Multi-Antenna Data-Driven Eavesdropping Attacks and Symbol-Level Precoding Countermeasures

Abderrahmane Mayouche, *Student Member, IEEE*, Wallace A. Martins, *Senior Member, IEEE*, Christos G. Tsinos, *Senior Member, IEEE*, Symeon Chatzinotas, *Senior Member, IEEE* and Björn Ottersten, *Fellow, IEEE*

***Abstract*—In this work, we consider secure communications in wireless multi-user (MU) multiple-input single-output (MISO) systems with channel coding in the presence of a multi-antenna eavesdropper (Eve), who is a legit user trying to eavesdrop other users. In this setting, we exploit machine learning (ML) tools to design soft and hard decoding schemes by using precoded pilot symbols as training data. The proposed ML frameworks allow an Eve to determine the transmitted message with high accuracy. We thereby show that MU-MISO systems are vulnerable to such eavesdropping attacks even when relatively secure transmission techniques are employed, such as symbol-level precoding (SLP). To counteract this attack, we propose two novel SLP-based schemes that increase the bit-error rate at Eve by impeding the learning process. We design these two security-enhanced schemes to meet different requirements regarding runtime, security, and power consumption. Simulation results validate both the ML-based eavesdropping attacks as well as the countermeasures, and show that the gain in security is achieved without affecting the decoding performance at the intended users.**

***Index Terms*—Physical-layer security, symbol-level precoding, machine learning, channel coding, and multi-user interference.**

I. Introduction

While fifth generation (5G) cellular networks are currently being provisioned worldwide, its successor generation, named 6G wireless system, is being proposed to overcome several limitations in 5G [1]–[3]. By 2023, there will likely be 5.7 billion total mobile users (71% of the world population) [4]. In such a crowded environment, unintended receivers, e.g., an eavesdropper (Eve), may decode sensitive information given the broadcasting nature of the wireless channel [5]. As a result, security is of primary importance in next generation networks. In particular, physical-layer security (PLS) stands out as a powerful technology to complement encryption-based methods [6], including application-layer encryption.

The essence of PLS is to exploit the characteristics of the wireless channel, i.e., fading, noise, interference, and diversity, to attain an acceptable decoding performance at intended users while obstructing the correct decoding at Eve. Alternatively, the aim of PLS is to increase the gap of correct decoding rates between intended users and Eve [7]. PLS is foreseen to be used as a complementary layer of protection, in addition to the existing cryptography-based security methods. As the rise of quantum computing [8], [9] is threatening both symmetric and asymmetric cryptography, non-cryptographic-based methods such as PLS are needed [10]–[12]. In this setting, the *artificial noise* (AN) scheme [13] and its extensions [14]–[17] have been proposed to improve PLS.

In this context, symbol-level precoding (SLP) [18]–[20] has been introduced as a new way for attaining PLS [21]. Although not originally conceived as a PLS method, SLP is more secure than block-level precoding, like zero-forcing (ZF) [22], as the precoder is redesigned for each symbol period (SP). In [23], [24], secure SLP precoding schemes were proposed in the context of a multiple-input single-output (MISO) wiretap channel while considering only a single-antenna Eve. In [25], the authors proposed to exploit the statistical characteristics of the received signal at Eve in order to improve its detection performance. To counter this vulnerability, the authors in [25] proposed secure SLP-based precoding schemes to degrade Eve's performance.

Machine learning (ML) has attracted significant interest in the area of wireless communications [26]. ML is a core subset of artificial intelligence (AI), which is an ensemble of tools and algorithms intended for making predictions or decisions through learning patterns from data [27]. In other words, based on a dataset, ML algorithms build a mathematical model in order to make predictions or decisions.

AI has been envisioned by several researchers as the most prominent feature of 6G [28], since it is an efficient tool for several contemporary complex scenarios. For instance, ML techniques can be categorized into two distinct objectives related to extracting patterns from data: first, performance improvement, in which ML is used to optimize the operating parameters at the lower layers; second, information processing of the huge data generated by wireless devices at the application layer [29].

Nevertheless, the potential of ML is not fully exploited in PLS, although ML for PLS has been explored in some recent works [30]–[32], [32]. In [30], the authors proposed an attack where ML is used to determine the underlying modulation scheme. In [31], the authors employed ML for wiretap code design considering Gaussian channels under finite block length, and a similar idea was proposed in [32].

In the context of multi-user (MU) MISO systems, a related PLS work is [33], where we proposed an ML-based attack in

The authors are with the Interdisciplinary Centre for Security Reliability and Trust (SnT), University of Luxembourg, L-1855, Luxembourg (E-mails: {abderrahmane.mayouche, wallace.alvesmartins, christos.tsinos, symeon.chatzinotas, and bjorn.ottersten}@uni.lu).

This work is supported by the Engineering and Physical Sciences Research Council (EPSRC) and the Luxembourg National Research Fund (FNR) project, titled Exploiting Interference for Physical Layer Security in 5G Networks (CI-PHY) under Grant 11607830, and the AGNOSTIC project with the European Research Council under Horizon 2020 grant agreement 742648.

Part of this work has been accepted for publication in the *Proceedings of the IEEE Wireless Communications and Networking Conference* (WCNC), 2021.

uncoded systems, in which an Eve can use ML to improve its detection performance via pilot symbols. Since most communication systems employ forward-error correction (FEC), it is important to investigate eavesdropping in systems that feature FEC. To that end, in our present work, we go beyond [33] by considering a practical scenario where channel coding is employed. It is worth mentioning that the Eve can exploit the redundancy induced by channel coding to improve its decoding capabilities during the attack.

Herein, in a FEC-enabled MU-MISO system with a multi-antenna Eve, who is a registered user, we first propose ML frameworks that allow an Eve to soft/hard decode the transmitted message with good accuracy, i.e., coded FER at Eve around 10^{-3}. After introducing these two decoding attacks, we validate them in the aforementioned MU-MISO system, and show that even conventional SLP-based schemes [21] are vulnerable to such attacks. As a countermeasure to these attacks, we propose two novel security-enhanced SLP-based schemes that impair the ML training process, thus enhancing security. Simulation results show the efficacy of the ML-based attacks against conventional precoders, i.e., very low bit-error rate (BER) at Eve, indicating good decoding performance, and the effectiveness of the proposed countermeasures, i.e., high BER at Eve even with numerous antennas, implying poor decoding performance. The primary contributions of the paper are listed below:

1) We introduce eavesdropping attacks in MU-MISO systems with FEC by proposing novel ML-based soft and hard decoding schemes, where a multi-antenna Eve can use ML and the knowledge of pilot symbols as well as the added redundancy related to channel coding to decode the transmitted data with high accuracy.
2) We introduce the soft decoding scheme by proposing an ML framework that can be used by an Eve to correctly soft-decode messages sent to a particular user in an MU-MISO system. Furthermore, we also propose an ML-based hard decoding scheme at the Eve. We design the ML framework of this scheme to directly predict the coded bits.
3) To counteract these eavesdropping attacks, we propose two security-enhanced SLP-based schemes that aim to increase the BER at Eve by impeding the learning process. This is performed by either embedding randomness in Eve's received signal or minimizing Eve's received power. We note that the proposed schemes assume perfect knowledge of Eve's channel at the BS [34]–[37], which is the case when Eve is part of the system trying to eavesdrop other users.
4) We design these two PLS schemes in such a way that different requirements for security, runtime, and power consumption are met, to provide the base station (BS) with options to choose the most suitable scheme depending on the desired criteria.
5) We validate the eavesdropping attacks as well as the countermeasures through extensive simulations, where we show the vulnerability when using non-secure precoding schemes and the drastic security gains when using our proposed PLS schemes.

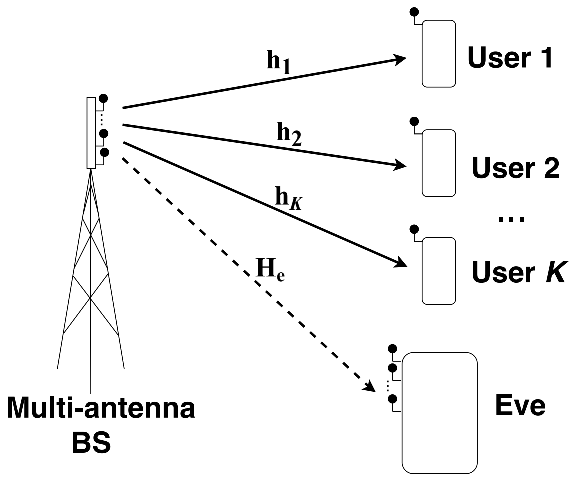


Fig. 1: Downlink MU-MISO system comprised of: a BS with N_t antennas, K single-antenna users, and one Eve with M antennas.

The rest of the paper is organized as follows: Section II describes the system model. In Section III, we introduce the ML-based attacks, whereas in Section IV, we propose our novel SLP-based schemes as countermeasures to this attack. Simulation results are discussed in Section V, followed by the conclusion in Section VI.

Notations: $\|\cdot\|$ represents the Euclidean norm. $\mathbb{R}^{m\times n}$ and $\mathbb{C}^{m\times n}$ represent the set of $m \times n$ real matrices, and the set of $m \times n$ complex matrices, respectively. The superscript $(\cdot)^{\mathrm{H}}$ the transpose operator, whereas $\mathrm{Re}\{\cdot\}$ and $\mathrm{Im}\{\cdot\}$ denote the real and the imaginary parts of a complex number. Upper and lower boldface symbols are used to denote matrices and column vectors, respectively.

II. System model

As depicted in Fig. 1, we consider a single-cell MU-MISO downlink system, where the BS is equipped with N_t transmit antennas serving K single-antenna users, with $K \leq N_\mathrm{t}$, and one multi-antenna Eve with M antennas. We assume a block fading channel $\mathbf{h}_k \in \mathbb{C}^{1\times N_\mathrm{t}}$ between the transmit BS antennas and the k-th user. The received coded signal by the k-th user at the symbol slot n can be expressed as

$$y_k[n] = \mathbf{h}_k \mathbf{x}_\mathrm{d}[n] + z_k[n], \tag{1}$$

where $\mathbf{x}_\mathrm{d}[n] \in \mathbb{C}^{N_\mathrm{t}\times 1}$ is the transmitted coded vector from the N_t transmit antennas, and $z_k[n] \in \mathbb{C}$ is the additive white Gaussian noise (AWGN) at the k-th user with variance σ_z^2.

The above model can be rewritten in a matrix form by collecting the received signal at all users in vector $\mathbf{y}[n] \in \mathbb{C}^{K\times 1}$ as

$$\mathbf{y}[n] = \mathbf{H}\mathbf{x}_\mathrm{d}[n] + \mathbf{z}[n], \tag{2}$$

where $\mathbf{H} = [\mathbf{h}_1^\mathrm{H} \dots \mathbf{h}_K^\mathrm{H}]^\mathrm{H} \in \mathbb{C}^{K\times N_\mathrm{t}}$ represents the system channel matrix and $\mathbf{z}[n] \in \mathbb{C}^{K\times 1}$ collects the independent AWGN components of all users.

Similarly, the received signal at Eve, $\mathbf{y}_\mathrm{e}[n] \in \mathbb{C}^{M\times 1}$, can be expressed as follows:

$$\mathbf{y}_{\mathrm{e}}[n] = \mathbf{H}_{\mathrm{e}}\mathbf{x}_{\mathrm{d}}[n] + \mathbf{z}_{\mathrm{e}}[n], \tag{3}$$

where $\mathbf{H}_{\mathrm{e}} = [\mathbf{h}_{\mathrm{e},1}^{\mathrm{H}} \dots \mathbf{h}_{\mathrm{e},M}^{\mathrm{H}}]^{\mathrm{H}} \in \mathbb{C}^{M \times N_{\mathrm{t}}}$ represents the system channel matrix between the BS and the multi-antenna Eve, and $\mathbf{z}_{\mathrm{e}}[n] \in \mathbb{C}^{M \times 1}$ assembles the independent AWGN components at the M antennas, with a variance of σ_{e}^2 each.

