SPP: Achieving Low-Probability-of-Intercept Cellular and Wi-Fi Communications via MIMO-based Spatial Pilot Perturbation

Peihao Yan, Milad Afshari, and Huacheng Zeng

***Abstract*—Low Probability of Intercept (LPI) wireless communication is a critical aspect of modern wireless technology. Despite various techniques developed for LPI wireless communication, most of them require some form of pre-existing knowledge (e.g., encryption keys) or specific information (e.g., eavesdropper location and channel details). In this paper, we propose a novel physical-layer precoding technique called spatial pilot perturbation (SPP) to achieve efficient LPI wireless communications. Unlike existing methods, SPP operates without the need for pre-shared information between the two communication devices, nor any knowledge about potential eavesdroppers. It remains transparent to users and thus backward-compatible with off-the-shelf 5G/WiFi user devices. The core idea of SPP is to use different precoders for pilot and data symbols in a signal frame at the physical layer. Through a systematic precoder design, the pilot and data symbols will experience identical compound channels upon arrival at intended receivers, but experience different compound channels when intercepted by eavesdroppers. Consequently, the intended receivers can demodulate the signal frame, while eavesdroppers cannot. We have implemented SPP on 5G and WiFi testbeds and evaluated its performance through over-the-air experiments. Extensive experimental results show that SPP achieves an eavesdropping rate of $\leq$0.2% for 5G and $\leq$0.9% for WiFi, both at the cost of less than 18% throughput.**

***Index Terms*—Low probability of intercept (LPI), wireless communications, physical-layer security, precoding, 5/6G, Wi-Fi**

I. Introduction

While the over-the-air broadcast nature of radio waves enables our society to enjoy mobile wireless Internet services, it also poses a threat to data privacy—data packets sent by a transmitter may be eavesdropped by an unintended receiver. To safeguard sensitive information against over-the-air interception, key-based data encryption is arguably the most powerful LPI approach. It has been widely used in real-life wireless communication systems like 4/5G and WiFi. But this approach requires either a secure key distribution infrastructure or a computation-intensive key exchange mechanism (e.g., Diffie–Hellman key exchange [1]), making it unsuitable for some applications such as low-power low-cost 6G IoT communications, 6G device-to-device, vehicle-to-vehicle communications, and military ad hoc communications in harsh battlefields.

To complement and strengthen key-encryption-based LPI solutions, a variety of physical-layer LPI techniques have been proposed, such as spectrum spreading, frequency hopping, artificial noise injection [2]–[5], preamble randomization [6], beamforming [7]–[26], beam nullification [8], [23], [24], spatial-time-modulation [27]–[29], and channel-based key generation [30], [31]. However, most existing physical-layer LPI communication techniques require pre-shared knowledge between the transmitter and receiver, instantaneous information about potential eavesdroppers, or rely upon other impractical assumptions. For instance, spectrum spreading and frequency hopping, albeit relatively easy to implement, suffer from inefficient spectrum utilization. Artificial noise injection requires the prior sharing of noise characteristics between the transmitter and receiver. Beam nullification depends on knowledge of the eavesdropper's channel or angular location, which is difficult to acquire in practice. More importantly, when deployed in real-world wireless communication systems, most of these techniques are incompatible with incumbent cellular and WiFi client devices. Consequently, physical-layer LPI techniques have not seen widespread adoption in real-world wireless communication networks.

To complement and strengthen the key-encryption-based LPI solution, physical-layer LPI techniques have been proposed in an increasingly sophisticated form, such as spectrum spreading, frequency hopping, artificial noise injection [2]–[5], preamble randomization [6], beamforming [7]–[26], beam nullification [8], [23], [24], misinformation [32], and channel-based key generation [30], [31]. However, existing physical-layer LPI techniques need pre-shared knowledge between transmitter and receiver, demand instantaneous information of potential eavesdroppers, or other demanding requirements. For instance, although spectrum spreading and frequency hopping are easy to deploy, they appear to be inefficient in spectrum utilization. Artificial noise injection needs to share the prior knowledge of noise between transmitter and receiver. Beam nullification relies on the knowledge of the channel between the transmitter and eavesdropper or their angular direction of the eavesdropper, which is to obtain in practice. More importantly, most of existing techniques, when applied to real-world wireless communication systems, are not compatible with billions of cellular and WiFi client devices that are already in use. As such, physical-layer LPI techniques have never been widely adopted by real-life wireless networks.

In this paper, we present a physical-layer MIMO-based (multi-input and multi-output based) precoding technique, called spatial pilot perturbation (SPP), to enable efficient LPI 5G and WiFi communications. Consider the downlink communication from a 5G base station (BS) to one or multiple

P. Yan, M. Afshari, and H. Zeng are with the Department of Computer Science and Engineering at Michigan State University, East Lansing, MI 48824. Corresponding author: H. Zeng (hzeng@msu.edu).

This work was supported in part by NSF Grant CNS-2312448.

users in the face of radio eavesdroppers. The BS is equipped with multiple antennas, while user and eavesdropper are equipped with one or multiple antennas. In such a network, SPP is designed based on two observations: **First**, radio signals in wireless communication systems are organized in a *frame* format. In general, each frame comprises two types of symbols: *pilot symbols* and *data symbols*. Pilot symbols are also referred to as reference signals (e.g., DMRS in 4/5G) and preamble (e.g., in WiFi). Pilot symbols are used for intended receivers to estimate channels while data symbols are used to carry payloads from the upper layer. **Second**, a receiver, either intended or unintended, relies on the pilot symbols in a frame for channel estimation, which plays a critical role in demodulating the data symbols in a frame. *A receiver can successfully demodulate the data symbols in a frame only if its pilot and data symbols experience identical (or very similar) compound channels when arriving at the receiver.* This is a foundation for the design of broadband wireless communication systems such as cellular and WiFi.

SPP leverages the above two observations to prevent eavesdroppers from demodulating the data symbols in a frame. The key idea behind SPP is to use different precoders for the pilot and data symbols in each frame. Through a systematic design of precoders, *the pilot and data symbols in a frame will experience identical compound channel when arriving at the intended users, but experience different compound channels when arriving at any unintended users (eavesdroppers).* As a result, the intended users are capable of demodulating the data symbols in the frame, while unintended users are not. The key question to ask is how to design different precoders for the pilot and data symbols in a frame so that they will experience the desired channels. To address this question, we formulate the precoder design problem as an optimization problem and introduce two important concepts to solve this optimization problem: *transmission vector* and *perturbation vector*. It turns out that these two concepts can significantly facilitate the design and analysis of the precoders. The *transmission vector* can be designed as if the network has no eavesdroppers; and the *perturbation vector* can be selected directly from the user channel's nullspace. Using the linear combination of transmission and perturbation vectors as the precoder, the pilot and data symbols will experience identical compound channel upon arriving at intended users, but they will encounter different compound channels when arriving at unintended users. Additionally, the precoding operation does not require any knowledge about eavesdroppers and remain transparent to intended users.

We have implemented SPP on 5G and WiFi software-defined radio (SDR) testbeds. We have conducted *real-time*, *over-the-air* experiments on both testbeds, and evaluated the performance (eavesdropping rate) and cost (throughput degradation) of SPP in a realistic environment when the BS/AP has two, three, and four antennas. Table I summarizes our experimental results when the BS/AP has no knowledge about eavesdroppers. In 5G, SPP achieves $\leq$0.2% eavesdropping rate at the cost of $\leq$17% throughput degradation. In WiFi, SPP demonstrates $\leq$0.9% eavesdropping rate at the cost of $\leq$18% throughput degradation.

TABLE I: A summary of SPP's average eavesdropping rate and throughput cost.

	5G			WiFi		
	BS has 2 antennas	BS has 3 antennas	BS has 4 antennas	AP has 2 antennas	AP has 3 antennas	AP has 4 antennas
Eavesdropping rate	3.1e-4	9.3e-4	2.1e-3	2.3e-3	6.2e-3	9.4e-3
Throughput cost	12%	17%	13%	10%	18%	14%

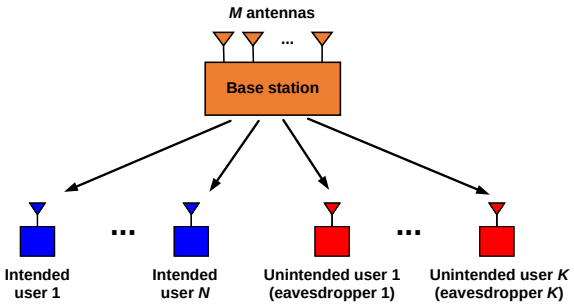


Fig. 1: System model.

Table II presents a comparison between SPP and existing LPI approaches, positioning it within the context of the literature. The contributions of this paper are summarized as follows.

- SPP is a novel physical-layer technique for LPI wireless communications. It does not need any knowledge about eavesdroppers. Its operations reside only in BS/AP and remain fully transparent to users. It is backward compatible with off-the-shelf cellular and WiFi client devices when applied in 5G/WiFi downlink.
- Efficient precoders have been designed for SPP. The precoders ensure that the pilot and data symbols in a frame experience identical channels upon arriving at users, but encounter different channels when intercepted by eavesdroppers.
- We have conducted extensive *real-time*, *over-the-air* experiments on 5G and WiFi testbeds to evaluate the performance of SPP. Experimental results confirm the high effectiveness and efficiency of SPP.

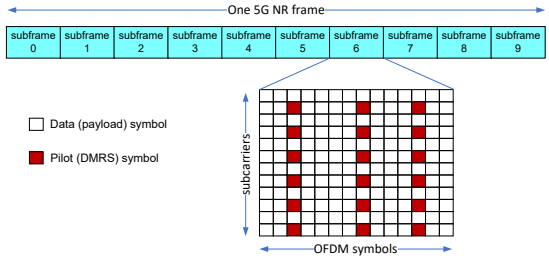
II. Problem Description

We consider a white-box eavesdropping attack in broadband wireless communication systems such as 4/5G and WiFi. Figure 1 shows an example of such an attack in 5G cellular networks. We assume that the BS is equipped with multiple antennas, while the user device is equipped with one or multiple antennas. In the proximity of the BS, there are one or more unintended users acting as eavesdroppers aimed at decoding the data packets from the BS. Each eavesdropper is equipped with one or multiple antennas. All eavesdroppers are capable of sharing information with each other and performing joint operations in their attempts to decode the data packets from the BS.

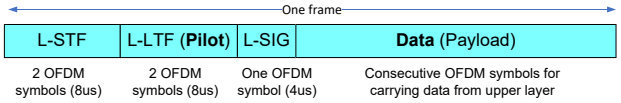
Our objective is to minimize the eavesdropping rate for the data packets from the BS to the user devices by leveraging MIMO-based precoding techniques at the physical layer. To the end, we consider two eavesdropping cases: *out-of-network eavesdropping* and *in-network eavesdropping*. In the former

TABLE II: Comparison of SPP and the representative LPI approaches in the literature.

LPI approaches	Need pre-shared knowledge?	Need knowledge of eavesdropper?	Digital or analog?	Work for OFDM?	Single eaves-dropper?	Spectral efficiency	Computation complexity	Compatible with commercial user devices?
Spectrum spreading and frequency hopping	Yes	No	Digital	No	No	Low	Medium	No
Key-based data encryption	Yes	No	Digital	Yes	No	High	High	No
Diffie–Hellman key exchange [1]	No	No	Digital	Yes	No	High	High	No
Artificial noise injection [2]–[5]	Yes	No	Digital	Yes	No	Low	High	No
Preamble randomization [6]	Yes	No	Digital	Yes	No	High	Medium	No
MU-MIMO beamforming DgDi [7]–[26]	No	Yes (channel)	Digital	Yes	Yes	Medium	Medium	Yes
Beam nullification [8], [23], [24]	No	Yes (direction)	Either	Yes	Yes	Medium	Low	Yes
Spatial-time-modulation [27]–[29],	No	No	Analog	No	Yes	Medium	Low	No
Channel-based key generation [30], [31]	No	No	Digital	Yes	No	High	High	No
SPP (This work)	**No**	**No**	**Digital**	**Yes**	**No**	**Medium**	**Low**	**Yes**



(a) 5G NR frame structure.



