dynamically adjusts beam selection and allocation strategies based on the RX's channel state. Experimental results using an 802.11ad/ay-compatible 60 GHz phased-array testbed demonstrate strong performance, achieving a 58.13% improvement with instantaneous RX knowledge and 124.86% with partial RF map knowledge, compared to naive uniform allocation.

This framework can be extended to mobile users by periodically updating beam configurations and CSI, allowing dynamic adaptation to mobility-induced channel changes while minimizing overhead. RL also presents a promising direction to optimize beam selection and time allocation [21], especially in dynamic environments where CKM evolves over time. Future work will investigate BeamSec's resilience to proactive eavesdroppers [39] and explore countermeasures using advanced machine learning techniques.

## References

[1] A. Ishtiaq, A. Asadi, L. Khaloopour, W. Ahmed, V. Jamali, and M. Hollick, "BeamSec: A practical mmWave physical layer security scheme against strong adversaries," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2023, pp. 1–9, doi: 10.1109/CNS59707.2023.10289003.

[2] G. Li, C. Sun, J. Zhang, E. Jorswieck, B. Xiao, and A. Hu, "Physical layer key generation in 5G and beyond wireless communications: Challenges and opportunities," *Entropy*, vol. 21, no. 5, p. 497, May 2019.

[3] G. Li, H. Yang, J. Zhang, H. Liu, and A. Hu, "Fast and secure key generation with channel obfuscation in slowly varying environments," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, May 2022, pp. 1–10.

[4] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sep. 2009.

[5] N. Valliappan, A. Lozano, and R. W. Heath Jr., "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, Aug. 2013.

[6] N. N. Alotaibi and K. A. Hamdi, "Switched phased-array transmission architecture for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1303–1312, Mar. 2016.

[7] (2024). *SatStar*. [Online]. Available: https://www.satstar.net/faq.html

[8] X. Lu, S. Venkatesh, B. Tang, and K. Sengupta, "Physical layer security through directional modulation with spatio-temporal millimeter-wave transmitter arrays," *IEEE J. Solid-State Circuits*, vol. 59, no. 9, pp. 2831–2847, Sep. 2024.

[9] J. Si, Z. Cheng, Z. Li, J. Cheng, H.-M. Wang, and N. Al-Dhahir, "Cooperative jamming for secure transmission with both active and passive eavesdroppers," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5764–5777, Sep. 2020.

[10] Y. Hong, X. Jing, H. Gao, and Y. He, "Fixed region beamforming using frequency diverse subarray for secure mmWave wireless communications," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2706–2721, 2020.

[11] D. Steinmetzer et al., "Eavesdropping with periscopes: Experimental security analysis of highly directional mmWaves," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Florence, Italy, 2015, pp. 335–343.

[12] H. Wang et al., "Resisting malicious eavesdropping: Physical layer security of mmWave MIMO communications in presence of random blockage," *IEEE Internet Things J.*, vol. 9, no. 17, pp. 16372–16385, Sep. 2022.

[13] Y. Ju, Y. Zhu, H.-M. Wang, Q. Pei, and H. Zheng, "Artificial noise hopping: A practical secure transmission technique with experimental analysis for millimeter wave systems," *IEEE Syst. J.*, vol. 14, no. 4, pp. 5121–5132, Dec. 2020.

[14] 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 Trans. Inf. Forensics Security*, vol. 13, no. 3, pp. 671–684, Mar. 2018.

[15] Y. Hong, X. Jing, Y. He, and J. Mu, "Dynamic rotated angular beamforming using frequency diverse phased-array for secure mmWave wireless communications," *Electronics*, vol. 9, no. 1, p. 10, Dec. 2019.

[16] J. Lin, Q. Li, and J. Yang, "Frequency diverse array beamforming for physical-layer security with directionally-aligned legitimate user and eavesdropper," in *Proc. 25th Eur. Signal Process. Conf. (EUSIPCO)*, Aug. 2017, pp. 2166–2170.

[17] Y. R. Ramadan and H. Minn, "Artificial noise aided hybrid precoding design for secure mmWave MISO systems with partial channel knowledge," *IEEE Signal Process. Lett.*, vol. 24, no. 11, pp. 1729–1733, Nov. 2017.

[18] M. E. Eltayeb and R. W. Heath Jr., "Securing mmWave vehicular communication links with multiple transmit antennas," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2018, pp. 1–6.