We note that the pilot symbols, also being referred to as reference signals, are an integral part of communication systems that are known entities to all parties. In particular, they are commonly used for channel-state information (CSI) and signal-to-interference-plus-noise ratio (SINR) estimation. Specifically, non-precoded pilot symbols are used for CSI estimation while precoded pilot signals are intended for SINR estimation [38]. In this work, we are interested in the latter case, precoded[1] pilot symbols, which uses the same modulation and coding scheme (MCS) used for precoding the data. In this context, we define N as the number of precoded pilot symbols used within a frame. We also note that these N pilot symbols are interleaved with data symbols in a frame that fits within the channel coherence time T. In this setting, we define the input data symbols intended for the K users as $\mathbf{d} \in \mathbb{R}^{K \times 1}$, with d_k being the symbol intended for user k.

In the case of block-level precoding, we define η as the mean power. For the SLP case, we define γ_k as the target SINR for the k-th user with $\boldsymbol{\gamma} = [\gamma_1 \dots \gamma_K] \in \mathbb{R}^{K \times 1}$ representing the target SINR for all users. For ease of notation, we drop the time index n in the remainder of the paper.

III. ML-based attacks

In this section, we will propose two ML eavesdropping attacks, where a multi-antenna Eve uses precoded pilot symbols as training data to accurately hard/soft decode the transmitted symbols. We start by presenting the motivation of our work along with the adversarial model. Next, we present the ML frameworks for the proposed soft and hard decoding schemes. We note that our proposed ML framework is valid in all cases where the transmitter sends also pilot symbols, which is actually the case for a standard downlink MU-MISO system, the one considered in this paper.

A. Motivation

To motivate our work, we study the received signal at Eve when the BS sends precoded pilot signals to the intended users. We investigate the case when the BS uses a conventional block-level precoder, i.e., ZF [22] as well as the case of a conventional SLP precoder, i.e., the constructive interference for sum power minimization (CISPM) approach in [39].

To that end, we first examine a special case scenario for illustration purposes. Afterwards, we present a more general scenario that represents a typical downlink MU-MISO system.

In the illustrative special case scenario, we consider the following toy example: an MU-MISO system with $N_{\mathrm{t}} = 15$, $K = 6$, $\sigma_z^2 = 1$, one channel realization, and quadrature phase-shift keying (QPSK) as a modulation scheme, where the BS sends to each user two precoded pilot signals of $N = 150$ symbols each. In this setting, a multi-antenna Eve attempts to eavesdrop a specific user k.

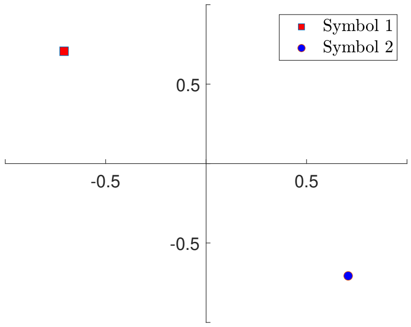


Fig. 2: Symbols used in the two pilot signals intended for user k.

To better understand the example visually, the BS sends the same symbols to user k while it sends pseudo-random sequences to the remaining users. The two symbols constructing the two pilot signals intended for user k are plotted in Fig. 2.

When the BS precodes the aforementioned pilot signals with ZF precoding of mean power of 5 dB, the noiseless received signals at user k and the Eve are respectively given as in Fig. 3(a) and Fig. 3(b), respectively. We note that the channel to the K users and Eve were generated randomly.

As depicted in Fig. 3(a), the received signal at user k shows no inter-user interference as it was cancelled by the ZF precoder. However, the received signal at Eve is spread due to the inter-user interference effect, as Eve's channel is different from user's k channel. Still, we can observe a precoding pattern that applies to both received signals, i.e., the red squares are mostly positioned on the top right of the blue circles.

A more inherently-secure precoding scheme, which does not depict patterns of the precoding used, is SLP precoding [39]. This particular SLP scheme is designed to exploit the multi-user interference for power gains. In other words, this scheme propels the intended users' received signals deeper into the correct detection region of the desired symbol for each intended user. The corresponding optimization problem is defined as

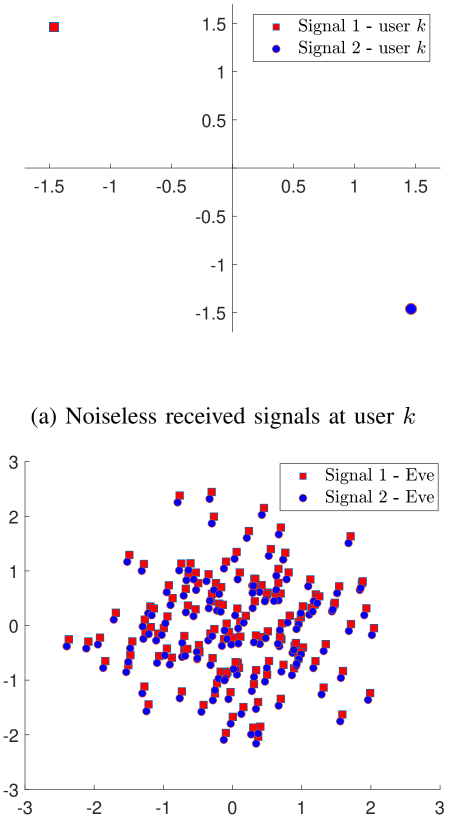
$$\begin{aligned} \mathbf{x}_{\mathrm{d}}(\mathbf{d}, \mathbf{H}, \boldsymbol{\gamma}) = & \arg\min_{\mathbf{x}} ||\mathbf{x}||^2 \\ & \text{subject to} \\ & \mathrm{Re}\{\mathbf{h}_k\mathbf{x}\} \trianglelefteq \sigma_z\sqrt{\gamma_k}\mathrm{Re}\{d_k\}, \ \forall k \\ & \mathrm{Im}\{\mathbf{h}_k\mathbf{x}\} \trianglelefteq \sigma_z\sqrt{\gamma_k}\mathrm{Im}\{d_k\}, \ \forall k, \end{aligned} \tag{4}$$

where the operator $\trianglelefteq$ guarantees that the real/imaginary parts of received signal lie in the same detection region as the data symbols d_k. In the case of QPSK constellation, for instance, when $d_k = 1 + 1j$, the operator $\trianglelefteq$ simplifies to $\geq$ for both constraints.

As shown in (4), the CISPM scheme minimizes the transmit power while guaranteeing a certain target SINR at the intended users through constructive interference (CI) constraints.

Thus, the CISPM precoding takes inputs: the channel to

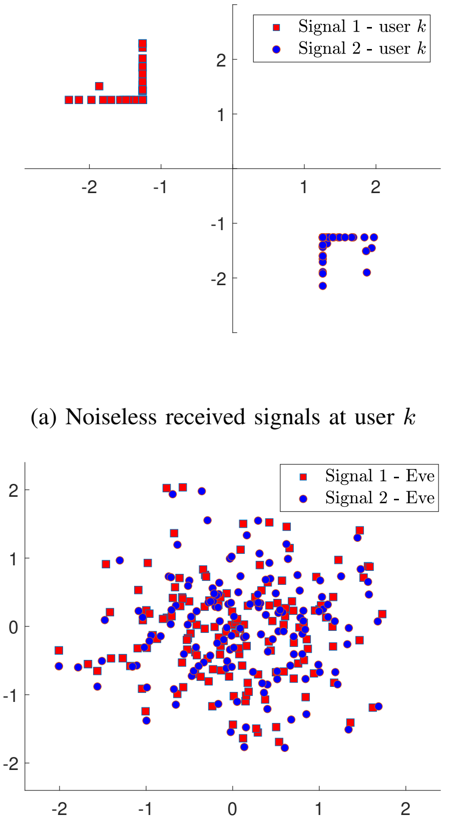
[1] We note that, we refer to precoded pilot symbols by the symbols that will be precoded before transmission [38].



(a) Noiseless received signals at user k

(b) Noiseless received signals at Eve

Fig. 3: Noiseless received signals at user k and Eve when the BS uses ZF precoding with a mean power of 5 dB.



(a) Noiseless received signals at user k

(b) Noiseless received signals at Eve

Fig. 4: Noiseless received signals at user k and Eve when the BS uses CISPM precoding.

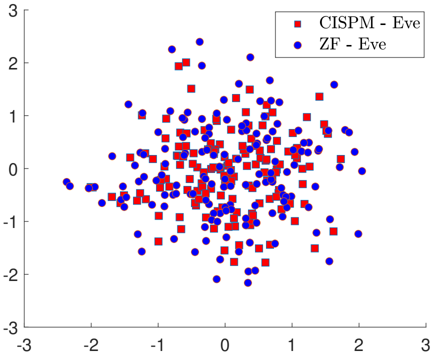


Fig. 5: Received signal at Eve when BS sends pseu-random sequences to every user.

the intended users, $\mathbf{H}$, the input data to be transmitted to the intended users, $\mathbf{d}$, the target SINR for all intended users, $\boldsymbol{\gamma}$, and the noise variance at the users σ_z^2. Herein, the transmitted waveform is designed so as to align the interference constructively at the receiver side, pushing the symbols deeper into the detection region in accordance with the CI constraints. The objective function's goal is to minimize the total transmit power while applying CI constraints to each user. The constraints' aim is to place the real/imaginary parts of the noiseless received signal at the kth user, $\mathbf{h}_k\mathbf{x}$, in the detection region of the real/imaginary parts of the kth corresponding data symbol. Specifically, using a minimum value of $\sigma_z\sqrt{\gamma_k}$ to guarantee a pre-defined target SINR value for each user.

Now we consider the aforementioned toy example of transmitted pilot signals illustrated in Fig. 2, but with the BS using CISPM precoding with a target SINR value of 5 dB for each user. The corresponding results of this example are illustrated in Fig. 4.

Fig. 4(a), represents the noiseless received signal at user k. As expected when using SLP precoding, the inter-user interference is transformed into power gains, resulting in deviations of the received signal deeper into the detection region while guaranteeing a specific target SINR value. The noiseless received signal at Eve when the aforementioned signals are transmitted is plotted in Fig. 4(b). As opposed to Fig. 3(b) where the blue circles are always below and to the left of the red boxes, in Fig. 4(b) there is no apparent fixed pattern.

This discrepancy is due to the randomness of the input data to transmit $\mathbf{d}$, which changes at each symbol slot resulting in $\mathbf{x}_{\mathrm{d}}$ to vary accordingly. Even though Eve is trying to eavesdrop user k whose received symbols do not change, what Eve receives provides no apparent insights about what was transmitted.

In a more general scenario representing a typical downlink

MU-MISO system, the BS is not constrained to send pilot signals where one user's pilots are constructed with the same symbol. In this case, the received signal will exhibit even more apparent randomness, as illustrated in Fig. 5, since the actual pilots are pseudo-random sequences for all users. Hence, since Eve does not know the CSI, using conventional detection techniques to directly decode the received signals will result in a poor performance.

Thus, in this work we propose to use ML to model the non-linear mappings underlying this apparent randomness, so that Eve can decode with an acceptable BER. Since the symbols used for the precoded pilots are known in communication standards to all parties, we propose to use ML to leverage this knowledge and decode the transmitted data to a particular user with decent accuracy. To that end, we propose ML-based soft and hard decoding schemes that can accurately decode the transmitted signal by using the precoded pilot symbols as training data.

B. Adversarial model

Contrary to the adversarial wiretap channel model proposed in [40] that considers active adversaries, herein, we consider a passive eavesdropper that can listen to the wireless medium with fading and noise effects.