(b) Legacy WiFi 802.11 frame structure.

Fig. 2: Pilot and data symbols in 5G and WiFi frames.

case, the BS has no channel/location knowledge about the eavesdroppers. In the latter case, the BS has some channel knowledge of the eavesdroppers and thus can better optimize its precoding design. Successful design will add a new layer of protection to the ubiquitous wireless communications. Particularly, for the case where key-based data encryption is not an option due to hardware, software and energy constraints, physical-layer LPI techniques are of paramount importance to safeguard communication privacy [33].

III. Background

A. Pilots in Signal Frame

When radio signal travels from a transmitter to a receiver, it experiences power attenuation, phase rotation, and multipath distortion. At the receiver, channel estimation and equalization play a crucial role in its signal detection pipeline. To enable signal detection at a receiver, both cellular and WiFi systems embed **pilot symbols** (a.k.a., preamble and reference signal) in their individual frames. The pilot symbols allow a receiver to estimate the compound channel[1] that a signal frame experiences, which is then used to recover **data symbols** in the frame.

Figure 2(a) shows the 5G New Radio (NR) frame structure. A frame has 10 subframes, each of which consists of two-dimensional resource elements in an array of OFDM symbols. Here, the pilots are demodulation reference signal (DMRS) as shown in the figure. They are distributed over different OFDM symbols and used by a receiver to estimate the compound channel for signal detection. Figure 2(b) shows the legacy 802.11 frame structure, which includes legacy short training field (L-STF), legacy long training field (L-LTF), signal (SIG), and payload data. Here, the pilot refers to the preamble (L-STF and L-LTF). While both cellular and WiFi frame structures are evolving, all OFDM frames are designed following the same principle—embedding pilot symbols in a frame for receivers to estimate channel and decode data symbols.

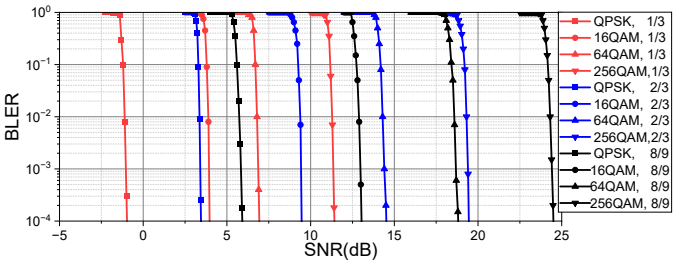
A foundation of cellular and WiFi systems is that the pilot and data symbols in the same frame (equivalently subframe or time slot in 5G NR) experience identical compound channels. To ground this foundation, the system parameters of 5G and WiFi are meticulously selected, including the frame length, the pilot density, and the user's maximum moving speed.

[1]In this paper, compound channel refers to the end-to-end channel effect including transmitter-side precoder, response of radio frequency circuits, and over-the-air channel.

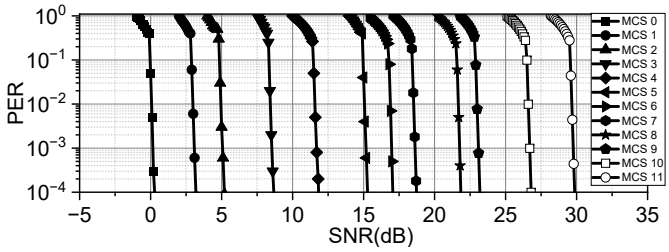
B. Understand PER, MCS and EVM

When a cellular or WiFi device receives a data packet, the probability of it successfully decoding this data packet is determined by two factors: i) *modulation and coding scheme (MCS)*, and ii) *error vector magnitude (EVM)*. Specifically, the packet error rate (PER) of a receiver can be written as a deterministic function of MCS and EVM: $\mathrm{PER} = f(\mathrm{MCS}, \mathrm{EVM})$. MCS is a mechanism of rate adaptation. The transmitter first probes the quality of the channel between itself and the receiver, and then selects the "best" MCS index for data transmission based on the channel quality. Here, "best" is in the sense of maximizing data rate while ensuring the PER at the receiver is below a pre-defined threshold (e.g., 0.1%). EVM is a system-level performance metric defined in many communication standards. It characterizes the average distance between the ideal and estimated QAM constellations at a receiver. Per IEEE 802.11 standards [34], $\mathrm{EVM} = \sqrt{\frac{\sum_{l=1}^{L_p}\sum_{k=1}^{N_c}|\hat{x}_{lk}-x_{lk}|^2}{L_p N_c P}}$, where L_p is the number of frames or transport blocks, N_c is the number of carriers, $\hat{x}_{ij}$ and x_{ij} are received and ideal constellation points, and P is the signal power. In additive white Gaussian noise (AWGN) channels, it is equivalent to the inverse of SNR.

Figure 3(a) shows 5G's curves of block error rate (BLER, equivalent to PER) versus SNR for different MCS indices. Figure 3(b) shows 802.11's curves of PER versus SNR for a set of MCS indices. It can be seen that the PER-SNR curves



(a) 5G BLER versus SNR [35].



(b) WiFi PER versus SNR [36].

Fig. 3: PER versus SNR in 5G and WiFi systems. Here, SNR (dB) = $(-1)\times$ EVM (dB).

are extremely steep, thanks to the power of LDPC code used by 5G and WiFi. In particular, ***a 3 dB decrease of SNR (equivalently, 3 dB increase of EVM) is more than enough to increase PER from 0.1% to 100%.*** This observation also applies to other coding schemes such as polar code [35]. It reveals that, to prevent an eavesdropper from decoding a data packet, we only need to make sure the EVM at the eavesdropper is 3 dB greater than that at the intended receiver. By doing so, through appropriate MCS selection and/or power control at the transmitter, the intended receiver will be able to decode the data packet while the eavesdropper will not. This observation motivates the design of SPP.

IV. SPP for LPI Communications

A. Basic Idea

SPP is a precoding technique for a transmitter equipped with two or more antennas. It aims to increase the EVM at unintended receiver(s) and decrease EVM at intended receiver(s), so that the data packets can be decoded by intended receiver(s) but cannot be decoded by unintended receivers. To attain this aim, it takes advantage of the spatial degrees of freedom (DoF) provided by the transmitter's multiple antennas and uses two different weight vectors to precode the pilot and data symbols in the same frame (alternatively: subframe, time slot, or resource block). Through a systematic design of the precoders, the pilot and data symbols in a frame will experience identical compound channels when traveling from the transmitter to the intended receiver(s), but experience different channels when traveling from the transmitter to the unintended receiver(s). As such, the intended users can demodulate the signal frame while the unintended users (eavesdroppers) cannot.

Figure 4 illustrates the basic idea of SPP in a small network. The transmitter uses different precoders to map the pilot and data symbols onto its two antennas. As a result, the pilot and data signals from each of its antennas have different amplitudes and initial phases. Both pilot and data signals go through the over-the-air channels. When impinging on the intended device, the pilot and data signals turn out to have identical amplitude and identical initial phase. Hence, this receiver can demodulate the data symbols. In contrast, when impinging on each of the unintended devices, the pilot and data signals are of different amplitudes and different initial phases. This means that the pilot and data symbols experience different compound channels when traveling from the transmitter to the unintended device. Consequently, the unintended device is incapable of decoding data symbols in the frame. The physical law behind it is that different users have different over-the-air channels almost surely.

B. SPP Problem Formulation

The key question is how to design the precoding vectors at the BS so that the signal distortion at unintended users can be maximized. Assume that the BS has M antennas and each user has one antenna. There are one intended user and K eavesdropping users. Denote the channel from the BS to the intended device as $\vec{h} \in \mathbb{C}^{M\times 1}$. Denote the channel from the BS to the kth unintended device as $\vec{g}_k \in \mathbb{C}^{M\times 1}$. Denote $\vec{a}$ as the precoding vector for the pilot symbols in a frame and $\vec{b}$ as the precoding vector for the data symbols in the frame. Let us focus on the received signal at the unintended device and assume that all users are working in a high-SNR regime. At the intended device, it will take two steps to demodulate the signal: (i) It first estimates the compound channel using pilot symbols; the estimated channel will be $\vec{h}^\top\vec{a}$. (ii) It uses the estimated channel to equalize the channel for signal demodulation. The estimated signal can be written as $\hat{x} = \frac{\vec{h}^\top\vec{b}}{\vec{h}^\top\vec{a}}x$, where x is the original signal from the BS with a normalized transmission power (i.e., $\mathbb{E}[|x|^2] = 1$). Then, the EVM at user and eavesdropper can be written as:

$$\text{EVM}_{usr} = \frac{\mathbb{E}[|\hat{x}-x|^2]}{\mathbb{E}[|x|^2]} = \left|\frac{\vec{h}^\top(\vec{a}-\vec{b})}{\vec{h}^\top\vec{a}}\right|^2, \tag{1a}$$

$$\text{EVM}_{eav} = \frac{\mathbb{E}[|\hat{x}-x|^2]}{\mathbb{E}[|x|^2]} = \left|\frac{\vec{g}_k^\top(\vec{a}-\vec{b})}{\vec{g}_k^\top\vec{a}}\right|^2. \tag{1b}$$

Recall that the objective is to maximize the signal distortion at the unintended device (i.e., $\text{EVM}_{eav} \to +\infty$) while maintaining the channel consistency at the intended user device (i.e., $\text{EVM}_{usr} \to 0$). Then, this problem can be formulated as:

$$\max_{\vec{a},\vec{b}} \ \min_{1\le k\le K} \left|\frac{\vec{g}_k^\top(\vec{a}-\vec{b})}{\vec{g}_k^\top\vec{a}}\right|^2 \tag{2a}$$

$$\text{s.t.} \quad \vec{h}^\top\vec{a} = \vec{h}^\top\vec{b}; \tag{2b}$$

$$\vec{b}^{\mathsf{H}}\vec{b} \le P. \tag{2c}$$

where P is the transmit power of the BS. (2a) is to maximize the signal distortion among unintended users, (2b) is to ensure that the pilot and data symbols in a frame experience the identical compound channels when arriving at the intended user device (i.e., $\text{EVM}_{usr} = 0$), and (2c) is the power constraint at the BS. We note that a frame typically has much more data symbols than pilot symbols. Therefore, (2c) applies the power constraint to data symbols only. It can be easily

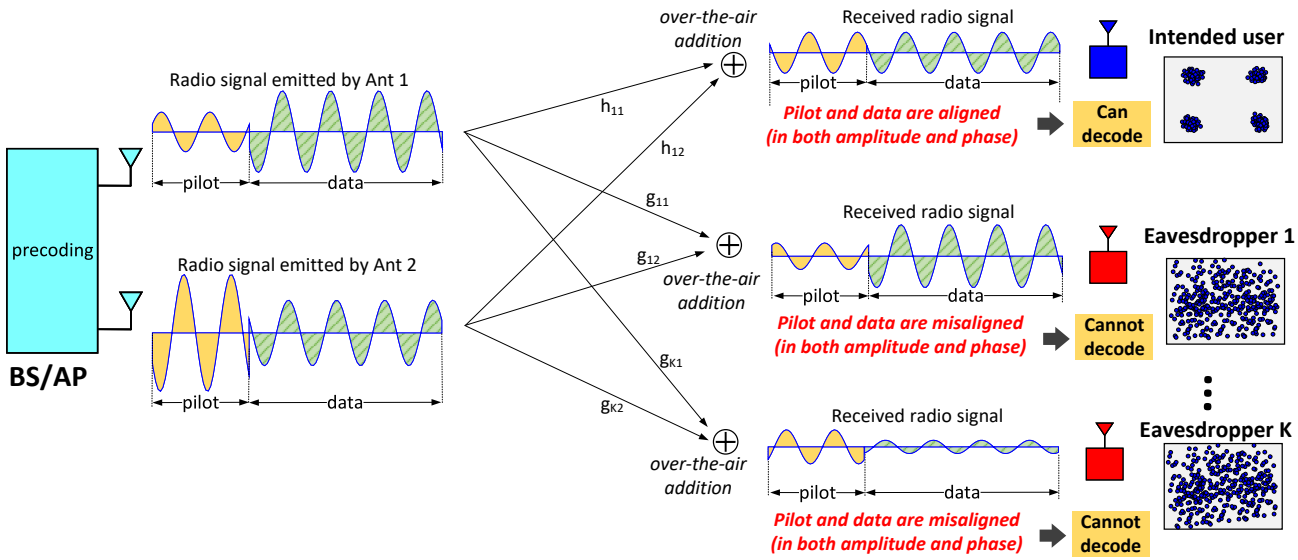


Fig. 4: Illustration of the core idea of SPP in an infrastructure-based wireless network.

extended to a total power constraint for both pilot and data symbols if needed.