[19] T. Hong, M.-Z. Song, and Y. Liu, "Dual-beam directional modulation technique for physical-layer secure communication," *IEEE Antennas Wireless Propag. Lett.*, vol. 10, pp. 1417–1420, 2011.

[20] B. Qiu et al., "Artificial-noise-aided secure transmission for proximal legitimate user and eavesdropper based on frequency diverse arrays," *IEEE Access*, vol. 6, pp. 52531–52543, 2018.

[21] X. Lu et al., "Reinforcement learning-based physical cross-layer security and privacy in 6G," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 425–466, 1st Quart., 2023.

[22] Y. Ju, H.-M. Wang, T.-X. Zheng, Q. Yin, and M. H. Lee, "Safeguarding millimeter wave communications against randomly located eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2675–2689, Apr. 2018.

[23] V. Petrov, D. Moltchanov, J. M. Jornet, and Y. Koucheryavy, "Exploiting multipath terahertz communications for physical layer security in beyond 5G networks," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2019, pp. 865–872.

[24] R. Talwar, N. Amala, G. Medina, A. S. Jida, and M. E. Eltayeb, "Exploiting multi-path for safeguarding mmWave communications against randomly located eavesdroppers," 2020, *arXiv:2010.00733*.

[25] C.-Y. Yeh, A. Cohen, R. G. L. D'Oliveira, M. Médard, D. M. Mittleman, and E. W. Knightly, "Angularly dispersive terahertz links with secure coding: From theoretical foundations to experiments," in *Proc. 15th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, May 2022, pp. 268–273.

[26] T. S. Rappaport, E. Ben-Dor, J. N. Murdock, and Y. Qiao, "38 GHz and 60 GHz angle-dependent propagation for cellular & peer-to-peer wireless communications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 4568–4573.

[27] S. Sur, X. Zhang, P. Ramanathan, and R. Chandra, "BeamSpy: Enabling robust 60 GHz links under blockage," in *Proc. USENIX NSDI*, 2016, pp. 193–206.

[28] R. F. Schaefer, H. Boche, and H. V. Poor, "Secure communication under channel uncertainty and adversarial attacks," *Proc. IEEE*, vol. 103, no. 10, pp. 1796–1813, Oct. 2015.

[29] Y. Zeng et al., "A tutorial on environment-aware communications via channel knowledge map for 6G," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 3, pp. 1478–1519, 3rd Quart., 2024.

[30] Z. Xing and J. Chen, "Constructing indoor region-based radio map without location labels," *IEEE Trans. Signal Process.*, vol. 72, pp. 2512–2526, 2024.

[31] X. Xu and Y. Zeng, "How much data is needed for channel knowledge map construction?," *IEEE Trans. Wireless Commun.*, vol. 23, no. 10, pp. 13011–13021, Oct. 2024.

[32] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 1, pp. 19–26, 2016.

[33] V.-P. Chowdappa, C. Botella, J. J. Samper-Zapater, and R. J. Martinez, "Distributed radio map reconstruction for 5G automotive," *IEEE Intell. Transp. Syst. Mag.*, vol. 10, no. 2, pp. 36–49, May 2018.

[34] C. B. Barneto, T. Riihonen, M. Turunen, M. Koivisto, J. Talvitie, and M. Valkama, "Radio-based sensing and indoor mapping with millimeter-wave 5G NR signals," in *Proc. Int. Conf. Localization GNSS (ICL-GNSS)*, Jun. 2020, pp. 1–5.

[35] The MathWorks, Inc. (2022). *Optimization Toolbox Version: 9.4 (R2022b)*. [Online]. Available: https://www.mathworks.com

[36] A. S. Glassner, *An Introduction to Ray Tracing*. San Mateo, CA, USA: Morgan Kaufmann, 1989.

[37] J. O. Lacruz, D. Garcia, P. J. Mateo, J. Palacios, and J. Widmer, "Mm-FLEX: An open platform for millimeter-wave mobile full-bandwidth experimentation," in *Proc. ACM MobiSys*, Jun. 2020, pp. 1–13.

[38] Sivers. (2024). *Evaluation Kit Evk06002*. [Online]. Available: https://shorturl.at/NZ8g5

[39] J. Chen, L. Tang, D. Guo, Y. Bai, L. Yang, and Y.-C. Liang, "Proactive eavesdropping in massive MIMO-OFDM systems via deep reinforcement learning," *IEEE Trans. Veh. Technol.*, vol. 71, no. 11, pp. 12315–12320, Nov. 2022.