Concerning Eve's environment, Eve is part of the downlink MU-MISO system that comprises of the sender, i.e., the BS, intended users, and Eve. Since Eve is a registered user of the MU-MISO system, the BS knows its CSI $\mathbf{H}_\mathrm{e}$ the same way it knows the CSI of the intended users $\mathbf{H}$. We highlight that Eve does not know $\mathbf{H}_\mathrm{e}$ nor $\mathbf{H}$. On the other hand, Eve knows the pilot symbols transmitted, the modulation scheme used, and the FEC parameters.

As for Eve's profile and capabilities, we consider Eve to have: 1) unlimited computation power, and 2) access to state-of-the-art machine-learning tools and algorithms. Contrary to the intended users who are single-antennas receivers, Eve is equipped with M antennas.

Next we present our proposed ML-based soft and hard decoding schemes. For a thorough explanation of our proposed ML-based decoding schemes, in the following, we use ZF precoding as an example. However, the proposed decoding frameworks are valid for any precoding technique used at the BS.

C. ML framework for the proposed soft decoding scheme

As illustrated in Fig. 6, the ML framework for soft-decoding encompasses two steps: 1) training phase, where the ML model is trained by using the precoded pilot symbols; 2) prediction phase, where probabilities are estimated and employed to calculate the LLRs which are consequently fed to a soft decoder.

1) ***Training phase:*** As pointed out earlier, the BS sends the pilot symbols $\mathbf{p} \in \mathbb{C}^{K\times 1}$ as training data, which are pseudo-random sequences for all users. For one SP, the overall received pilot signal at Eve's all antennas, $\mathbf{y}_\mathrm{e}^\mathrm{p} \in \mathbb{C}^{M\times 1}$, can be written as

$$\mathbf{y}_\mathrm{e}^\mathrm{p} = \mathbf{H}_\mathrm{e}\mathbf{x}_\mathrm{p} + \mathbf{z}_\mathrm{e}, \tag{5}$$

where $\mathbf{x}_\mathrm{p} \in \mathbb{C}^{N_\mathrm{t}\times 1}$ is the transmitted precoded pilot signal from the N_t BS's transmit antennas.

As depicted in Fig. 6, the transmitted signal $\mathbf{x}_\mathrm{p}$ depends on all the users' symbols. Thus, Eve could target any user individually by retraining the ML model according to the pilot sequences used for each user. As such, Eve would create a mapping between the received signal $\mathbf{y}_\mathrm{e}^\mathrm{p}$ and the pilot symbols p_s^k corresponding to the targeted user k. We note that the subscript s in p_s^k stands for "soft", where the pilot symbols are represented in bits, i.e., $p_\mathrm{s}^k \in \{$"00", "01", "11", "10"$\}$ in the case of QPSK modulation.

We note that, as the number of antennas at Eve, M, increases, the number of received signals at Eve increases accordingly, which often leads to better accuracy. In essence, each antenna at Eve receives a different distorted version of the same transmitted signal $\mathbf{x}_\mathrm{p}$; the more different copies of $\mathbf{x}_\mathrm{p}$ received by Eve, the better the performance.

Hence, the training set $\mathcal{D}_\mathrm{s}$ is the collection of $\{\mathbf{y}_\mathrm{e}^\mathrm{p}[n], p_\mathrm{s}^k[n]\}, n \in \{1,\ldots,N\}$, where $\mathbf{y}_\mathrm{e}^\mathrm{p}[n]$ represents the received pilot signal at Eve during the n-th SP, while $p_\mathrm{s}^k[n]$ is the corresponding pilot symbol of user k. Therefore, the training set $\mathcal{D}_\mathrm{s}$ can be written in a more compact form as

$$\mathcal{D}_\mathrm{s} = \{\mathbf{Y}_\mathrm{e}^\mathrm{p}, \mathbf{p}_\mathrm{s}^k\}, \tag{6}$$

where $\mathbf{Y}_\mathrm{e}^\mathrm{p} \in \mathbb{C}^{N\times M}$ are the received pilot symbols at Eve during N SPs and $\mathbf{p}_\mathrm{s}^k \in \mathbb{C}^{N\times 1}$ are the corresponding transmitted pilot symbols to the k-th user. Using ML terminology, $\mathbf{Y}_\mathrm{e}^\mathrm{p}$ represents the features[2] while $\mathbf{p}_\mathrm{s}^k$ represents the labels, where both constitute the training dataset. For non-binary modulation schemes, this ML problem is considered as a multi-label classification (MLC) problem [41], [42] as more than 1 bit is required to encode the symbols. Namely, MLC is a supervised learning problem where an observation, i.e, a scalar or a vector of features, is associated with multiple labels. Hence, as depicted in Fig. 6, the training dataset is fed to the MLC fitting module which will in turn output a trained ML model, that will subsequently be used in the prediction phase.

2) ***Prediction phase:*** As depicted in Fig. 6, in each SP, the BS sends the symbols $\mathbf{d} \in \mathbb{C}^{K\times 1}$ to the K users after precoding them using the same precoding scheme employed in the previous phase. The received signals at Eve in each SP, $\mathbf{y}_\mathrm{e}^\mathrm{d} \in \mathbb{C}^{M\times 1}$, can be written as

$$\mathbf{y}_\mathrm{e}^\mathrm{d} = \mathbf{H}_\mathrm{e}\mathbf{x}_\mathrm{d} + \mathbf{z}_\mathrm{e}, \tag{7}$$

where $\mathbf{x}_\mathrm{d} \in \mathbb{C}^{N_\mathrm{t}\times 1}$ represents the transmitted precoded data from the N_t transmit antennas, intended for all the users during one SP. If we assume that there are T symbols in one coherence time, $\mathbf{Y}_\mathrm{e}^\mathrm{d} \in \mathbb{C}^{(T-N)\times M}$ represents the collection of all received signals at Eve during one coherence time of the transmitted $(T-N)$ data symbols. In ML nomenclature, $\mathbf{Y}_\mathrm{e}^\mathrm{d}$ is commonly being referred to as the test/evaluation dataset.[2]

[2] We note that the input features in $\mathbf{Y}_\mathrm{e}^\mathrm{p}$ are complex-valued and cannot be directly processed by ML algorithms in general. Usually, this is addressed by considering real and imaginary parts separately.

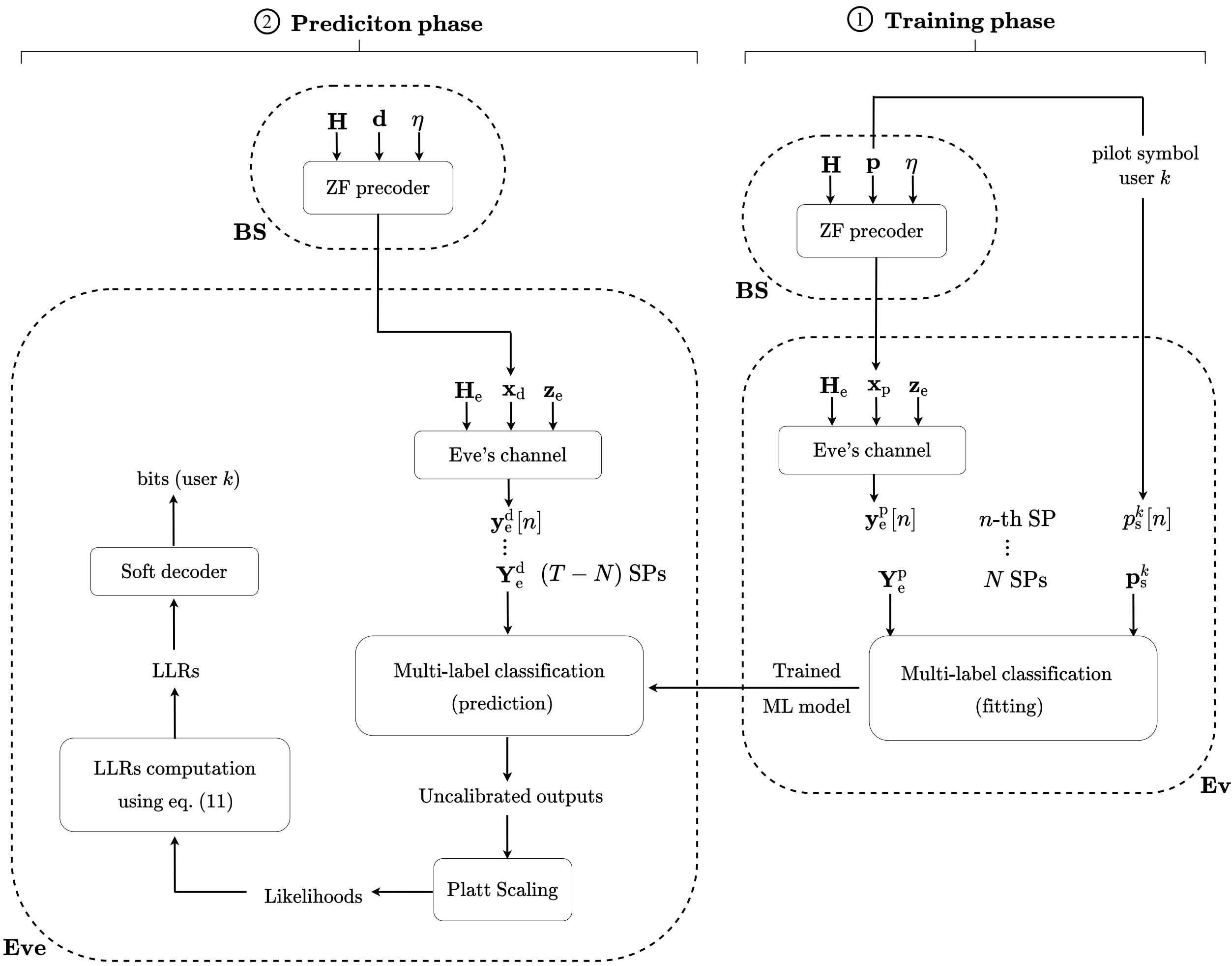


Fig. 6: Overview of the ML-based soft decoding scheme.

In principle, the goal of classification is to predict labels. In this context, however, we are not interested in the labels (hard outputs) but rather in the corresponding probabilities (soft outputs) to be used subsequently for LLR computation. Before tackling the computation of these probabilities, we first provide an overview of LLRs computation based on probabilities. We start by recalling some fundamental definitions in the context of LLR computation in binary detection [43].

Let U be a binary random variable (RV), acting as the correct hypothesis, with possible values $\{a_0, a_1\}$ and a priori probabilities p_0 and p_1. Let V be an RV with conditional probability density $f_{V|U}(v|a_m)$ that is finite and non-zero for all $v \in \mathbb{R}$ and $m \in \{0,1\}$. In our context, V models the received signal at Eve at a fixed time instant. We note that the conditional densities $f_{V|U}(v|a_m), m \in \{0,1\}$, are called *likelihoods*. The marginal density of V is given by $f_V(v) = p_0 f_{V|U}(v|a_0) + p_1 f_{V|U}(v|a_1)$. Hence, the *a posteriori* probability of U can be expressed as

$$f_{U|V}(a_m|v) = \frac{p_m f_{V|U}(v|a_m)}{f_V(v)}, \tag{8}$$

where $m \in \{0,1\}$. To maximize the probability of correct detection, the maximum a posteriori (MAP) rule can be written as

$$\frac{p_0 f_{V|U}(v|a_0)}{f_V(v)} \underset{\tilde{U}=a_1}{\overset{\tilde{U}=a_0}{\gtrless}} \frac{p_1 f_{V|U}(v|a_1)}{f_V(v)}, \tag{9}$$

where $\tilde{U}$ denotes the decision on the RV U. Rearranging (9) and canceling $f_V(v)$, we obtain the *likelihood ratio*

$$\Lambda(v) = \frac{f_{V|U}(v|a_0)}{f_{V|U}(v|a_1)} \underset{\tilde{U}=a_1}{\overset{\tilde{U}=a_0}{\gtrless}} \frac{p_1}{p_0}, \tag{10}$$

where the quantity $\frac{p_1}{p_0}$ is called the *threshold* and depends only on the a priori probabilities. Hence, the log-likelihood ratio $\mathrm{LLR}(v)$ can be expressed as follows:

$$\mathrm{LLR}(v) = \ln\left[\frac{f_{V|U}(v|a_0)}{f_{V|U}(v|a_1)}\right]. \tag{11}$$

As depicted in Fig. 6, to obtain the likelihoods in eq. (11), we feed the test dataset and the trained ML model to the MLC prediction module. A common and efficient implementation of predicting these probabilities is the Platt scalling approach in [44]. This method is used to transform the uncalibrated outputs of the classification module into probabilities. Platt scaling works by fitting a logistic regression model to the classifier's scores. The probabilities $f_{V|U}(v|a_m)$ according to the Platt scaling algorithm can be computed as

$$f_{V|U}(v|a_m) = \frac{1}{1+\exp(Af_v(a_m)+B)}, \tag{12}$$

where $f_v(a_m)$ is the classifier score and scalars A and B are the sigmoid parameters [44] learned by the algorithm, which are calculated using a cross-entropy loss function and an internal threefold cross-validation to prevent overfitting.