In what follows, we design solutions to the optimization in (2) in two cases: *out-of-network eavesdropping* and *in-network eavesdropping*. In the former case, the BS has no channel knowledge about eavesdroppers; in the latter case, the BS has some channel knowledge about eavesdroppers.

V. SPP for Out-of-Network Eavesdroppers

In this section, we assume that *the BS has channel knowledge about the intended user(s) but does not have any knowledge about eavesdroppers*. This scheme does not need any hardware/software modifications on user devices, making SPP backward compatible with billions of off-the-shelf WiFi and 4/5G user devices that are already in use. In what follows, we first focus on the precoder design when the BS has one intended user and then extend the results to the case where the BS has multiple intended users for MU-MIMO transmission.

A. Single-User Transmission

To facilitate our discussion below, we introduce the singular vectors of the channel from the BS to the intended user:

$$[\vec{u}_1, \underbrace{\vec{u}_2, \ldots, \vec{u}_M}_{\text{nullspace}}] = \text{left\_singular\_vectors}(\vec{h}_1), \tag{3}$$

where $\vec{h}_1 \in \mathbb{C}^{M\times 1}$ is the intended user's channel. In Eqn (3), $[\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_M]$ are the singular vectors sorted in the non-increasing order of their corresponding singular values. To design the precoding vector for the SPP problem in Eqn (2), we introduce two concepts: *transmission vector* and *perturbation vector*. The transmission vector aims to minimize the EVM for the intended user(s), while the perturbation vector aims to maximize the EVM for unintended users. For this case, we construct the transmission and perturbation vectors as follows.

- **Transmission vector $\vec{p}$:** The BS employs the transmission vector for precoding to maximize the signal strength at the intended device. This is actually a well-known multi-input-single-output (MISO) transmission paradigm, and the optimal precoding scheme is a coherent precoder, i.e., $\vec{p} = \frac{\vec{h}_1^{\mathsf{H}}}{\|\vec{h}_1\|}$. It can be easily verified that $\vec{p} = \vec{u}_1$.
- **Perturbation vector $\vec{q}$:** In order to prevent the eavesdroppers from decoding the signal frame, a perturbation vector is needed for precoding the pilot and data symbols. Additionally, the perturbation vector should remain transparent to the intended user, i.e., $\vec{h}_1^{\top}\vec{q} = 0$. Therefore, the perturbation vector $\vec{q}$ must be orthogonal to $\vec{h}_1$. Given the properties of singular vectors in Eqn (3), the perturbation vector must lie in the subspace spanning over $\{\vec{u}_2, \ldots, \vec{u}_M\}$, i.e., $\vec{q} \in \langle \vec{u}_2, \ldots, \vec{u}_M \rangle$. A natural question to ask is, within this nullspace, which direction offers the best performance? To this question, since the BS has no knowledge about eavesdroppers, any unity vectors have the same performance of pilot perturbation. For notation simplicity, we let $\vec{q} = \vec{u}_M$.

Recall that $\vec{a}$ and $\vec{b}$ are precoding vectors for the pilot and data symbols in a frame, respectively. Based on the above transmission and perturbation vectors, we design the precoding vectors as follows:

$$\begin{cases} \vec{a} = \sqrt{P}(\sqrt{1-\eta}\vec{u}_1 + \sqrt{\eta}\vec{u}_M), \\ \vec{b} = \sqrt{P}(\sqrt{1-\eta}\vec{u}_1 - \sqrt{\eta}\vec{u}_M), \end{cases} \tag{4}$$

where P is the total transmission power at the BS, η is the portion of power allocated for pilot perturbation. Correspondingly, $1-\eta$ is the portion of power allocated for data transmission. η is a parameter for system operators to choose. Increasing η will enhance the protectivity of SPP against eavesdropping while decreasing η will increase the communication throughput. When $\eta = 0$, SPP is disabled and the system degrades to the conventional network communications.

For the two precoding vectors in Eqn (4), we have two remarks on SPP. **Remark 1: The pilot and data symbols in the same frame experience identical compound**

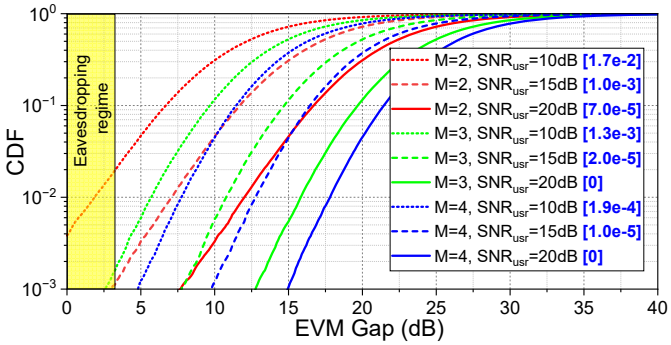
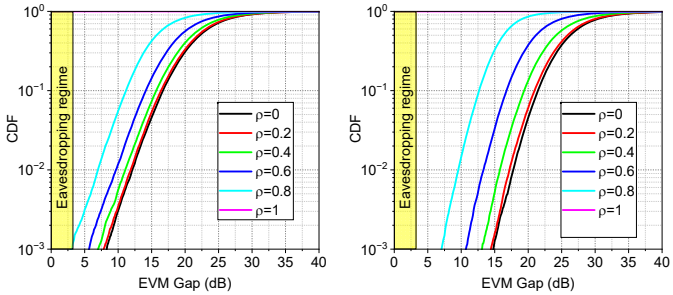


Fig. 5: EVM gap between user and eavesdropper in single-user transmission when $\mathrm{SNR}_{eav} = \mathrm{Inf}$. Blue numbers in the legend are the projected eavesdropping rate.



(a) BS has two antennas. (b) BS has four antennas.

Fig. 6: EVM gap between user's and eavesdropper's demodulated signals when the BS-to-user and BS-to-eavesdropper channels have different correlation values (ρ).

channels for intended receiver. Recall that the compound channel includes the precoder at transmitter and the over-the-air channel. The compound channel experienced by pilot is $\vec{h}_1^{\top}\vec{a}$, and the compound channel experienced by data is $\vec{h}_1^{\top}\vec{b}$. Since $\vec{u}_2, \vec{u}_2, \ldots, \vec{u}_M$ are within the nullspace of $\vec{h}_1$, we have $\vec{h}_1^{\top}\vec{a} = \vec{h}_1^{\top}\vec{b}$. Therefore, for the intended user, the pilot and data symbols experience the same compound channel. **Remark 2: The pilot and data symbols in a frame experience different compound channels for unintended receiver.** Given the randomness and independence of over-the-air wireless channels, it is almost sure that $\vec{g}_k^{\top}\vec{u}_m \neq 0$ for $1 \leq m \leq M$, where $\vec{g}_k$ is the over-the-air channel from the transmitter to the kth unintended user. Thus, we have $\vec{g}_k^{\top}\vec{a} \neq \vec{g}_k^{\top}\vec{b}$. This means that the pilot and data symbols in a frame experience different compound channels for an unintended user.

Numerical Analysis. To evaluate the precoders in Eqn (4), we consider the case where a BS serves one user in the face of one eavesdropper. We define $\mathrm{EVM\_Gap} = \mathrm{EVM}_{eav} - \mathrm{EVM}_{usr}$. The BS allocates 20% of its power for pilot perturbation (i.e., $\eta = 0.2$). The intended user and the eavesdropper have independent frequency-selective channels (with five-tap delays). We assume that the eavesdropper has $\mathrm{SNR}_{eav} = \mathrm{Inf}$. This means that the eavesdropper is very close to the BS and its signal distortion is solely from SPP. One million cases have been simulated. Figure 5 shows our numerical results. Per our discussion in §III-B, when $\mathrm{EVM\_Gap} \geq 3$, the eavesdropper is incapable of decoding data packets. Therefore, the probability of EVM gap less than 3 dB can be treated as the eavesdropping rate, which is shown in the figure legend. It can be seen that the eavesdropping rate is low for all cases. Even for the case where $\mathrm{SNR}_{usr} = 10$ dB and $\mathrm{SNR}_{eav} = \mathrm{Inf}$, the eavesdropping rate is less than 1.7%. Moreover, numerical results show that the eavesdropping rate decreases as BS antenna number increases or user SNR increases.

Impact of Channel Correlation. Consider the case where both the user and the eavesdropper have a single antenna. Denote ρ as the correlation coefficient between the BS-to-user and BS-to-eavesdropper channels, i.e., $\rho = \frac{|\vec{h}^{\mathsf{H}}\vec{g}|}{|\vec{h}||\vec{g}|}$. To study the impact of ρ on the performance of SPP, we conducted simulations using the above parameters, i.e., $\eta = 0.2$, $\mathrm{SNR}_{\mathrm{usr}} = 20$ dB, and $\mathrm{SNR}_{\mathrm{eav}} = \infty$. Figure 6 presents the simulation results under two settings: (i) the BS equipped with 2 antennas, and (ii) the BS has 4 antennas. In both settings, it is evident that the EVM_Gap decreases slightly as the channel correlation increases from 0 to 0.8. When $\rho = 1$, the EVM_Gap decreases to zero as expected. This demonstrates the resilience of SPP to channel correlation. This observation contrasts with our understanding of MU-MIMO, whose capacity is sensitive to channel correlation. The reason lies in the design goals: MU-MIMO aims to maximize the capacity of all users, whereas SPP seeks to maximize the capacity difference (i.e., EVM_Gap) between the legitimate user and the eavesdropper.

Impact of Eavesdropper's Antenna Number: If an eavesdropper is equipped with multiple antennas, it may use them to increase either channel gain or channel diversity. However, increasing channel gain does not help the eavesdropper's signal demodulation, as SPP relies on pilot perturbation—not SNR—for preventing unauthorized demodulation of data symbols. Increasing channel diversity can slightly improve the eavesdropper's ability to demodulate signals, since having more antennas raises the probability that at least one of its channels is similar to the BS-to-user channel. Fortunately, SPP is resilient to such channel correlation, as demonstrated in Figure 6.

We conducted simulations to evaluate the impact of eavesdropper's antenna number. In our setup, the BS has 4 antennas, the user has 1 antenna, and the eavesdropper has K antennas, where K ranges from 1 to 20. For each eavesdropper antenna, the channel correlation between the BS-to-user and BS-to-eavesdropper paths is set to 0.2. The user's SNR is 20 dB, while the eavesdropper's SNR is set to infinity. Figure 7 shows the simulation results. As expected, increasing the number of eavesdropper antennas reduces the EVM of the demodulated signal and narrows the EVM_Gap. However, even with 20 antennas, the EVM_Gap remains beyond the eavesdropping threshold with high probability. These results confirm the robustness of SPP against eavesdroppers equipped with large antenna arrays.