Once the likelihoods $f_{V|U}(v|a_m)$ are obtained, the LLRs can be computed using eq. (11), after which Eve can simply feed the computed LLRs to the soft decoder to obtain the transmitted message to user k.

D. ML framework for the proposed hard decoding scheme

The proposed ML-based hard decoding scheme also comprises of two phases: 1) training phase, where the ML model is trained by using the precoded pilot symbols; 2) prediction phase, where the module directly predicts the transmitted symbols to a particular user, which are in turn mapped into bits to finally be fed to a hard decoder to obtain the transmitted bits to user k.

*1) **Training phase**:* As depicted in Fig. 7, for each SP, the BS first sends pilot symbols $\mathbf{p} \in \mathbb{C}^{K\times 1}$ to the K users, which after precoding become the signal $\mathbf{x}_\mathrm{p} \in \mathbb{C}^{N_\mathrm{t}\times 1}$. Eve receives $\mathbf{y}_\mathrm{e}^\mathrm{p}[n] \in \mathbb{C}^{M\times 1}$ from all its antennas at the n-th SP, as in eq. (5).

For Eve to eavesdrop user k, it creates a mapping between the received signal $\mathbf{y}_\mathrm{e}^\mathrm{p}$ and the pilot symbols p_h^k corresponding to the targeted user k. We note that the subscript h in p_h^k stands for “hard”, which defines the decimal representation of the pilot symbols, for instance, $p_\mathrm{h}^k \in \{0, 1, 2, 3\}$ in the case of QPSK modulation.

Thus, the training set $\mathcal{D}_\mathrm{h}$ is the collection of $\{\mathbf{y}_\mathrm{e}^\mathrm{p}[n], p_\mathrm{h}^k[n]\}, n \in \{1, \ldots, N\}$, where $p_\mathrm{h}^k[n]$ is the pilot symbol of user k corresponding to the received pilot signal $\mathbf{y}_\mathrm{e}^\mathrm{p}[n]$ at the n-th SP. Thus,

$$\mathcal{D}_\mathrm{h} = \{\mathbf{Y}_\mathrm{e}^\mathrm{p}, \mathbf{p}_\mathrm{h}^k\}, \tag{13}$$

where $\mathbf{Y}_\mathrm{e}^\mathrm{p} \in \mathbb{C}^{N\times M}$ are the received pilot signals at Eve and $\mathbf{p}_\mathrm{h}^k \in \mathbb{C}^{N\times 1}$ are the transmitted pilot symbols, represented in decimals, to the k-th user, both during N SPs.

For non-binary modulation schemes, this problem is a single-label multi-class classification (MCC) problem. Namely, MCC is a supervised learning problem where an observation, i.e, a scalar or a vector of features, is associated with a single-label with multiple classes. Considering a modulation order M_o, the label space is $\{0, 1, \ldots, M_\mathrm{o} - 1\}$ with M_o total classes. Thus, as depicted in Fig. 7, the training dataset $\mathcal{D}_\mathrm{h}$ is fed to the MCC fitting module that in sequence outputs a trained ML model, which will be used thereafter in the prediction phase.

*2) **Prediction phase**:* As depicted in Fig. 7, the BS transmits $\mathbf{d} \in \mathbb{C}^{K\times 1}$ data symbols to the K users in each SP in the form of the precoded signal $\mathbf{x}_\mathrm{d} \in \mathbb{C}^{N_\mathrm{t}\times 1}$. We note that the precoding at BS herein uses the same precoding scheme employed in the training phase. The corresponding received signals at Eve is $\mathbf{y}_\mathrm{e}^\mathrm{d} \in \mathbb{C}^{M\times 1}$, as detailed in eq. (7).

Considering a coherence time of T symbols, there are $(T - N)$ symbols dedicated to data transmission. Thus $\mathbf{Y}_\mathrm{e}^\mathrm{d} \in \mathbb{C}^{(T-N)\times M}$ represents the collection of all received data signals at Eve during one coherence time, which constitutes the test/evaluation dataset.

Contrary to the proposed soft decoding scheme, herein we are interested in predicting the labels, i.e., hard outputs. As depicted in Fig. 7, to obtain the labels, we feed the test dataset and the trained ML model to the MCC prediction module. We note that the labels are in the form of decimals, i.e., the same nature of the labels used in the training phase. Once the labels are predicted, they will be first mapped into bits and then fed to the hard decoder for decoding to finally obtain the bits transmitted to user k.

We note that the proposed soft and hard decoding schemes are also valid for other constellations, including higher-order quadrature amplitude modulation (QAM). For instance, in 16-QAM, 4 bits are needed to represent the symbols as opposed to 2 in the QPSK case. Consequently, for the soft scheme in Fig. 6, the pilot symbols of user k will contain 4 bits instead and the prediction module will generate 4 uncalibrated outputs as a result. However, for the hard scheme in Fig. 7, the pilot symbols of user k will be represented using 16 classes, and therefore the prediction module will output a label in the set $\{0, 1, \ldots, 15\}$. Therefore, the proposed soft and hard decoding frameworks are valid for any constellation, where the modulation order determines the number of bits used in pilot/data symbols and also defines the number of labels/classes employed, all the rest of the processing remain unchanged.

IV. Countermeasure: Physical-layer Security

In this section, we propose novel security-enhanced SLP schemes that yield high BER at Eve. Similar to [45] and [33], the idea is to design the transmitted signal $\mathbf{x}_\mathrm{d}$ to have constructive interference at the intended users, while at the same time, increasing the BER at Eve. We note that the CSI to Eve is available at the BS.[3] This assumption is reasonable when Eve is a legitimate user attempting to eavesdrop other users. It gives Eve the advantage to access the control signaling of the BS and obtain the modulation and coding parameters used, which further improves its detection performance.

A. PLS random scheme

We design this scheme to have constructive interference at the intended users and destructive interference at Eve. To that end, we align the transmitted signal to the corresponding detection regions of the intended users using their CSI while we force Eve’s received signal to lie at the boundaries of the detection regions using Eve’s CSI.

In order to illustrate the idea, consider the QPSK constellation in Fig. 8. The aim here is to propel the received signals

[3] We follow the same methodology used in the relevant PLS work in [34]–[37], which assumed the knowledge of Eve’s CSI at the transmitter. However, we intend to extend our work to a more general eavesdropper, by considering no Eve’s CSI at the BS [46].

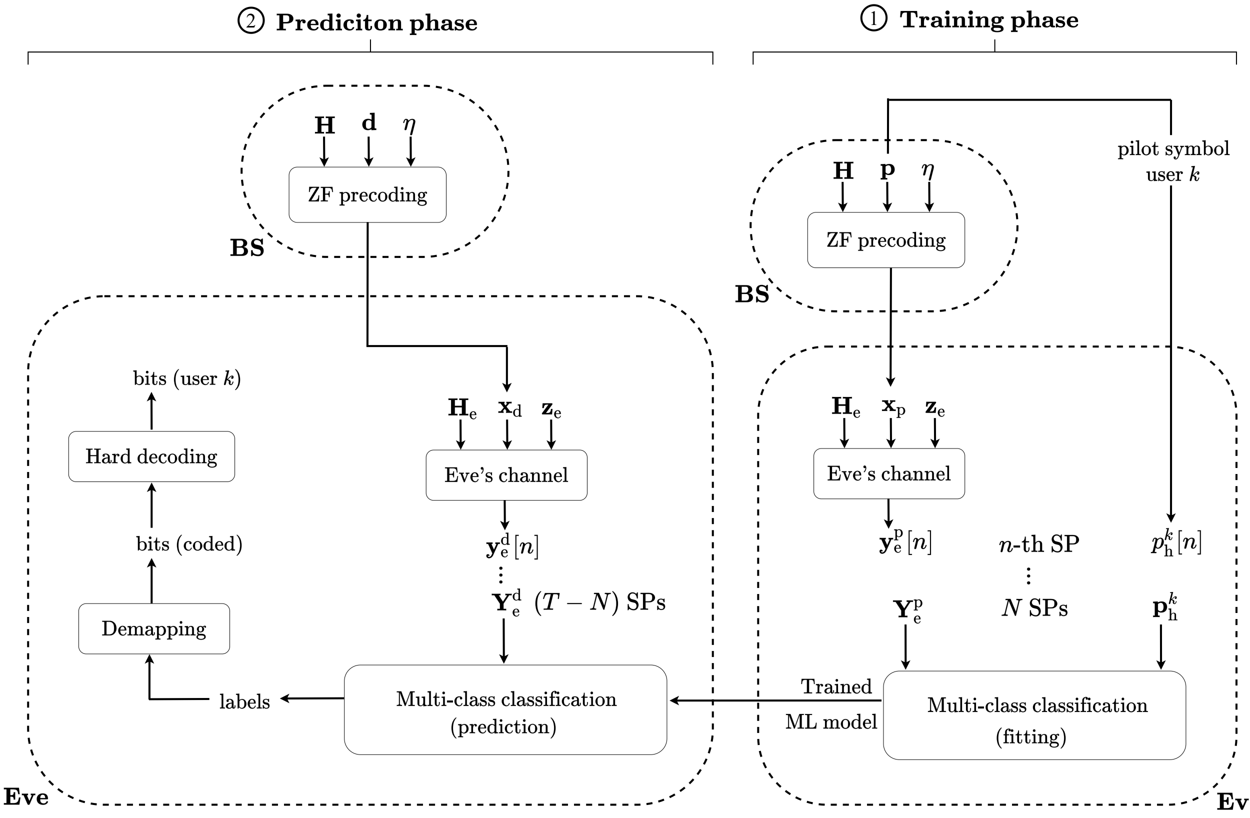


Fig. 7: Overview of the ML-based hard decoding scheme.

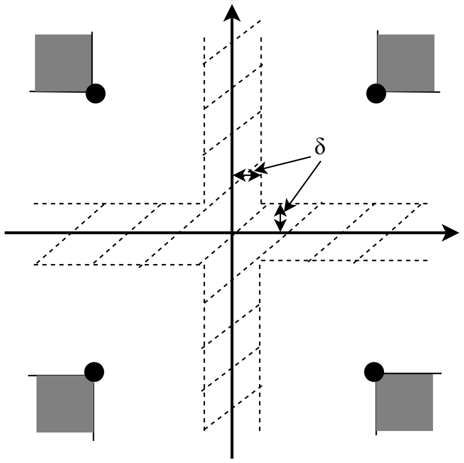


Fig. 8: Intended user's and Eve's received signals in the case of PLS random scheme.

deeper into the detection regions, which are illustrated by the gray squares (actually, those regions are unbounded).

On the other hand, we design Eve's received signal to lie in the strapped region, which is centered at the boundary of the detection regions. The strapped region's width is governed by the parameter δ. The smaller the δ, the tighter the strapped region, leading to higher probability of landing into the opposite region when noise adds up, resulting in higher BER at Eve.

Inspired by the boundary scheme presented in [33, §IV.B eq. (11)], we propose to embed randomness in Eve's received signal by randomly selecting the boundary region, either horizontal or vertical, as depicted in Fig. 8. We decompose the non-convex strapped region in Fig. 8 into two convex regions: the vertical part and the horizontal one. And at each SP and for each antenna at Eve, we *randomly* choose between the two regions, so that on average, Eve's received signals would lie evenly on both regions, assuming the symbol distribution is equiprobable. We refer to this scheme as "PLS random scheme".

The optimization problem for this scheme can be formulated as

$$\mathbf{x}_{\mathrm{d}}(\mathbf{d},\mathbf{H},\mathbf{h}_{\mathrm{e}},\boldsymbol{\gamma},\delta,\mathbf{b})=\arg\min_{\mathbf{x}}\|\mathbf{x}\|^2 \tag{14}$$

subject to

$$\mathrm{Re}\{\mathbf{h}_k\mathbf{x}\} \trianglelefteq \sigma_z\sqrt{\gamma_k}\mathrm{Re}\{d_k\},\ \forall k \tag{15}$$

$$\mathrm{Im}\{\mathbf{h}_k\mathbf{x}\} \trianglelefteq \sigma_z\sqrt{\gamma_k}\mathrm{Im}\{d_k\},\ \forall k \tag{16}$$

$$b_i\mathrm{Re}\{y_{\mathrm{e}}^i\}+(1-b_i)\mathrm{Im}\{y_{\mathrm{e}}^i\}\lesseqgtr\delta, \forall i \tag{17}$$

where $\mathbf{h}_k\mathbf{x}$ is the k-th user's noiseless received signal, $y_{\mathrm{e}}^i = \mathbf{h}_{\mathrm{e}}^i\mathbf{x}$ is the noiseless received signal at Eve's i-th antenna, $b_i \in \{0,1\}$ is the realization of a binary RV that represents the boundary region to use for Eve's i-th antenna, $\mathbf{b}$ is the vector collecting the b_i realizations, which select the corresponding strapped sub-region in Fig. 8 — either vertical ($b_i = 1$) or horizontal ($b_i = 0$) —, of the M antennas at Eve, and $\delta > 0$ is the distance parameter controlling the width of the boundary region. This problem is convex and can be solved efficiently using standard optimization toolboxes such as CVX [47]. Algorithm 1 details the process of signal design of the

PLS random scheme, which is executed for every symbol slot.

Algorithm 1 PLS random scheme

```
Input: $\mathbf{d}, \mathbf{H}, \mathbf{H}_{\mathrm{e}}, \boldsymbol{\gamma}, \sigma_z^2, \delta, \mathbf{b}$;
Do: solve problem (14) as follows:
    Satisfy CI constraints in (15) and (16)
    for Each antenna $i$ at Eve do
        if $b_i = 1$ then
            Push $y_{\mathrm{e}}^i$ to the vertical boundary region
        else
            Push $y_{\mathrm{e}}^i$ to the horizontal boundary region
Output: $\mathbf{x}_{\mathrm{d}}$
```

As demonstrated in Algorithm 1, the PLS random scheme designs Eve's received signal to have no pattern as to which boundary region it will fall into, thus it will be extremely difficult for a ML-based engine to find relationships between the known pilot symbols and Eve's received signals.

The advantages of this scheme are: 1) enhance PLS as the detection decisions at the Eve will be mostly made on the basis of noise, and 2) save the transmit power since this scheme involves only a small deviations of the targeted received constellation points at Eve.

B. PLS Eve-min-power scheme

Targeting a computationally simpler scheme, herein we take the basic SLP scheme for constructive interference at the intended users, the CISPM, and change the cost function to achieve PLS. Specifically, we do not include any PLS related constraints. To attain security with the CISPM scheme, in addition to minimizing the transmit power, we also minimize the power of Eve's noiseless received signal simultaneously, hence the name "PLS Eve-min-power".

Compared to the PLS random scheme that has the strict constraint of forcing Eve's received signal to lie in the boundary region, in the PLS Eve-min-power, we allow Eve's signal to lie anywhere in the plane but as close to zero as possible, whatever the degrees of freedom at the transmitter allow. This scheme can be formulated as follows:

$$\mathbf{x}_{\mathrm{d}}(\mathbf{d}, \mathbf{H}, \mathbf{H}_{\mathrm{e}}, \boldsymbol{\gamma}) = \arg\min_{\mathbf{x}_{\mathrm{d}}} ||\mathbf{x}_{\mathrm{d}}|| + ||\mathbf{H}_{\mathrm{e}}\mathbf{x}_{\mathrm{d}}|| \tag{18}$$

$$\text{subject to}$$

$$\mathrm{Re}\{\mathbf{h}_k\mathbf{x}_{\mathrm{d}}\} \trianglelefteq \sigma_z\sqrt{\gamma_k}\mathrm{Re}\{d_k\},\ \forall k \tag{19}$$

$$\mathrm{Im}\{\mathbf{h}_k\mathbf{x}_{\mathrm{d}}\} \trianglelefteq \sigma_z\sqrt{\gamma_k}\mathrm{Im}\{d_k\},\ \forall k. \tag{20}$$

As shown in (18), the PLS Eve-min-power scheme minimizes the sum of the transmit power and the noiseless received power at Eve, while guaranteeing a certain target SINR at the intended users through constructive interference constraints (19) and (20). Similarly, this problem is convex and can be solved efficiently using standard optimization toolboxes.

We note that this PLS scheme leads to higher security than the CISPM, as it makes it considerably harder for an ML-enabled Eve to correctly detect the low-power signal induced by minimizing the power at Eve.

We note that, low-complexity and computationally efficient SLP design was developed for practical and real-time implementations [48], [49]. For instance, an FPGA-accelerated design of computationally efficient SLP for high-throughput communication systems was proposed in [48], which enables real-time operation and provides a high symbol throughput for multiple receive terminals. In [49], a low-complexity FPGA design for SLP was proposed for MU-MISO downlink communication systems, by developing an approximate yet computationally-efficient closed-form solution to alleviate the excessive complexity incurred by the SLP design.

To validate the proposed schemes, we have conducted numerical simulations according to the same methodology as [46]. Future extensions of our work include adapting and optimizing the SLP technique for real-time validation similar to [48], [49]. To that end, since the formulations of the proposed and benchmark SLP precoding schemes are convex, in the numerical results we use the CVX modeling framework to solve the SLP precoders' underlying optimization problems. CVX's employed solvers rely on primal-dual interior point methods to solve the problems. However, the time complexity analysis of the SLP precoders employed in this paper depends heavily on the solver used and its implementation, which makes it challenging to obtain a closed-form big $\mathcal{O}$ representation of it. Nevertheless, we resort to *runtime* [50] analysis of the implementations, where we measure the total time it takes for the algorithm to solve the optimization problem (in milliseconds). We present the runtime analysis of the proposed and benchmark schemes in the following section.

V. Numerical results

To make this section more comprehensive, we split it into three parts: 1) Parameters, metrics, and benchmarks where we defined the simulations' setting, 2) selection of ML algorithms for Eve attack in which we experiment with several algorithms and select the most performing, and 3) comparisons and insights to assess the performance of our proposed schemes in terms of security, power consumption, and runtime.

A. Parameters, metrics, and benchmarks

As a benchmark to the proposed SLP-based PLS schemes, we employed the CISPM [39] and ZF precoding [22] schemes. We note that in the following simulations, for a fair comparison, we set $\eta = \gamma_k$ such that all the examined schemes have the same transmit power.

Regarding the metrics used to evaluate the different schemes, we use the BER at Eve to assess the security offered by a particular decoding scheme for a given precoding design. The lower the BER at Eve, the lower the security and vice versa. In a similar way, we also evaluate the frame-error rate (FER) at Eve since we have channel coding in the system, which is defined as the ratio of frames in error (one altered bit suffices to make the entire frame erroneous) to the total number of frames received. We also evaluate the BER/FER at the intended user to examine the impact of using the PLS schemes on the intended user's performance. Finally, we define the total transmit power by the BS antennas as $P_{\mathrm{tot}} = \|\mathbf{x}_{\mathrm{d}}\|^2$.

Parameters	Values
Code rates	⅓, ¼
Constraint length	7
Frame Size	150
Number of frames	100
Trace-back length	96
Decoder decision technique	Hard, Soft

TABLE I: Channel coding parameters used for the simulations

In the simulations, we take the average of the above quantity over a large number of symbol slots to obtain the frame-level total transmit power, which is then averaged over a large number of channel realizations.

In the following simulations, we use QPSK modulation. For the PLS random scheme, we set $\delta = \sigma_z^2/10$ to make sure that the noise will push Eve's received signal outside the boundary region, i.e., to cause higher error rates at Eve. For simplicity, we consider unitary noise variance σ_z^2. As for the channel coding part, we use convolutional coding [51] and Viterbi decoding [52] with the parameters in Table I. We note that low coding rates are chosen in order to consider a worst case eavesdropping scenario, where Eve can take advantage of the redundancy to correct as much errors as possible.

B. Selection of ML algorithms for the Eve attack

For the MLC modules used for the ML-based soft decoding scheme, in this simulation, we adopt problem transformation methods that remodel our MLC problem into single-label problem(s). Since our labels are bits, the MLC problem will be decomposed into k binary classifiers, where $k = \log_2 M_o$ is the number of bits constructing each symbol.

Herein, we use two transformation methods, binary relevance (BR) [41] and classifier chain (CC) [42]. BR is the most simple and efficient method to solve MLC problems, which trains the k binary classifiers independently; its only drawback is that it does not consider labels correlation. CC, however, takes into account the correlation between labels by using the outputs of the previously trained classifiers as features for the subsequent ones in the chain, except for the first classifier. We refer to these soft-decoding implementation by "Soft - BR" and "Soft - CC" accordingly.

Concerning the MCC module used for the ML-based hard decoding scheme, it does not require any transformation or specific approach. It can be solved using any classifier. We refer to this scheme subsequently by "Hard". It is worth mentioning that the ML-based decoding schemes apply only to Eve, whereas the intended users employ conventional (not ML-based) soft and hard decoding techniques.

To make Eve as sophisticated as possible, we experiment with several state-of-the-art classifiers and choose the one with the best performance. In Table II, we compare the prediction accuracy of the proposed soft[4] and hard decoding schemes, considering ZF and CISPM precoding as well as the proposed PLS precoding schemes. The parameters used for this simulation are: $N_\mathrm{t} = 15$, $K = 6$, $M = 9$, and $\eta = \gamma_k = 6$ dB. We note that these results represent the averaged results over 100 different channel realizations. We also note that this accuracy applies before channel decoding, i.e., by comparing the ML predicted labels to the actual coded transmitted symbols to user k.

As observed in Table II, the logistic regression classifier achieves the highest prediction accuracy among all the precoding and decoding schemes. Therefore, in the following simulations, we use this classifier in our proposed ML-based decoding schemes.

C. Comparison and insights

We note that a BER value of 0.5 indicates full confusion. Regarding the target FER values at the intended users, it varies depending on the application scenario. For instance, enhanced mobile broadband (eMBB) in 5G requires an FER on the order of 10^{-3} while massive machine-type communications (mMTC) require only 10^{-1} [53]. In this section, we will validate the eavesdropping attacks by showing the FER at Eve to be in the order of the intended users' FER values.