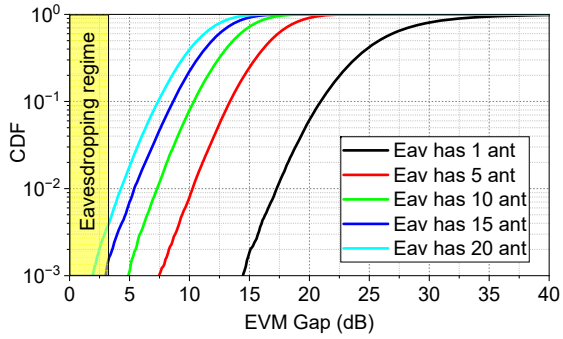


Fig. 7: Impact of eavesdropper's antenna number on the performance of SPP. Eav: eavesdropper; ant: antenna(s).

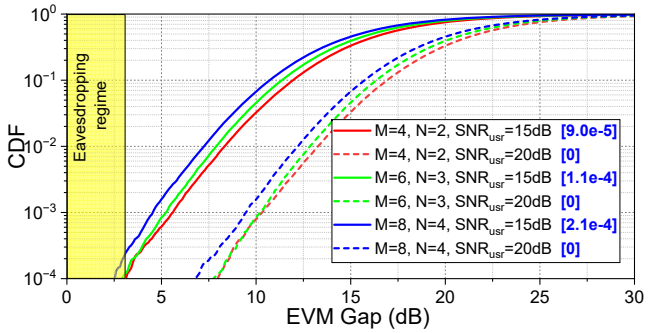


Fig. 8: EVM gap between user and eavesdropper in MU-MIMO when $\mathrm{SNR}_{eav} = \mathrm{Inf}$. Blue numbers in the legend are the projected eavesdropping rate.

Algorithm 1: Precoder design for the case where the BS has no knowledge about eavesdroppers.

Data: Intended users' channels $\mathbf{H}=[\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_N]$ and the power allocation value η
Result: Pilot precoders $\mathbf{A} = [\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_N]$ and data precoders $\mathbf{B} = [\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_N]$
1. $\mathbf{P} = \mathbf{H}^{\mathsf{H}}(\mathbf{H}\mathbf{H}^{\mathsf{H}} + \sigma^2\mathbf{I})^{-1}$;
2. $[\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_M] = \text{singular\_vectors}(\mathbf{H}\mathbf{H}^{\mathsf{H}})$;
3. $\vec{p}_i = \frac{[\mathbf{P}]_i^{\mathsf{H}}}{\|[\mathbf{P}]_i\|}$ for $i = 1, 2, \ldots, N$;
4. $\vec{a}_i = \sqrt{P}\left(\sqrt{1-\eta}\vec{p}_i + \sqrt{\eta}\vec{u}_M\right), \quad i{=}1, 2, \ldots, N$;
5. $\vec{b}_i = \sqrt{P}\left(\sqrt{1-\eta}\vec{p}_i - \sqrt{\eta}\vec{u}_M\right), \quad i{=}1, 2, \ldots, N$;

B. MU-MIMO Transmission

When there are multiple intended users, the BS may use MU-MIMO scheme for concurrent data transmission. MU-MIMO is a key technology for many wireless communication systems. When a BS has multiple antennas, it can send multiple data streams to multiple user devices on the same time-frequency resource block. Minimum mean square error (MMSE) and zero-forcing (ZF) are two widely used precoding techniques for MU-MIMO. The MMSE precoder can be written as:

$$\mathbf{P}_{\text{mu}} = \mathbf{H}^{\mathsf{H}}(\mathbf{H}\mathbf{H}^{\mathsf{H}} + \sigma^2\mathbf{I})^{-1}, \tag{5}$$

where $\mathbf{H}$ is the channel matrix, $(\cdot)^{\mathsf{H}}$ is the conjugate transpose operator, and σ^2 is the noise power. When letting $\sigma = 0$, MMSE precoder degrades to ZF precoder. It is worth noting that MU-MIMO is also vulnerable to over-the-air intercept because an eavesdropper can decode all data streams when it has more antennas than BS (transmitter).

Denote N as the number of intended user devices participating in the MU-MIMO transmission. Denote $\mathbf{H} = [\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_N]$ as the MU-MIMO channel matrix. Assume that $M \geq N+1$. Then, the singular vectors of the channel matrix can be written as:

$$[\underbrace{\vec{u}_1, \ldots, \vec{u}_N}_{\text{signal space}}, \underbrace{\vec{u}_{N+1}, \cdots, \vec{u}_M}_{\text{nullspace}}] = \text{singular\_vectors}(\mathbf{H}\mathbf{H}^{\mathsf{H}}). \tag{6}$$

Alg. 1 presents the precoder design of SPP for downlink MU-MIMO transmission. For the precoders produced by Alg. 1, we have the following remarks. **Remark 1:** The pilot and data symbols in a frame experience identical compound channels when reaching every intended user, i.e., $\vec{h}_i^{\top}\vec{a}_i = \vec{h}_i^{\top}\vec{b}_i$ for $1 \leq i \leq N$. **Remark 2:** The pilot and data symbols in a frame experience different compound channels almost surely when intercepted by every eavesdropper, i.e., $\vec{g}_k^{\top}\vec{a}_i \neq \vec{g}_k^{\top}\vec{b}_i$ for $1 \leq k \leq K$ and $1 \leq i \leq N$. This is because the over-the-air channels of different users/eavesdroppers are different almost surely.

Numerical Analysis: We use the above simulation setting to evaluate the precoder design in 4×2, 6×3, and 8×4 MU-MIMO cases, with $\eta = 0.2$. The eavesdropper has N antennas, where N is the number of intended users. We assume the eavesdropper has no noise in signal detection, i.e., $\mathrm{SNR}_{eav} = \mathrm{Inf}$. Figure 8 presents the CDF of the measured EVM gap. It can be observed that SPP has an extremely low eavesdropping rate ($\leq$2.1e-4).

VI. SPP for In-Network Eavesdroppers

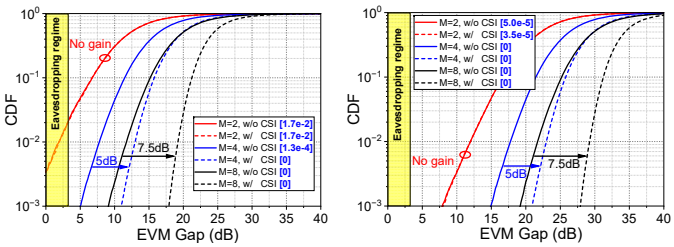
In this section, we consider the case where the eavesdroppers are compromised in-network users who respond to the requests/commands from BS in a normal way but attempt to decode the data packets for other users. As we will present in §VII, BS will be able to obtain the implicit channel knowledge about those eavesdroppers as long as they respond to the requests/commands from BS.

A. SUSE: Single User and Single Eavesdropper

We first consider the case where the BS sends data packets to a user in the presence of an eavesdropper. We assume that both user and eavesdropper have one antenna. We also assume that the BS has the implicit channel knowledge about both of them. Denote $\vec{g} \in \mathbb{C}^{M\times1}$ as the implicit channel from the BS to the eavesdropper. Recall that the optimal transmission vector for this case is $\vec{u}_1$ in Eqn (3). Then, the perturbation vector design problem can be formulated as:

$$\max_{\vec{q}} \ \|\vec{g}^{\top}\vec{q}\| \quad \text{s.t.} \ \ \vec{q} = \sum_{i=2}^{M}\lambda_m\vec{u}_m \quad \text{and} \quad \sum_{m=2}^{M}|\lambda_m|^2 = 1, \tag{7}$$

where $\lambda_m \in \mathbb{C}$ are weights for linear combination. The first constraint ensures that the perturbation vector is in the nullspace of the user's channel, and the second one ensures that its power is normalized.



(a) User's SNR = 10dB. (b) User's SNR = 20dB.

Fig. 9: EVM gap comparison in two cases: with and without eavesdropper's channel knowledge. Blue numbers in legends are the projected eavesdropping rate.

This optimization problem can be analytically solved. A closed-form solution can be obtained by projecting the eavesdropper's channel vector into the nullspace of the user's channel vector. Mathematically, the optimal solution to Eqn (7) can be written as follows:

$$\vec{q}^{\star} = \frac{\sum_{m=2}^{M} \vec{u}_m^{\mathsf{H}} \vec{g}^{*} \vec{u}_m}{\| \sum_{m=2}^{M} \vec{u}_m^{\mathsf{H}} \vec{g}^{*} \vec{u}_m \|}. \tag{8}$$

Based on Eqn (8), the precoder vectors for pilot and data symbols in a frame can be written as:

$$\begin{cases} \vec{a} = \sqrt{P}(\sqrt{1-\eta}\vec{u}_1 + \sqrt{\eta}\vec{q}^{\star}), \\ \vec{b} = \sqrt{P}(\sqrt{1-\eta}\vec{u}_1 - \sqrt{\eta}\vec{q}^{\star}), \end{cases} \tag{9}$$

where $\vec{u}_1$ is given in Eqn (3) and η is the portion of power allocated for pilot perturbation.

Numerical Analysis: We evaluate the impact of eavesdropper's channel knowledge on the EVM gap through simulation using the above parameters ($\mathrm{SNR}_{eav} = \mathrm{Inf}$ and $\eta = 0.2$). Figure 9 presents the numerical results. It can be seen that, when the BS has 4 and 8 antennas, the EVM gap increases by about 5.0 dB and 7.5 dB, respectively. When the BS has 2 antennas, the channel knowledge does not increase the EVM gap. Based on our numerical analysis and extensive simulation, we have the following remark: *The channel knowledge about eavesdroppers is not useful to decrease the eavesdropping rate in the case of $M \leq N+1$. It is useful only in the case of $M > N+1$. In this case, the more antennas the BS has, the larger gain it will generate.*

B. SUME: Single User and Multiple Eavesdroppers

We now consider the case where the BS sends data packets to one user in the presence of multiple eavesdroppers. For ease of exposition, we assume that each eavesdropper has one antenna. To the end, it should be seen that our approach also works in the case where the eavesdroppers have multiple antennas and/or work collaboratively for eavesdropping. In this case, there are different ways to define the optimization objective. Here, we set our optimization objective to maximize the minimum signal distortion among all eavesdroppers, i.e., $\min_{1\leq k\leq K}\left\{\|\vec{g}_k^{\top}\vec{q}\|\right\}$, where $\vec{g}_k \in \mathbb{C}^{M\times 1}$ is the channel of eavesdropper k, $\vec{q} \in \mathbb{C}^{M\times 1}$ is the perturbation vector, and K is the total number of eavesdroppers. Recall that $\langle \vec{u}_2, \vec{u}_3, \ldots, \vec{u}_M \rangle$ is the nullspace of the user's channel. The optimization problem can be formulated as:

$$\begin{aligned} &\max_{\vec{q}} \left\{ \min_{1\leq k\leq K} \|\vec{g}_k^{\top}\vec{q}\| \right\} \\ &\text{s.t. } \vec{q} = \sum_{i=2}^{M} \lambda_m \vec{u}_m \text{ and } \sum_{m=2}^{M} |\lambda_m|^2 = 1\,, \end{aligned} \tag{10}$$

where $\vec{g}_k$ and $\vec{u}_m$ are given values, and λ_m and $\vec{q}$ are optimization variables. The constraints in Eqn (10) ensure that $\vec{q}$ lies in the nullspace of user's channel and that $\vec{q}$ is a unity vector.

The problem in Eqn (10) is a nonconvex optimization problem. It is challenging to find its optimal solution due to its max-min objective function involving the product of two complex vectors. To address this challenge, we propose a heuristic that consists of two steps. The first step is to decouple the max-min operation in the objective function, and the second step is to greedily improve the solution (i.e., perturbation vector $\vec{q}$) from the previous step. We elaborate the proposed heuristic as follows.

• **Step 1: Solve Subproblems for Individual Eavesdroppers.** Consider the max-min operation in the objective function of Eqn (10). In this step, we consider the design of perturbation vector for individual eavesdropper k. The subproblem can be expressed as:

$$\max_{\vec{q}_k} \|\vec{g}_k^{\top}\vec{q}_k\| \quad \text{s.t. } \vec{q}_k = \sum_{m=2}^{M} \lambda_m \vec{u}_m \text{ and } \sum_{m=2}^{M} |\lambda_m|^2 = 1.$$

It is easy to see that this subproblem has already been solved previously. Based on Eqn (7) and Eqn (8), its optimal solution is:

$$\vec{q}_k^{\star} = \frac{\sum_{m=2}^{M} \vec{u}_m^{\mathsf{H}} \vec{g}_k^{*} \vec{u}_m}{\| \sum_{m=2}^{M} \vec{u}_m^{\mathsf{H}} \vec{g}_k^{*} \vec{u}_m \|}, \quad 1 \leq k \leq K. \tag{11}$$

In light of this, we first use Eqn (11) to calculate the optimal perturbation for each individual eavesdropper (i.e., $1 \leq k \leq K$) and then identify the best one from $\{\vec{q}_1^{\star}, \vec{q}_2^{\star}, \ldots, \vec{q}_K^{\star}\}$ as follows:

$$k^{\circ} = \arg\max_{1\leq k\leq K} \left\{ \min_{1\leq k'\leq K} \left(\|\vec{g}_{k'}^{\top}\vec{q}_k^{\star}\| \right) \right\}. \tag{12}$$

The result, $\vec{q}_{k^{\circ}}^{\star}$, offers the best objective value among the vectors in $\{\vec{q}_1^{\star}, \vec{q}_2^{\star}, \ldots, \vec{q}_K^{\star}\}$.

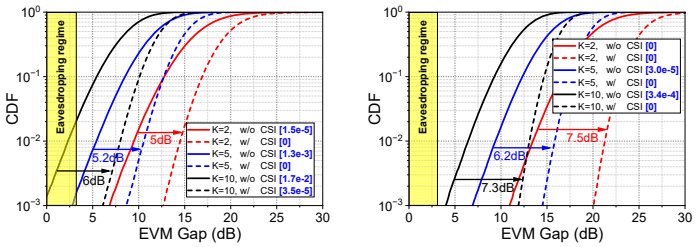
• **Step 2: Improve Bottleneck Perturbation Vector.** While $\vec{q}_{k^{\circ}}^{\star}$ offers the best objective value among $\{\vec{q}_1^{\star}, \vec{q}_2^{\star}, \ldots, \vec{q}_K^{\star}\}$, it may not be the optimal solution to the original problem in Eqn (10). Therefore, we further improve it as follows. Denote k^{+} as the index of the eavesdropper whose channel vector throttles the performance of $\vec{q}_{k^{\circ}}^{\star}$. Then, we have

$$k^{+} = \arg\min_{1\leq k\leq K} \left(\|\vec{g}_k^{\top}\vec{q}_{k^{\circ}}^{\star}\| \right). \tag{13}$$

To improve the objective value of current solution $\vec{q}_{k^{\circ}}^{\star}$, we move it towards $\vec{q}_{k^{+}}^{\star}$ so that the performance bottleneck can be elevated. Specifically, we seek a weight $w \in \mathbb{R}$ to combine

Algorithm 2: Precoder design for SUME.

Data: user' channel $\vec{h}_1$ and eavesdroppers' channels $[\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_K]$
Result: $\vec{a}$ and $\vec{b}$
1. $[\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_M] = \text{singular\_vectors}(\vec{h}_1 \vec{h}_1^{\mathsf{H}})$;
2. Calculate $\{q_1^\star, q_2^\star, \ldots, q_K^\star\}$ using Eqn (11);
3. Calculate k° using Eqn (12) and k^+ using Eqn (13);
4. Calculate $w^\star$ using Eqn (14) and $\vec{q}^\star$ using Eqn (15);
5. $\vec{a} = \sqrt{P}\left(\sqrt{1-\eta}\vec{u}_1 + \sqrt{\eta}\vec{q}^\star\right)$;
6. $\vec{b} = \sqrt{P}\left(\sqrt{1-\eta}\vec{u}_1 - \sqrt{\eta}\vec{q}^\star\right)$;



(a) BS has 4 antennas ($M = 4$). (b) BS has 8 antennas ($M = 8$).

Fig. 10: EVM gap comparison in two cases: with and without eavesdropper's channel knowledge. Blue numbers in legends are the projected eavesdropping rate.

$\vec{q}_{k^\circ}^\star$ and $\vec{q}_{k^+}^\star$ by $\vec{q} = w\vec{q}_{k^\circ}^\star + (1-w)\vec{q}_{k^+}^\star$, where

$$w^\star = \arg\max_{0 \le w \le 1} \left(\min_{1 \le k' \le K} \frac{\|w\vec{g}_{k'}^\top \vec{q}_{k^\circ}^\star + (1-w)\vec{g}_{k'}^\top \vec{q}_{k^+}^\star\|}{\|w\vec{q}_{k^\circ}^\star + (1-w)\vec{q}_{k^+}^\star\|} \right). \tag{14}$$

Since solving Eqn (14) is nontrivial, we shrink the search space of w by letting $w \in \{\frac{n}{N_w} : n = 0, 1, 2, \cdots, N_w\}$. We empirically set N_w to a small number (i.e., $N_w = 10$). Then, we employ exhaustive search to find the optimal $w^\star$. The final perturbation vector can be written as:

$$\vec{q}^\star = w^\star \vec{q}_{k^\circ}^\star + (1 - w^\star)\vec{q}_{k^+}^\star. \tag{15}$$

Alg. 2 summarizes our precoder design for SPP in this case. It can be verified that $\vec{q}^\star$ is orthogonal to $\vec{h}_1$, i.e., $(\vec{q}^\star)^\top \vec{h}_1 = 0$. This warrants that the employment of $\vec{q}^\star$ at the BS will interfere with the eavesdropper but will not generate interference for the user.

Numerical Analysis: We perform a simulation to evaluate the impact of channel knowledge on the EVM gap using the parameters stated before ($\text{SNR}_{eav} = \text{Inf}$ and $\eta = 0.2$). We consider the case of $\text{SNR}_{usr} = 15$ dB. The number of eavesdroppers ranges from 2 to 10. Figure 10 presents our numerical results. It can be seen that, with eavesdroppers' channel knowledge, the proposed precoder design algorithm can increase the EVM gap by 5dB to 7.5dB in the studied cases. More importantly, the eavesdropping rate is very low for all the cases. This confirms the effectiveness of our precoder design.

C. MUME: Multiple Users and Multiple Eavesdroppers

We then consider the case where a BS sends data packets to multiple users using MU-MIMO in the face of multiple eavesdroppers. Suppose that the BS has implicit channel knowledge about all users and eavesdroppers. In this case, an eavesdropper is not possible to decode the data packets if its antenna number is less than N. Therefore, we assume that each eavesdropper is equipped with N antennas.

This problem is nontrivial. It remains unknown how to find the optimal solution. Therefore, we extend the heuristic in §VI-B to this case. Specifically, we treat the K N-antenna eavesdroppers as KN one-antenna eavesdroppers. Then, we employ the heuristic in §VI-B by pursuing $q_1^\star$ with respect to the KN one-antenna eavesdroppers. Alg. 3 presents our precoder design for this case. It can be verified that the designed perturbation vector $\vec{q}^\star$ is orthogonal to all the users' channels. Therefore, the perturbation vector will not cause interference for the MU-MIMO transmission but effectively lower the eavesdropping rate.

Algorithm 3: Precoder design for MUME.

Data: users' channels $\mathbf{H} = [\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_N]$ and eavesdroppers' channels $[\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_{NK}]$
Result: $\mathbf{A} = [\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_N]$ and $\mathbf{B} = [\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_N]$
1. $\mathbf{P} = \mathbf{H}^{\mathsf{H}}(\mathbf{H}\mathbf{H}^{\mathsf{H}} + \sigma^2\mathbf{I})^{-1}$;
2. $\vec{p}_i = \frac{[\mathbf{P}]_i^{\mathsf{H}}}{\|[\mathbf{P}]_i\|}$ for $i = 1, 2, \ldots, N$;
3. $[\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_M] = \text{singular\_vectors}(\mathbf{H}\mathbf{H}^{\mathsf{H}})$;
4. Calculate $\{q_1^\star, q_2^\star, \ldots, q_{NK}^\star\}$ using Eqn (11);
5. Calculate k° using Eqn (12) and k^+ using Eqn (13);
6. Calculate $w^\star$ using Eqn (14) and $\vec{q}^\star$ using Eqn (15);
7. $\vec{a}_i = \sqrt{P/N}\left(\sqrt{1-\eta}\vec{p}_i + \sqrt{\eta}\vec{q}^\star\right)$ for $i = 1, 2, \ldots, N$;
8. $\vec{b}_i = \sqrt{P/N}\left(\sqrt{1-\eta}\vec{p}_i - \sqrt{\eta}\vec{q}^\star\right)$ for $i = 1, 2, \ldots, N$;

VII. Implementation

In this section, we present our implementation of SPP for evaluation. The implementation of SPP is similar to that of traditional downlink MU-MIMO transmission in 5G and WiFi. More importantly, SPP is limited its operations to the BS, requiring no software/hardware modification of user devices.

A. Implicit Channel Acquisition

One challenge in the implementation of SPP is channel acquisition. Explicit channel feedback involves channel sounding, channel coefficient quantization and compression, and channel reporting. It not only complicates the network protocol and operation, but also entails a large airtime overhead. To address this challenge, we found that the precoder design of SPP actually does not need the exact channel coefficients (i.e., $\vec{h}_i$ for $1 \le i \le N$). In fact, the relative channel coefficients (i.e., $\gamma_i \vec{h}_i$ with $\gamma_i \in \mathbb{C}$ being any non-zero value) are sufficient for the precoder design of SPP. In light of this, we employ the following implementation for channel acquisition.

Implicit Channel Feedback: We perform implicit channel feedback for BS/AP to obtain the implicit downlink channel from itself (with multiple antennas) and one user/eavesdropper. This implicit channel feedback is based on the reciprocity of uplink and downlink over-the-air channels. It comprises the following steps. **First**, the BS/AP sends a command to trigger the user for a packet (e.g., Ack) transmission. **Second**, the BS/AP receives the data packet from the user and estimates the uplink channel based on the received data packet. Denote $\vec{z}_i$ as the estimated uplink channel. **Third**, the BS/AP calculates

the implicit downlink channel $\vec{h}_i$ by letting $\vec{h}_i \equiv \mathbf{C}\vec{z}_i$, where $\mathbf{C} \in \mathbb{C}^{M\times M}$ is a complex diagonal matrix for RF calibration. Next, we introduce how to estimate RF calibration matrix $\mathbf{C}$.

RF Calibration: There are different approaches for RF calibration to obtain $\mathbf{C}$, such as using an extra RF chain for calibration and user-assisted calibration [37]. Here, we employed the user-assisted approach for calibration. It consists of three steps. **First**, the BS sends a trigger command packet to a specific user, which estimates the downlink channel $\vec{h}_0$ and reports it back to the BS. **Second**, based on the received uplink report packet, the BS estimates the uplink channel $\vec{z}_0$ through channel estimation and obtains the downlink channel $\vec{h}_0$ from the packet's payload. **Third**, it calculates the calibration diagonal matrix as follows: $\mathbf{C} = \frac{[\vec{z}_0]_1}{[\vec{h}_0]_1}\text{diag}(\vec{h}_0./\vec{z}_0)$, where $[\cdot]_1$ denotes the first element of the vector, $./$ denotes element-wise division, and $\text{diag}(\cdot)$ is to transform a vector to a diagonal matrix. We note that $\mathbf{C}$ is stable over time. It is not be affected by channels and environments. In our experiments, we measure and update $\mathbf{C}$ infrequently (once per 5 seconds). We also note that only one user is needed to participate in the RF calibration.