Fig. 9 depicts the coded BER at Eve as a function of its number of antennas M. We compare the proposed hard and soft decoding schemes. The parameters used in the simulation are: $r = 1/3$, $N_\mathrm{t} = 15$, $K = 6$, and $\eta = \gamma_k = 6$ dB. Fig. 9(a) represents the non-secure precoding schemes, ZF and CISPM. For our hard and soft decoding schemes, we observe that the more antennas at Eve, the lower is the BER, i.e., the more antennas at Eve, the higher the prediction accuracy (more versions of the same signal, hence more features used for training and prediction), leading to lower BER. In addition, our Soft technique outperforms the Hard one, where Soft - BR and Soft - CC are equivalent. Moreover, with 9 antennas at Eve, the BER at Eve is so low to the point that it could be compared to an intended user's decoding performance, leading to a big vulnerability in systems that use ZF and CISPM precoding. In addition, as expected, CISPM is more secure than ZF as predicted in Sec. III. As for the case of the PLS random scheme in Fig. 9(b), we observe the same pattern as in Fig. 9(a), the more antennas at Eve, the lower is the BER, with Soft decoding outperforming the Hard one. However, when M values are lower or equal to 9, the BER at Eve is at 0.5, indicating total equivocation. In fact, even for higher values than 9, the BER at Eve is still very high compared to ZF and CISPM schemes, i.e., PLS random scheme is offering a significant security gain when compared to the latter ones. Similarly, for the PLS Eve-min-power scheme in Fig. 9(c), we observe the same behavior as for PLS random scheme, with the PLS Eve-min-power scheme BER going lower than PLS random, i.e., PLS Eve-min-power is less secure than PLS random. However, when compared to non-secure precoding schemes, ZF and CISPM, PLS Eve-min-power still offers a drastic security gain.

Fig. 10(a) depicts the distribution of the estimated LLRs for Soft - CC decoding scheme. We note that for this particular plot, we used 1000 symbols to obtain a smooth histogram. We

[4] In the table, we did not show results for Soft - BR to avoid redundancy, as its results were almost the same as Soft - CC.

Classifiers	ZF		CISPM		PLS random		PLS Eve-min-power	
	Soft - CC	Hard	Soft - CC	Hard	Soft - CC	Hard	Soft - CC	Hard
Gaussian_NB	0.8338	0.8378	0.8271	0.8298	0.5431	0.5429	0.5708	0.5712
Log_Reg	0.9375	0.9374	0.8935	0.8929	0.5427	0.5433	0.5732	0.5732
SVM	0.9370	0.9361	0.8925	0.8931	0.5429	0.5426	0.5697	0.5718
R_Forest	0.8831	0.8798	0.8538	0.8491	0.5382	0.5354	0.5669	0.5650
KNN	0.9047	0.8994	0.8623	0.8570	0.5265	0.5245	0.5474	0.5454
Decision_Tree	0.8101	0.7951	0.7738	0.7571	0.5178	0.5207	0.5372	0.5374
Extra_Trees	0.9017	0.8970	0.8669	0.8644	0.5387	0.5377	0.5670	0.5679
LightGBM	0.8998	0.8958	0.8655	0.8611	0.5359	0.5356	0.5645	0.5629
XGB	0.8983	0.8946	0.8633	0.8609	0.5326	0.5349	0.5598	0.5605

TABLE II: Prediction accuracy of our proposed ML-based decoding schemes with several classifiers when using ZF, CIPSM, PLS random, and PLS Eve-min-power precoding at the BS.

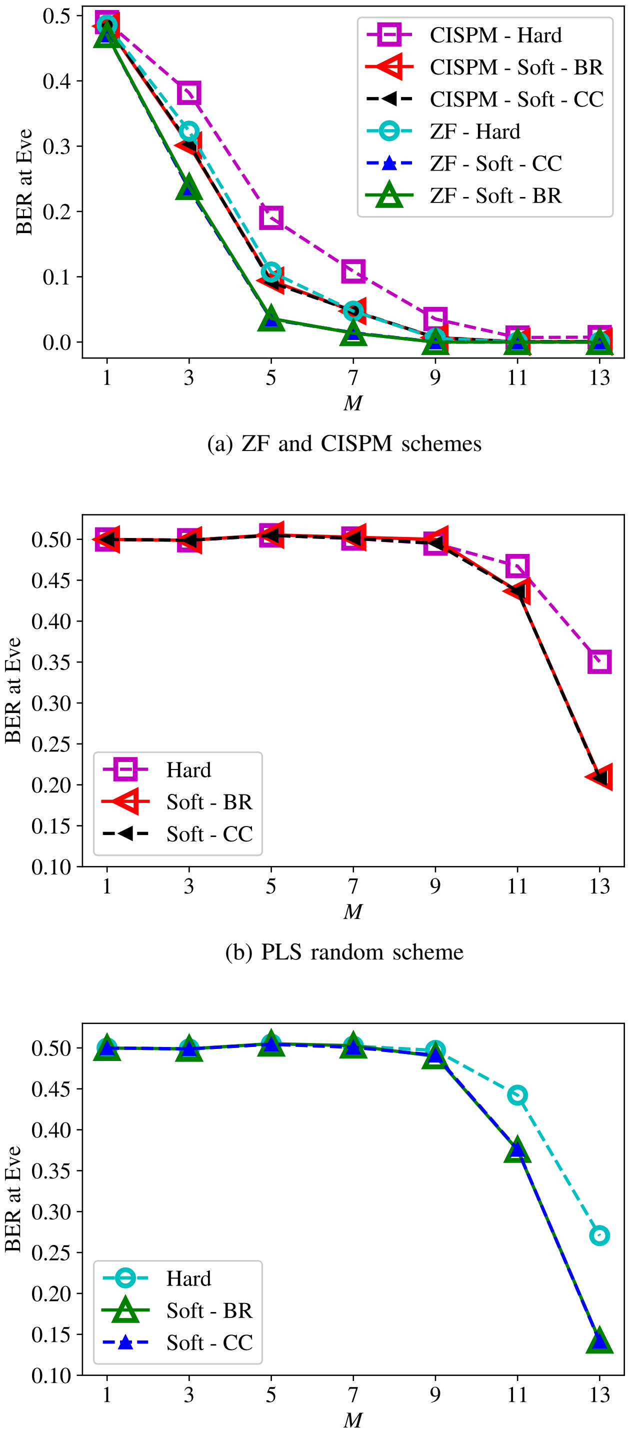
recall that a probability of 0.5 indicates that the predictor is not sure whether the predicted bit should be 0 or 1; a value close to 1 means the predictor is very sure that it is a 1, whereas a probability close to 0 indicates the opposite, i.e., it is very sure that it is not a 1. As expected, the LLRs values for the case of 9 antennas at Eve are distributed mostly away from 0, indicating high quality LLRs. Namely, the corresponding probabilities are mostly different than 0.5, thus yielding a high prediction accuracy. Using a higher number of antennas entails more features that can be employed in both training and prediction phases, therefore leading to higher accuracy when estimating the likelihoods. However, when Eve uses only 1 receive antenna, the LLRs are close to 0 as their probabilities are close to 0.5, implying poor quality LLRs. Therefore, we conclude that higher number of antennas at Eve leads to higher prediction accuracy, and therefore lower BER.

Fig. 11 depicts the coded BER at Eve as a function of η/γ_k [dB], which we set to the same value for all users for simplicity. The parameters used in the simulation setup are: $r = 1/3$, $N_{\rm t} = 15$, $K = 6$, and $M = 11$. Concerning ZF and CISPM schemes in Fig. 11(a), with the proposed soft and hard decoding approaches we notice that the higher the values of η/γ_k, the lower the BER. Particularly, higher η/γ_k values leads to higher transmit power, which cause higher received power at Eve, thus better decoding performance. Moreover, Soft decoding is outperforming the Hard one. Additionally, CISPM precoding is more secure than ZF, i.e. BER at Eve for CISPM is higher than the one of ZF. As for the use of the PLS random scheme, in Fig. 11(b), we notice that, similarly, the higher the values of η/γ_k, the lower the BER. We also observe that soft decoding is the most performing with the difference being that using PLS random scheme offers much higher security compared to ZF and CISPM scheme, with high BER values at Eve even when using 11 antennas at Eve. Concerning the PLS Eve-min-power scheme in Fig. 11(c), it depicts the same behavior as PLS random. However, the latter scheme is more secure because of its incurred randomness in the precoding design, while PLS Eve-min-power scheme is designed with Eve's channel in the objective function that lowers the received power at Eve.

Fig. 12 depicts the coded FER at Eve as a function of η/γ_k [dB]. The parameters used in the simulation are: $r = 1/4$, $N_{\rm t} = 15$, $K = 6$, and $M = 11$. In Fig. 12(a), for ZF and CISPM precoding, we notice that the higher the values of η/γ_k, the lower the FER, which is due to the increase of the transmit power. Particularly, soft decoding outperforms hard decoding, with FER values decently low, which validates the eavesdropping attack for ZF and CISPM precoding schemes, with CISPM being more secure. In Fig. 12(b) however, when we use the PLS random scheme, we notice that the higher the values of η/γ_k, the lower the FER. Particularly, the high FER values validate the security of the PLS random scheme. Lastly, when using the PLS Eve-min-power scheme, in Fig. 12(c), we observe the same behavior as in the case of the PLS random scheme, with FER values at Eve lower than ones for the PLS random approach. This validates the high security exhibited by the PLS random scheme, which outperforms the PLS Eve-min-power scheme's security performance. Yet, the FER values for the PLS Eve-min-power are still very high compared to the non-secure schemes, i.e., ZF and CISPM schemes.

Next, we investigate the FER at user k as a function of η/γ_k [dB] by comparing ZF and CISPM schemes with the PLS schemes. The parameters used in the simulation setup are: $r = 1/3$, $N_{\rm t} = 15$, $K = 6$, and $M = 11$. We found out that the values of the FER at user k are all zeros for all of the schemes even when $M = 11$, which was the reason to omit the plot in the manuscript. With such a low code rate, we do not obtain a single error for the entire range of $\eta/\gamma_k \in \{0, 1, 2, 3\}$. This happens in both schemes since we align the transmitted signal to the intended users' channels, which in turn will receive their intended symbols in the corresponding detection regions. Thus, the proposed PLS schemes provide much higher security without impacting the intended user's performance.

Fig. 13 shows the total transmit power $P_{\rm tot}$, in dBW, as a function of η/γ_k, which we set to the same value for all users for simplicity. We compare ZF and CISPM schemes with the PLS ones. The parameters used in the simulation are: $N_{\rm t} = 15$, $K = 6$, and $M = \{1, 13\}$. As explained above, the higher the η/γ_k values, the higher is the transmit power, for all the schemes. For the CISPM scheme, we observe that $P_{\rm tot}$ is lower than the target SINR at the intended users, which is due to the constructive interference turning into power gains at the receivers, hence less transmit power is required to attain the desired SINR value. However for ZF precoding, as predicted,



(a) ZF and CISPM schemes

(b) PLS random scheme

(c) PLS Eve-min-power scheme

Fig. 9: BER at Eve vs. number of antennas at Eve, with $r = {}^1\!/_3$, $N_{\rm t} = 15$, $K = 6$, and $\eta = \gamma_k = 6$ dB.