B. SPP for Cellular 5G

We built a TDD 5G testbed using USRP N310 and X310 devices as well as the modules from srsRAN 4G (those in `srsRAN/lib/src/phy` and `srsRAN/lib/src/radio` [38]). The testbed uses one USRP N310 device for BS, one USRP X310 for user, and another USRP X310 for eavesdropper. To leverage the reciprocity of over-the-air uplink and downlink channels, the BS must use the same antenna array for transmission and reception. functionHowever, srsRAN does not support this function. Therefore, we rewrote the UHD functions in `srsRAN/lib/src/phy/rf/rf_uhd_imp.cc`) so that all USRP devices use their "TX/RX" RF port (antenna) for both signal transmission and reception (in TDD mode). At the PHY layer, it uses the frame as shown in Figure 2(a). The bandwidth is 20MHz. The sampling rate is 30.72 MSps. The subcarrier spacing is 15 kHz. The carrier frequency is 2.1 GHz. This frequency band was used under our FCC experimental spectrum license 0954-EX-CN-2022.

To simplify the evaluation, we implement a simple MAC protocol for the communications between BS and users. It works in three steps as shown in Figure 11. **(i) RF calibration:** The BS uses the approach in section VII-A to obtain the RF calibration matrix. To reduce the airtime overhead, the user reports only three subcarriers' channel coefficients to the BS for calculating RF calibration matrix. **(ii) Uplink channel sounding:** The BS sends a `REQUEST_FOR_SOUNDING` command to the user/eavesdropper. Upon receiving this command, the user/eavesdropper sends an `NULL_DATA_PACKET` to the BS. Upon receiving this packet, the BS first estimates the uplink channel and then calculates the implicit downlink channel based on the uplink channel and the RF calibration matrix. **(iii) Downlink transmission with SPP:** Once obtaining the downlink channel, the BS calculates the SPP precoders for downlink transmission. As illustrated in Figure 11, a total of

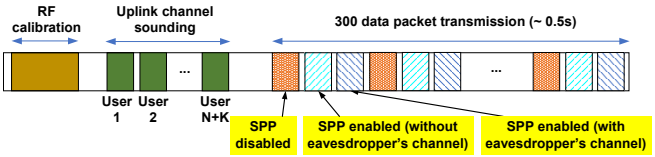


Fig. 11: MAC protocol of SPP evaluation.

300 data packets are transmitted in each round, which lasts for about 0.5 seconds. Among the 300 data packets, 100 are transmitted without SPP, 100 are transmitted with SPP when BS has not knowledge about eavesdropper(s), and 100 are transmitted with SPP when BS has implicit channel of eavesdropper(s).

C. SPP for 802.11 WiFi

We also built a WiFi testbed using the same hardware and the modules in gr-ieee802-11 on GitHub [39]. The WiFi testbed is similar to 5G. The main difference is the PHY-layer parameter and frame structure as well as the usage of pilots (preamble) in a frame. Specifically, we use the frame as shown in Figure 2(b). A frame has 20 OFDM symbols in total, with 4 symbols for preamble, one for the SIG field, and 15 for carrying data payload. The FFT size is 64, and the subcarrier spacing is 312.5 kHz. The bandwidth is 20 MHz and the sampling rate is 20 MSps. The carrier frequency is 2.46 GHz (ISM band). The MAC layer runs in the same way as shown in Figure 11.

VIII. Experimental Evaluation

A. Methodology, Objectives, Main Results

Ideally, the SPP should be evaluated in terms of PER at users and eavesdroppers. However, implementing the state-of-the-art MCS selection mechanism for rate adaption as the real 5G and WiFi systems requires extremely large engineering effort. Based on the relation of PER, MCS and EVM presented in §III-B and the PER-versus-EVM curves in [35], [36], we learned that SPP is capable of preventing an eavesdropper from decoding data packets as along as the eavesdropper's EVM is 3 dB greater than the user's EVM. Specifically, ***we use*** $\text{EVM\_Gap} = \text{EVM}_{eas} - \text{EVM}_{usr}$ ***as the performance metric. If*** $\text{EVM\_Gap} \geq 3$ ***dB, the data packets are secured against eavesdropping; otherwise, they can be eavesdropped.*** Our evaluation aims to answer the following questions.

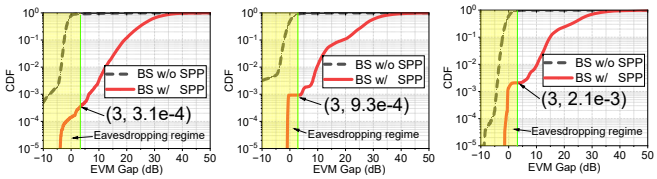
- **Q1 (§VIII-B):** When the BS/AP has no knowledge about eavesdroppers, what is the eavesdropping rate in the cases with and without SPP.
- **Q2 (§VIII-C):** How useful is the eavesdropper's CSI for improving the performance of SPP?
- **Q3 (§VIII-D):** What is the throughput cost of SPP? In other words, what is the user throughput degradation when the BS/AP uses SPP for LPI transmission.

Experimental Setup: To investigate the above questions, we deploy 5G and Wi-Fi networks in an indoor environment, as illustrated in Figure 12. The BS/AP device is placed at a

Fig. 12: Illustration of experimental scenario. There are 50 blue markers and 50 yellow markers. Blue markers indicate candidate locations for the user device, while yellow markers represent candidate locations for the eavesdropping device. In total, there are 2,500 user-eavesdropper location pairs.

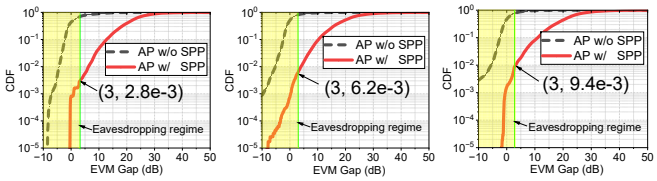
TABLE III: A summary of SPP's performance when BS/AP has no channel knowledge about eavesdropper. ('E': Eavesdropper; 'U': intended user.)

	5G			WiFi		
	M=2	M=3	M=4	M=2	M=3	M=4
E's EVM increase (dB)	30.0	31.4	28.6	21.3	22.2	22.3
E's eavesdropping rate	3.1e-4	9.3e-4	2.1e-3	2.3e-3	6.2e-3	9.4e-3
U's EVM increase (dB)	2.9	4.5	3.3	2.3	3.7	2.7
U's throughput cost	12%	17%	13%	10%	18%	14%



(a) BS has 2 ants. (b) BS has 3 ants. (c) BS has 4 ants.

Fig. 13: EVM gap distribution in a 5G network.



(a) AP has 2 ants. (b) AP has 3 ants. (c) AP has 4 ants.

Fig. 14: EVM gap distribution in a WiFi network.

fixed location and equipped with four omnidirectional antennas. The network includes one user and one eavesdropper, each equipped with a single antenna. The scenario has 50 blue markers and 50 yellow markers as shown in the figure. The 50 blue numbers denote candidate positions for the user device, while the 50 yellow numbers represent candidate positions for the eavesdropper. This results in a total of 2,500 user–eavesdropper location pairs. In some cases, the user and eavesdropper are placed very close to each other (less than 20 cm apart). For each location pair, 2,000 data packets are collected over 40 iterations. For all data samples across all location pairs, the EVM of demodulated signals is recorded at both the user and eavesdropper devices, and used to construct the EVM Gap dataset. We set $\eta = 0.2$ for all experiments.

Main Results: Table III summarizes our main experimental observations, including the benefits (low eavesdropping rate) and the cost (user throughput degradation) of SPP. In what follows, we delve into the details.

B. EVM Gap without Eavesdropper's CSI

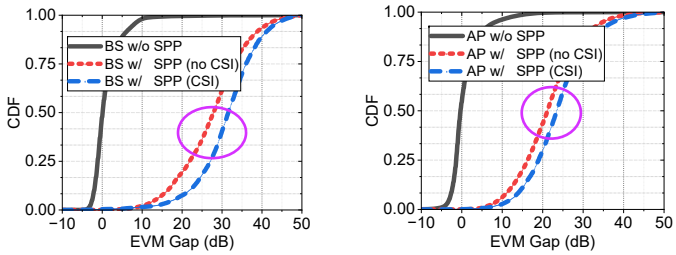
To answer **Q1**, we consider the case where the BS/AP has two, three, and four antennas. We collected the EVM data from user and eavesdropper to plot their EVM Gap.

5G Network: Figure 13 plots the EVM gap distributions when the BS has 2, 3, and 4 antennas. It can be seen that the use of SPP creates a significant EVM gap between the user and the eavesdropper. On average, the EVM gap is 30.0 dB when the BS has 2 antennas, 31.4 dB when the BS has 3 antennas, and 28.6 dB when the BS has 4 antennas.

While the EVM gap is significant in all cases, the impact of BS's antenna number on the EVM gap does not agree with our numerical results in Figure 5. We expected to see that the more antennas the BS has, the larger the EVM gap appears. However, this was not observed in our experimental results. We believe this discrepancy can be attributed to the channel feedback errors in real systems. In the simulation, we assumed that the channel knowledge is perfect at BS. In our experiments, the channels are obtained via implicit feedback. More antennas introduce a larger error in channel acquisition. A better channel acquisition scheme can further improve the EVM gap (and thus reduce the eavesdropping rate).

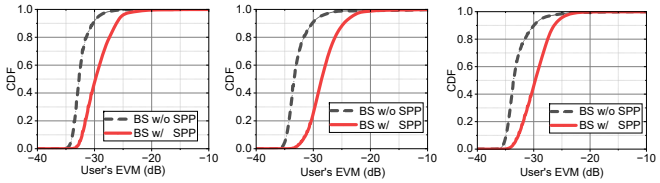
A crucial point on the CDF curves in Figure 13 is EVM_Gap = 3 dB. Recall that we use 3 dB as the threshold to determine if an eavesdropper can decode the data packet (see §III-B). Therefore, based on the results in Figure 13, the projected eavesdropping rate is 3.1e-4 when the BS has 2 antennas, 9.3e-4 when the BS has 3 antennas, and 2.1e-3 when the BS has 4 antennas.

WiFi Network: Figure 14 shows the measured EVM gap in the WiFi network. Similarly, we can observe that the use of SPP creates a significant EVM gap between user and eavesdropper. Numerically, the average of EVM gap is 21.3 dB when the AP has 2 antennas, 22.2 dB when the AP has 3 antennas, and 22.3 when the AP has 4 antennas. In addition, the probability of EVM gap less than 3 dB is 2.3e-3 when the AP has 2 antennas, 6.2e-3 when the AP has 3 antennas, and 9.4e-3 when the AP has 4 antennas. This indicates that the probability of an eavesdropper successfully decoding the data packets from an AP is 2.3e-3, 6.2e-3, and 9.4e-3 in these three cases, respectively.



(a) 5G network. (b) WiFi network.

Fig. 15: Impacts of eavesdropper's CSI.



(a) BS has 2 ants. (b) BS has 3 ants. (c) BS has 4 ants.

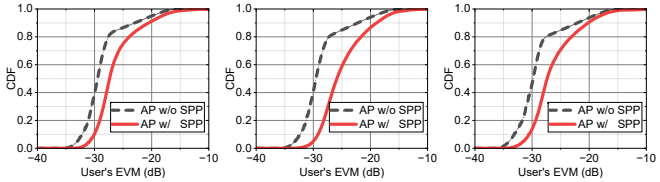
Fig. 16: CDF of user's EVM in a 5G network.