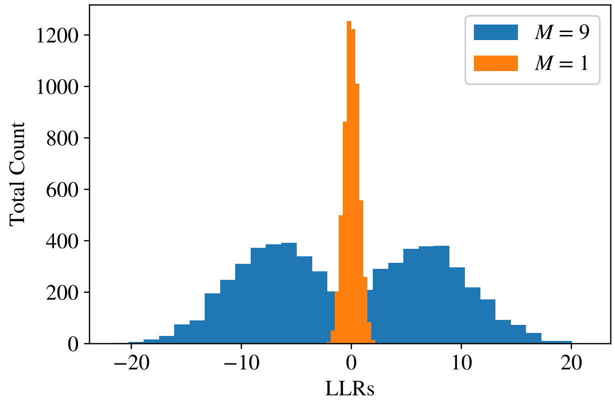


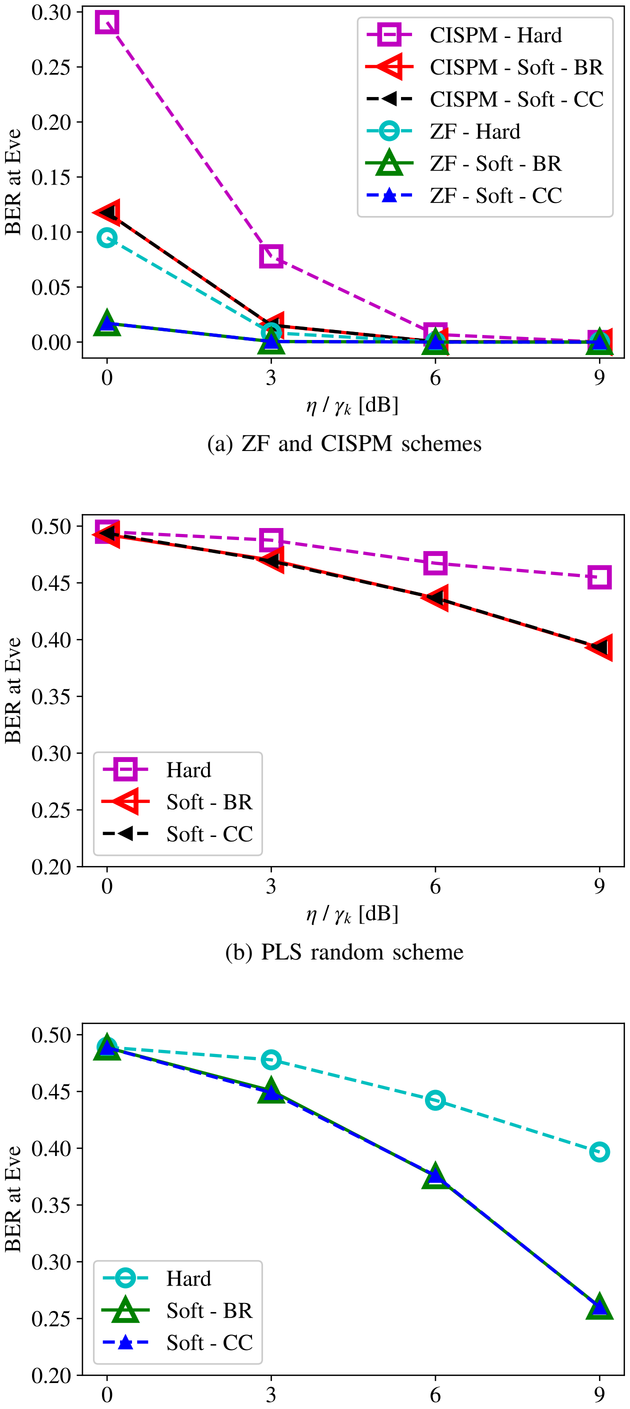
Fig. 10: LLRs distribution of the Soft - CC decoding scheme with $r = {}^1\!/_3$ and $M \in \{1, 9\}$.

$P_{\rm tot}$ is the same as the mean power η, as it has been set. As for the PLS schemes, $P_{\rm tot}$ depends on the number of antennas at Eve M, higher M leads to higher $P_{\rm tot}$. This increase is due to the fact that more antennas at Eve imply more constraints in the case of PLS random that result in the observed big increase in $P_{\rm tot}$ for $M = 13$. To elaborate more, this behavior is due to the fact that, the more we constrain our signal design problem, the more power is required to solve it. However, in the case of PLS Eve-min-power, the higher M, the higher the power consumption, i.e., the more antennas at Eve, the Eve-related part of the objective function tends to have higher values due to the higher degrees of freedom at the Eve's side, thus higher power consumption; even for $M = 13$, PLS Eve-min-power does not consume as much power as PLS random, its consumption is in fact equivalent to ZF scheme in $P_{\rm tot}$. However, for $M = 1$, the two proposed PLS schemes consume the same power.

Next, we investigate the impact of pilot overhead on our proposed ML-based attacks and countermeasures. We refer to [54] for some practical pilot overhead values. Fig. 1 in [54] shows the ergodic spectral efficiency as a function of pilot overhead in a high velocity setting. We observe that maximum spectral efficiency is achieved when using 0.1 pilot overhead. Thus, we evaluate our proposed Soft - CC decoding scheme using such value and lower.

Fig. 14 plots the coded BER at Eve using Soft - CC as a function of the pilot overhead. The parameters used in the simulation are: $r = {}^1\!/_3$, $N_{\rm t} = 15$, $K = 6$, $M = 11$, $\eta = \gamma_k = 6$ dB, and a frame size of 900 symbols. When the BS uses the non-secure schemes, ZF and CISPM, we observe that the higher the pilot overhead, the lower the BER, in particular, with a pilot overhead value of 0.1 the BER at Eve is as low as 10^{-3}, which is a sufficiently small BER that threatens the communication security. Thus, this validates again our ML-based attack even with pilot overhead values as low as 0.1. However, when the BS uses PLS schemes, the BER at Eve remains high, which again validates our countermeasures.

Lastly, in Fig. 15 we plot the runtime per SP [ms] as a function of the number of antennas at Eve M of the proposed and benchmark SLP schemes. The parameters used in the simulation are: $N_{\rm t} = 15$, $K = 6$, and $\gamma_k = 6$ dB, and a frame size of 900 symbols. We observe that for both PLS Eve-min-power and CISPM schemes, the runtime does not depend on M because both schemes do not have Eve-related constraints. And as expected, the PLS Eve-min-power scheme's runtime is a bit higher than the CISPM's one because of the extra Eve-

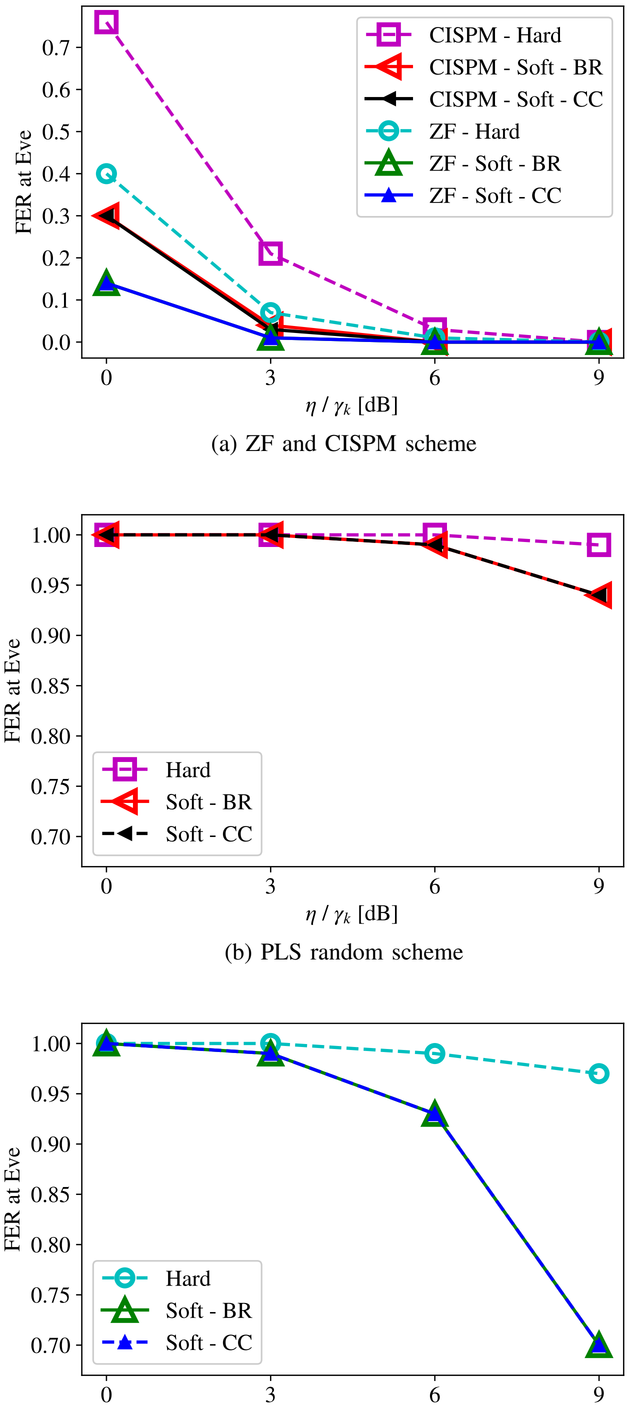


(a) ZF and CISPM schemes

(b) PLS random scheme

(c) PLS Eve-min-power scheme

Fig. 11: BER at Eve vs. η/γ_k [dB], with $r = 1/3$, $N_t = 15$, $K = 6$, and $M = 11$.



(a) ZF and CISPM scheme

(b) PLS random scheme

(c) PLS Eve-min-power scheme

Fig. 12: FER at Eve vs. η/γ_k [dB], with $r = 1/4$, $N_t = 15$, $K = 6$, and $M = 11$.

related term in the PLS Eve-min-power scheme's objective function in eq. (18). However, the runtime of PLS random increases with M and is higher than the runtime of PLS Eve-min-power. This increase is due to the Eve-related constraints in eq. (17) of the PLS random scheme, where in addition to the CI constraints in eqs. (15) and (16), there will be M Eve-related constraints. Thus, the higher M, the more constraints in the PLS random optimization problem, and therefore the higher the runtime.

We conclude this section by summarizing the insights from the numerical results.

1) Soft decoding schemes always outperform hard decod-

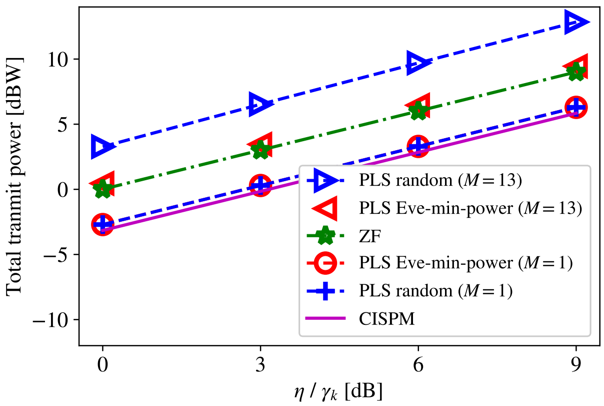


Fig. 13: QPSK-Total tansmit power [dBW] vs. target SINR [dB], with $N_{\mathrm{t}} = 15$, $K = 6$, and $M \in \{1, 13\}$.

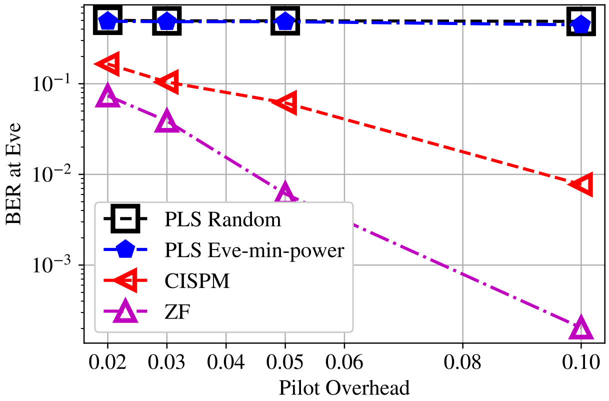


Fig. 14: BER at Eve using Soft - CC vs. the pilot percentage, with $r = 1/3$, $N_{\mathrm{t}} = 15$, $K = 6$, $M = 11$, $\eta = \gamma_k = 6$ dB, and a frame size of 900 symbols.

ing, i.e., soft values carry extra information that is used by the decoder to better estimate the original data.