C. EVM Gap with Eavesdropper's CSI

To answer **Q2**, we consider the case where the BS/AP has 4 antennas. The BS/AP sends data packets to one user in the presence of one eavesdropper. Both user and eavesdropper have one antenna. The BS/AP has the implicit channel knowledge for both user and eavesdropper. For a fair comparison, the BS/AP sends its data packets following the sequence as shown in Figure 11: i) no SPP, ii) SPP without CSI, and iii) SPP with CSI. We measured the EVM gap and plot the results in Figure 15(a-b). It can be seen that the eavesdropper's CSI is indeed useful to increase the EVM gap. On average, the eavesdropper's CSI can increase the EVM gap by 3.6 dB in the 5G network and by 2.1 dB in the WiFi network. This experimental observation agrees with the numerical results in Figure 10(a). This confirms that the eavesdropper's CSI is indeed useful to increase the EVM gap between user and eavesdropper.

D. User Throughput Cost of SPP

The core idea of SPP lies in the design of transmission and perturbation vectors. A coefficient η has been used to allocate BS/AP's power between the transmission vector (for data transmission) and the perturbation vector (for anti-eavesdropping). This means that SPP enables LPI communications at the cost of reducing user throughput. In this part,



(a) AP has 2 ants. (b) AP has 3 ants. (c) AP has 4 ants.

Fig. 17: CDF of user's EVM in a WiFi network.

TABLE IV: EVM-to-MCS mapping in a 5G network [35].

EVM (dB)	-2	-5	-10	-14	-16	-19	-20	-23	-26	-30	-33
Modulation order	2	2	6	6	6	6	8	8	8	10	10
Coding rate	1/3	2/3	1/3	1/2	2/3	5/6	2/3	5/6	8/9	13/14	17/18
Data rate (bps/Hz)	2/3	4/3	2	3	4	5	16/3	20/3	64/9	65/7	85/9

TABLE V: EVM-to-MCS mapping in 802.11ac [41].

EVM (dB)	-5	-10	-13	-16	-19	-22	-25	-27	-30	-32
Modulation order	1	2	2	4	4	6	6	6	8	8
Coding rate	1/2	1/2	3/4	1/2	3/4	2/3	3/4	5/6	3/4	5/6
Data rate (bps/Hz)	0.5	1	1.5	2	3	4	4.5	5	6	6.7

we aim to answer **Q3** by conducting experiments to evaluate the throughput degradation caused by SPP.

EVM Increase: To evaluate the user throughput degradation, we measure the EVM at the intended user. Figure 16 presents our experimental results collected in the 5G network. We observed that the use of SPP increases the intended user's average EVM by 3.0 dB (from -32.9 dB to -29.9 dB) when the BS is equipped with 2 antennas, by 4.5 dB (from -33.2 dB to -28.7 dB) when the BS is equipped with 3 antennas, and by 3.3 dB (from -33.4 dB to -30.1 dB) when the BS is equipped with 4 antennas. Figure 17 presents our experimental results from a WiFi network. We observed that the EVM increases 2.4 dB, 3.7 dB, and 2.7 dB in the three cases. We note that the increased EVM depends on many factors such as power allocation η, BS' antenna correlation, and channel conditions. At least, the above experimental results showcase that user's EVM increase is in an acceptable range.

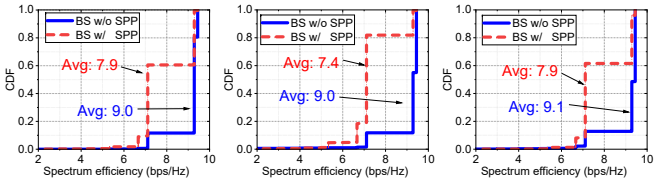
Throughput Cost: To better understand the cost of SPP, we now study the user throughput degradation caused by SPP. We convert the measured EVM values to user throughput following the classic system-level simulation methodology [40]. Specifically, we use the EVM-to-MCS mapping values in Table IV and Table V to calculate the user throughput for 5G and WiFi networks, respectively.

Figure 18 presents the calculated user throughput in a 5G network when the BS is with and without SPP. We observed that, on average, the use of SPP at BS decreases the user throughput by 12% (from 9.0 to 7.9 bps/Hz) when the BS has two antennas, by 17% (from 9.0 to 7.4 bps/Hz) when the BS has three antennas, and by 13% (from 9.1 to 7.9 bps/Hz) when the BS has four antennas. Similar user throughput degradation was observed in the WiFi network. Specifically, Figure 19 presents the calculated user throughput in a WiFi network when the AP is with and without SPP. On average, the use of SPP at AP decreases the user throughput by 10% (from 5.3 to 4.8 bps/Hz) when the AP has 2 antennas, 18% (from 5.4 to 4.4 bps/Hz) when the AP has 3 antennas, and 14% (from 5.5 to 4.8 bps/Hz) when the AP has 4 antennas.

Table III summarizes our observed eavesdropping rate and user throughput cost of SPP in both 5G and WiFi networks.

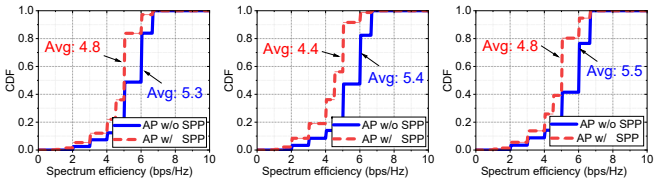
IX. Discussions and Limitations

SPP in Mobility: SPP and conventional MU-MIMO have the same CSI requirements (e.g., channel acquisition and channel coherence time). They share the same precoding operations and only differ in precoding purposes. Therefore,



(a) AP has 2 ants. (b) AP has 3 ants. (c) AP has 4 ants.

Fig. 18: User throughput in a 5G network.



(a) AP has 2 ants. (b) AP has 3 ants. (c) AP has 4 ants.

Fig. 19: User throughput in a WiFi network.

SPP should be applicable to all scenarios where MU-MIMO has been applied. We note that MU-MIMO has been widely used in both Wi-Fi and 5G, indoor and outdoor, stationary and mobile scenarios. We expect that SPP can work in those scenarios as well. In our future work, we will experimentally evaluate the performance of SPP in high-mobility outdoor scenarios.

Application Scenario: While our design of SPP focuses on the downlink transmission, SPP can also be used for safeguarding uplink transmission as long as the user devices have two or more antennas. Moreover, SPP is not limited to infrastructure-based networks or OFDM-based wireless networks. It is also applicable to ad hoc networks or non-OFDM communications, as long as their data transmissions use QAM modulation.

SPP in FDD Systems: The channel acquisition design of SPP was based on the channel reciprocity in TDD mode. A question to ask is if SPP can work in FDD systems. We believe so. FDD only affects implicit CSI feedback. Many works have already shown that downlink channel can be inferred based on uplink channel in FDD systems via model-based approach [42] or learning-based approach [43], [44]. Therefore, SPP should work in FDD mode.

SPP in Narrowband Communications: SPP is specifically designed for broadband communication systems such as 5G and Wi-Fi, both of which employ powerful LDPC codes. In contrast, narrowband communication systems like Bluetooth, ZigBee, and LoRa typically use lightweight coding schemes (e.g., convolutional codes) or may not use any coding at all. Moreover, devices in these systems often lack multiple antennas, which are essential for SPP to function. As a result, SPP is not applicable to these narrowband communication systems.

Experimental Evaluation: Our current experimental evaluation is limited to a single-user, single-eavesdropper setup in indoor environments. It is important to evaluate the performance of SPP in more complex scenarios, including multi-user, multi-eavesdropper cases and large-scale outdoor networks. Additionally, studying the effectiveness of SPP in low-SNR regimes is a critical direction for future investigation. These extensions will be explored in our future work.

X. Related Work

SPP is a transmitter-side precoding technique that uses different precoders for the pilot and data symbols in a frame. Such an approach has never been explored in the literature. However, it is related to the following PHY-layer LPI techniques.

Beamforming: Beamforming has been widely used for enhancing PHY-layer security, and the prior work has produced a large amount of results [7]–[26]). This work mainly focuses on either maximizing the signal strength at the intended user through beam steering [7], [9], [18], [21], or minimizing the signal strength at eavesdropper through beam nullification [8], [23], [24]. The former requires the channel/location information of the user, while the latter needs the channel/location information of the eavesdropper(s). SPP belongs to this research category. However, the idea of differentiating the pilot and data symbols in a frame for precoding has never been explored before. Thus, SPP is a new precoding technique.

Preamble Randomization: SPP is also related to preamble randomization [6]. The key idea is to use different preambles following a pre-given pattern. To use this technique, transmitter and receiver need to sync their randomization pattern at the initialization stage, which may lead to security risks. On the contrary, SPP does not need pre-shared knowledge between transmitter and receiver.

Artificial Noise (AN): AN is another popular technique to protect wireless communications against eavesdropping at the PHY layer [2], [3], [45]–[56]. One approach of AN is injection [2], [3]. When the receiver has the information of AN, it can first pre-cancel the AN and then decode the data packet. Assume that the eavesdropper does not know the information of AN, the AN will prevent the eavesdropper from decoding the data packet. AN is always used with beamforming [16], [54]. In this case, a transmitter nullifies the noise beam towards the user(s) and maximizes the noise beam towards eavesdroppers. In contrast, SPP does not involve AN as it is a purely precoding technique.

Other LPI Techniques: There are many other PHY-layer LPI techniques to secure the communication privacy, such as channel-based key generation [30], [31], spectrum spreading, time/frequency hopping, and spatial-time-modulation [27]–[29]. However, SPP differs itself from these techniques significantly. For instance, spectrum sharing and frequency hopping require pre-shared knowledge between transmitter and receiver. Channel-based key generation does not explore the spatial domain of wireless channels.

XI. Conclusion

In this paper, we introduced SPP for LPI wireless communications. SPP is a physical-layer precoding technique that does not require any knowledge about eavesdroppers. SPP has been designed based on the observation that a radio receiver can demodulate a signal frame only if the pilot and data symbols in the signal frame experience identical compound channels.

The key idea behind SPP is using different weight vectors for precoding the pilot and data symbols in the same signal frame. We have implemented and evaluated SPP on 5G and WiFi testbeds. Extensive experimental results have confirmed the effectiveness and efficiency of SPP. We hope that SPP will open up a new research line of MIMO, with the aim of improving physical-layer security in addition to maximizing the spectral efficiency for wireless networks.

REFERENCES

[1] N. Li, "Research on diffie-hellman key exchange protocol," in *2010 2nd International Conference on Computer Engineering and Technology*, vol. 4, pp. V4–634, IEEE, 2010.

[2] J. Choi, J. Joung, and Y.-S. Cho, "Artificial-noise-aided space–time line code for enhancing physical layer security of multiuser mimo downlink transmission," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1289–1300, 2021.

[3] G. Jang, D. Kim, I.-H. Lee, and H. Jung, "Cooperative beamforming with artificial noise injection for physical-layer security," *IEEE Access*, vol. 11, pp. 22553–22573, 2023.

[4] M. Gao, Y. Chen, Y. Liu, J. Xiong, J. Han, and K. Ren, "Cancelling Speech Signals for Speech Privacy Protection against Microphone Eavesdropping," in *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*, pp. 1–16, 2023.

[5] X. Li, C. Feng, F. Song, C. Jiang, Y. Zhang, K. Li, X. Zhang, and X. Chen, "Protego: securing wireless communication via programmable metasurface," in *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, pp. 55–68, 2022.

[6] J. D. Monti, *User Equipment-Side Initiation for 5G Communications*. PhD thesis, Monterey, CA; Naval Postgraduate School, 2021.

[7] F. Dong, W. Wang, X. Li, F. Liu, S. Chen, and L. Hanzo, "Joint beamforming design for dual-functional mimo radar and communication systems guaranteeing physical layer security," *IEEE Transactions on Green Communications and Networking*, vol. 7, no. 1, pp. 537–549, 2023.

[8] H. Jung and I.-H. Lee, "Distributed null-steering beamformer design for physical layer security enhancement in internet-of-things networks," *IEEE Systems Journal*, vol. 15, no. 1, pp. 277–288, 2020.

[9] Z. Kong, S. Yang, D. Wang, and L. Hanzo, "Robust beamforming and jamming for enhancing the physical layer security of full duplex radios," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3151–3159, 2019.

[10] Ö. Cepheli, S. Tedik, and G. K. Kurt, "A high data rate wireless communication system with improved secrecy: Full duplex beamforming," *IEEE communications letters*, vol. 18, no. 6, pp. 1075–1078, 2014.

[11] W. Zhang, J. Chen, Y. Kuo, and Y. Zhou, "Transmit beamforming for layered physical layer security," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 10, pp. 9747–9760, 2019.

[12] 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.

[13] Z. Sheng, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Beamforming optimization for physical layer security in miso wireless networks," *IEEE Transactions on Signal Processing*, vol. 66, no. 14, pp. 3710–3723, 2018.

[14] F. Zhu, F. Gao, H. Lin, S. Jin, J. Zhao, and G. Qian, "Robust beamforming for physical layer security in bdma massive mimo," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 775–787, 2018.

[15] X. Tian, M. Li, Z. Wang, and Q. Liu, "Hybrid precoder and combiner design for secure transmission in mmwave mimo systems," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pp. 1–6, IEEE, 2017.

[16] Y. R. Ramadan and H. Minn, "Artificial noise aided hybrid precoding design for secure mmwave miso systems with partial channel knowledge," *IEEE Signal Processing Letters*, vol. 24, no. 11, pp. 1729–1733, 2017.

[17] N. Zhao, D. Li, M. Liu, Y. Cao, Y. Chen, Z. Ding, and X. Wang, "Secure transmission via joint precoding optimization for downlink miso noma," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 8, pp. 7603–7615, 2019.

[18] C. Wang, Z. Li, T.-X. Zheng, H. Chen, and X.-G. Xia, "Robust hybrid precoding design for securing millimeter-wave iot networks under secrecy outage constraint," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 13024–13038, 2021.

[19] E. Yaacoub and M. Al-Husseini, "Achieving physical layer security with massive mimo beamforming," in *2017 11th European conference on antennas and propagation (EUCAP)*, pp. 1753–1757, IEEE, 2017.

[20] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information-and jamming-beamforming for physical layer security with full duplex base station," *IEEE Transactions on Signal Processing*, vol. 62, no. 24, pp. 6391–6401, 2014.

[21] J. Chu, R. Liu, Y. Liu, M. Li, and Q. Liu, "Joint transmit beamforming design for secure communication and radar coexistence systems," in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 205–209, IEEE, 2022.

[22] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2016.

[23] Y. Alsaba, C. Y. Leow, and S. K. A. Rahim, "Null-steering beamforming for enhancing the physical layer security of non-orthogonal multiple access system," *IEEE Access*, vol. 7, pp. 11397–11409, 2019.

[24] J. Kong, F. T. Dagefu, and B. M. Sadler, "Simultaneous beamforming and nullforming for covert wireless communications," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pp. 1–6, IEEE, 2020.

[25] S. Komeylian, C. Paolini, and M. Sarkar, "Beamforming technique for improving physical layer security in an mimo-ofdm wireless channel," in *Advances in Distributed Computing and Machine Learning: Proceedings of ICADCML 2023*, pp. 127–134, Springer, 2023.

[26] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Physical layer security of mimo–ofdm systems by beamforming and artificial noise generation," *Physical Communication*, vol. 4, no. 4, pp. 313–321, 2011.

[27] K. Chen, S. Yang, Y. Chen, D. Yang, M. Huang, S.-W. Qu, and J. Hu, "Lpi beamforming based on 4-d antenna arrays with pseudorandom time modulation," *IEEE Transactions on Antennas and Propagation*, vol. 68, no. 3, pp. 2068–2077, 2019.

[28] S. Venkatesh, X. Lu, B. Tang, and K. Sengupta, "Secure space–time-modulated millimetre-wave wireless links that are resilient to distributed eavesdropper attacks," *Nature Electronics*, vol. 4, no. 11, pp. 827–836, 2021.

[29] J. Zhao, S. Qiao, J. H. Booske, and N. Behdad, "Low-probability of intercept/detect (lpi/lpd) secure communications using antenna arrays employing rapid sidelobe time modulation," *IEEE Transactions on Antennas and Propagation*, 2024.

[30] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, 2016.

[31] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *Ieee access*, vol. 4, pp. 614–626, 2016.

[32] Z. Liu, K. P. Dasala, D. Mu, R. Doost-Mohammady, and E. W. Knightly, "M3a: Multipath multicarrier misinformation to adversaries," in *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*, pp. 1–15, 2023.

[33] DEVCOM ARL, "Current research topics for devcom arl baa for foundational research." Document updated as of October 31, 2023, 2023. W911NF-23-S-0001.

[34] I. S. Association *et al.*, "802.11 a-1999—ieee standard for telecommunications and information exchange between systems—lan/man specific requirements—part 11: Wireless medium access control (mac) and physical layer (phy) specifications: High speed physical layer in the 5 ghz band," tech. rep., Technical Report, 1999.

[35] J. H. Bae, A. Abotabl, H.-P. Lin, K.-B. Song, and J. Lee, "An overview of channel coding for 5g nr cellular communications," *APSIPA transactions on signal and information processing*, vol. 8, p. e17, 2019.

[36] "Ns-3: Wi-fi module: Design documentation - 34.1.3.1.6. tablebasederrorratemodel." https://www.nsnam.org/docs/models/html/wifi-design.html. Online: Accessed [18-08-2023].

[37] H. Pirayesh, S. Zhang, P. K. Sangdeh, and H. Zeng, "Maloragw: Multi-user mimo transmission for lora," in *Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems*, pp. 179–192, 2022.

[38] srsRAN Project, "srsRAN 4G: Open Source 4G LTE RAN Software." https://github.com/srsran/srsRAN_4G, 2023. Accessed on December-6-2023.

[39] B. Bloessl, M. Segata, C. Sommer, and F. Dressler, "Performance Assessment of IEEE 802.11p with an Open Source SDR-based Prototype," *IEEE Transactions on Mobile Computing*, vol. 17, pp. 1162–1175, May 2018.

[40] L. Chenand, W. Chen, B. Wang, X. Zhang, H. Chen, and D. Yang, "System-level simulation methodology and platform for mobile cellular systems," *IEEE Communications Magazine*, vol. 49, no. 7, pp. 148–155, 2011.

[41] Tektronix, "Wi-fi: Overview of the 802.11 physical layer and transmitter measurements," 2014.

[42] D. Vasisht, S. Kumar, H. Rahul, and D. Katabi, "Eliminating channel feedback in next-generation cellular networks," in *Proceedings of the 2016 ACM SIGCOMM Conference*, pp. 398–411, 2016.

[43] A. Bakshi, Y. Mao, K. Srinivasan, and S. Parthasarathy, "Fast and efficient cross band channel prediction using machine learning," in *The 25th Annual International Conference on Mobile Computing and Networking*, pp. 1–16, 2019.

[44] Z. Liu, G. Singh, C. Xu, and D. Vasisht, "Fire: enabling reciprocity for fdd mimo systems," in *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, pp. 628–641, 2021.

[45] M. R. Khandaker, C. Masouros, and K.-K. Wong, "Constructive interference based secure precoding: A new dimension in physical layer security," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2256–2268, 2018.

[46] W. Wang, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1470–1482, 2017.

[47] L. Hu, J. Peng, Y. Zhang, H. Wen, S. Tan, and J. Fan, "Artificial noise assisted interference alignment for physical layer security enhancement," in *GLOBECOM 2022-2022 IEEE Global Communications Conference*, pp. 4148–4153, IEEE, 2022.

[48] B. He, Y. She, and V. K. Lau, "Artificial noise injection for securing single-antenna systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9577–9581, 2017.

[49] A. Al-Nahari, G. Geraci, M. Al-Jamali, M. H. Ahmed, and N. Yang, "Beamforming with artificial noise for secure misome cognitive radio transmissions," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 1875–1889, 2018.

[50] Y. Deng, L. Wang, S. A. R. Zaidi, J. Yuan, and M. Elkashlan, "Artificial-noise aided secure transmission in large scale spectrum sharing networks," *IEEE Transactions on Communications*, vol. 64, no. 5, pp. 2116–2129, 2016.

[51] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, "Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8286–8297, 2016.

[52] M. Zeng, N.-P. Nguyen, O. A. Dobre, and H. V. Poor, "Securing downlink massive mimo-noma networks with artificial noise," *IEEE Journal of Selected Topics in Signal Processing*, vol. 13, no. 3, pp. 685–699, 2019.

[53] F. Shu, L. Xu, J. Wang, W. Zhu, and Z. Xiaobo, "Artificial-noise-aided secure multicast precoding for directional modulation systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6658–6662, 2018.

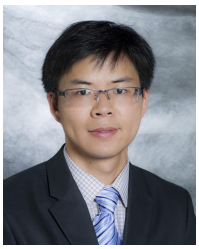
[54] S. Wang, X. Xu, K. Huang, X. Ji, Y. Chen, and L. Jin, "Artificial noise aided hybrid analog-digital beamforming for secure transmission in mimo millimeter wave relay systems," *IEEE Access*, vol. 7, pp. 28597–28606, 2019.

[55] B. Li, M. Zhang, Y. Rong, and Z. Han, "Artificial noise-aided secure relay communication with unknown channel knowledge of eavesdropper," *IEEE Transactions on Wireless Communications*, vol. 20, no. 5, pp. 3168–3179, 2021.

[56] A. Özçelikkale and T. M. Duman, "Cooperative precoding and artificial noise design for security over interference channels," *IEEE Signal Processing Letters*, vol. 22, no. 12, pp. 2234–2238, 2015.

Peihao Yan is currently a PhD student in the Department of Computer Science and Engineering at Michigan State University (MSU), East Lansing, MI. She received her B.E. degree in communication engineering in 2020 and her M.S. degree in Computer Science and Technology in 2023 from China University of Petroleum (East China), Qingdao, China. Her current research interests include wireless networking and communications, with emphasis on 5G systems and O-RAN.

Milad Afshari received the B.Sc. degree in Electrical Engineering from the University of Zanjan, Zanjan, Iran, in 2014, and the M.Sc. degree in Electrical Engineering from K. N. Toosi University of Technology, Tehran, Iran, in 2017. He also completed graduate-level coursework in Electrical Engineering at the University of Tehran, Tehran, Iran, from 2019 to 2022. He is currently working toward the Ph.D. degree in the Department of Computer Science and Engineering at Michigan State University, East Lansing, MI, USA. His research interests include wireless communications, signal processing, machine learning, explainable AI, and natural language processing.



Huacheng Zeng (SM'20) is an Associate Professor in the Department of Computer Science and Engineering at Michigan State University (MSU). Prior to joining MSU, Dr. Zeng was an Assistant Professor in the Department of Electrical and Computer Engineering at the University of Louisville. He also worked as a Senior System Engineer at Marvell Semiconductor, where he contributed to the development of wireless system solutions. He received his Ph.D. in Computer Engineering from Virginia Polytechnic Institute and State University (Virginia Tech). Dr. Zeng is a recipient of the NSF CAREER Award (2019), the Best Paper Award at IEEE SECON (2021), and the Best Student Paper Award at ACM WUWNET (2014). His research interests broadly include wireless networking and mobile sensing systems. He is serving on the editorial board of IEEE Transactions of Wireless Communications.