2) Soft – CC and Soft – BR performance is the same because of the lack of label-correlation, due to the random nature of data to be transmitted.
3) Our proposed soft decoding schemes operates well with pilot overhead values as low as 0.1.
4) CISPM precoding is more secure than ZF because the precoding pattern changes at each symbol-period while ZF precoding is fixed throughout the whole coherence time.
5) Proposed PLS schemes are much more secure than CISPM and ZF, with PLS random being the most secure because of its induced randomness in the signal design that makes it harder for Eve to learn the precoding pattern.
6) Tremendous security gains are offered by the PLS Eve-min-power scheme when compared to the benchmark SLP scheme, CISPM, at the expense of only a marginal extra runtime.
7) PLS random scheme offers higher security than PLS Eve-min-power, however, its runtime increases linearly with the number of antennas at Eve.

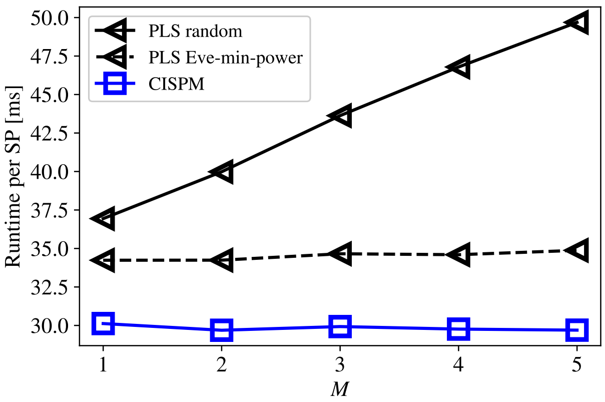


Fig. 15: Runtime per SP [ms] vs. M of proposed and benchmark schemes with $N_{\mathrm{t}} = 15$, $K = 6$, $\gamma_k = 6$ dB, and a frame size of 900 symbols.

8) Logistic regression is the most performing classifier amongst the tested state-of-the-art classifiers.
9) The system parameters that directly affect the BER/FER at Eve are: the number of antennas at Eve, the total transmit power, and the coding rate.
10) PLS schemes offer significant security gains compared to ZF and CISPM precoding schemes at the expense of additional power consumption at the transmitter.
11) More importantly, these security gains are achieved without affecting the performance at the intended users.

VI. Conclusions

In this paper, we proposed ML-based decoding schemes for a multi-antenna Eve in the context of a FEC-enabled MU-MISO systems. The proposed eavesdropping attacks use precoded pilot symbols as training data and enable an Eve to soft/hard decode a message with high accuracy. As a countermeasure to these attacks, we proposed two novel security-enhanced SLP precoders that seek to obstruct the learning process at Eve. Numerical results validated both the attacks as well as the countermeasures, where the soft decoding scheme always outperforms the hard decoding one. In addition, our proposed PLS schemes outperform ZF and CISPM precoding in security at the expense of additional power consumption at the transmitter, with PLS random scheme offering the highest security. Thus, the proposed PLS schemes provide different trade-offs between security, runtime, and power consumption, which would give the BS the option to select the most suited scheme depending on the required criteria. Notably, despite all the security gains offered by our proposed PLS schemes, their use does not affect the performance at the intended user. Future research topics would include investigating secure precoding schemes that assume imperfect Eve's CSI knowledge at the BS and developing secure schemes for the case when the channel to Eve is unknown to the BS.

References

[1] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May/June 2019.

[2] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G wireless communications: Vision and potential techniques," *IEEE Netw.*, vol. 33, no. 4, pp. 70–75, July/Aug 2019.

[3] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security and intelligence," *IEEE Wireless Commun.*, pp. 1–7, 2020.

[4] Cisco VNI Forecast, "Cisco Visual Networking Index: Forecast and Trends, 2018-2023 White Paper," *Cisco Public Inf.*, Feb 2019.

[5] Y. Liu, H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 2017.

[6] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas in Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[7] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, Secondquarter 2019.

[8] S. X. Ng, A. Conti, G. Long, P. Muller, A. Sayeed, J. Yuan, and L. Hanzo, "Guest editorial advances in Quantum communications, computing, cryptography, and sensing," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 405–412, Mar. 2020.

[9] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Josang, "The impact of quantum computing on present cryptography," *Int. J. Adv. Comput. Sci. Appl. (IJACSA)*, vol. 9, no. 3, pp. 405–414, Mar. 2018.

[10] Z. Wei, C. Masouros, F. Liu, S. Chatzinotas, and B. Ottersten, "Energy- and cost-efficient physical layer security in the era of IoT: The role of interference," *IEEE Commun. Mag.*, vol. 58, no. 4, pp. 81–87, 2020.

[11] W. Wang, J. Tang, N. Zhao, X. Liu, X. Y. Zhang, Y. Chen, and Y. Qian, "Joint precoding optimization for secure SWIPT in UAV-aided NOMA networks," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 5028–5040, 2020.

[12] N. Zhao, Y. Li, S. Zhang, Y. Chen, W. Lu, J. Wang, and X. Wang, "Security enhancement for NOMA-UAV networks," *IEEE Trans. Vehicular Tech.*, vol. 69, no. 4, pp. 3994–4005, 2020.

[13] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, 2008.

[14] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, 2012.

[15] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Process. Letters*, vol. 20, no. 1, pp. 39–42, 2013.

[16] H.-M. Wang, T. Zheng, and X.-G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, 2015.

[17] H.-M. Wang, C. Wang, and D. W. K. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285–6298, 2015.

[18] A. Li, D. Spano, J. Krivochiza, S. Domouchtsidis, C. G. Tsinos, C. Masouros, S. Chatzinotas, Y. Li, B. Vucetic, and B. Ottersten, "A tutorial on interference exploitation via symbol-level precoding: Overview, state-of-the-art and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 796–839, Secondquarter 2020.

[19] M. Alodeh, D. Spano, A. Kalantari, C. G. Tsinos, D. Christopoulos, S. Chatzinotas, and B. Ottersten, "Symbol-level and multicast precoding for multiuser multiantenna downlink: A state-of-the-art, classification, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1733–1757, thirdquarter 2018.

[20] C. Masouros and E. Alsusa, "Dynamic linear precoding for the exploitation of known interference in MIMO broadcast systems," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1396–1404, Mar. 2009.

[21] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Directional modulation via symbol-level precoding: A way to enhance security," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1478–1493, Dec. 2016.

[22] Taesang Yoo and A. Goldsmith, "On the optimality of multiantenna broadcast scheduling using zero-forcing beamforming," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 3, pp. 528–541, 2006.

[23] R. Liu, M. Li, Q. Liu, and A. L. Swindlehurst, "Secure symbol-level precoding in MU-MISO wiretap systems," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3359–3373, 2020.

[24] Y. Fan, A. Li, X. Liao, and V. C. M. Leung, "Secure interference exploitation precoding in MISO wiretap channel: Destructive region redefinition with efficient solutions," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 402–417, 2021.

[25] Q. Xu, P. Ren, and A. L. Swindlehurst, "Rethinking secure precoding via interference exploitation: A smart eavesdropper perspective," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 585–600, 2021.

[26] J. Wang, C. Jiang, H. Zhang, Y. Ren, K. C. Chen, and L. Hanzo, "Thirty years of machine learning: The road to Pareto-Optimal wireless networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1472–1514, 2020.

[27] C. Jiang, H. Zhang, Y. Ren, Z. Han, K. Chen, and L. Hanzo, "Machine learning paradigms for next-generation wireless networks," *IEEE Wireless Commun.*, vol. 24, no. 2, pp. 98–105, Apr. 2017.

[28] N. Kato, B. Mao, F. Tang, Y. Kawamoto, and J. Liu, "Ten challenges in advancing machine learning technologies toward 6G," *IEEE Wireless Commun.*, vol. 27, no. 3, pp. 96–103, 2020.

[29] M. Kulin, T. Kazaz, I. Moerman, and E. de Poorter, "A survey on machine learning-based performance improvement of wireless networks: PHY, MAC and network layer," vol. arXiv preprint arXiv:2001.04561, 2020. [Online]. Available: http://arxiv.org/abs/2001.04561

[30] M. Z. Hameed, A. Gyorgy, and D. Gunduz, "Communication without interception: Defense against deep-learning-based modulation detection," vol. arXiv preprint arXiv:1902.10674, 2019. [Online]. Available: http://arxiv.org/abs/1902.10674

[31] K. L. Besser, P.-H. Lin, C. R. Janda, and E. A. Jorswieck, "Wiretap code design by neural network autoencoders," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3374–3386, 2019.

[32] R. Fritschek, R. F. Schaefer, and G. Wunder, "Deep learning for the gaussian wiretap channel," vol. arXiv preprint arXiv:1810.12655, 2018. [Online]. Available: http://arxiv.org/abs/1810.12655

[33] A. Mayouche, D. Spano, C. G. Tsinos, S. Chatzinotas, and B. Ottersten, "Learning-assisted eavesdropping and symbol-level precoding countermeasures for downlink MU-MISO systems," *IEEE Open J. Comm. Soc.*, vol. 1, pp. 535–549, 2020.

[34] Q. Li and W. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, 2013.

[35] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, 2011.

[36] W. Liao, T. Chang, W. Ma, and C. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, 2011.

[37] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, 2008.

[38] ETSI, "Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications; Part 2: DVB-S2 Extensions (DVB-S2X)," European Telecommunications Standards Institute (ETSI), Deliverable 302.307-2, 10 2014, version 1.1.1.

[39] M. Alodeh, S. Chatzinotas, and B. Ottersten, "Constructive Multiuser Interference in Symbol Level Precoding for the MISO Downlink Channel," *IEEE Trans. Signal Process.*, vol. 63, no. 9, pp. 2239–2252, May 2015.

[40] P. Wang and R. Safavi-Naini, "A model for adversarial wiretap channels," *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 970–983, 2016.

[41] M.-L. Zhang, Y.-K. Li, X.-Y. Liu, and X. Geng, "Binary relevance for multi-label learning: an overview," *Springer Front. Comput. Sci.*, vol. 12, no. 1, p. 191–202, Jan 2018.

[42] Z. Yu, Q. Wang, Y. Fan, H. Dai, and M. Qiu, "An improved classifier chain algorithm for multi-label classification of big data analysis," *IEEE 17th Int. Conf. High Performance Comput. Commun., IEEE 7th Int. Symposium Cyberspace Safety Security, 12th Int. Conf. Embedded Softw. and Syst.*, pp. 1298–1301, 2015.

[43] R. Gallager, *Chapter 8, course materials for 6.450 Principles of Digital Communications I.* MIT OpenCourseWare, Fall 2006.

[44] J. C. Platt, "Probabilistic outputs for support vector machines and comparisons to regularized likelihood methods," in *Advances in Large Margin Classifiers*. MIT Press, 1999, pp. 61–74.

[45] A. Mayouche, D. Spano, C. G. Tsinos, S. Chatzinotas, and B. Ottersten, "SER-constrained symbol-level precoding for physical-layer security," *IEEE Conf. Commun. Netw. Security*, pp. 1–5, June 2019.

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

[47] S. Boyd and L. Vandenberghe, *Convex optimization.* Cambridge Univ. Press, 2004.

[48] J. Krivochiza, J. Merlano Duncan, S. Andrenacci, S. Chatzinotas, and B. Ottersten, "FPGA acceleration for computationally efficient symbol-level precoding in multi-user multi-antenna communication systems," *IEEE Access*, vol. 7, pp. 15 509–15 520, 2019.

[49] A. Haqiqatnejad, J. Krivochiza, J. C. M. Duncan, S. Chatzinotas, and B. Ottersten, "Design optimization for low-complexity FPGA implementation of symbol-level multiuser precoding," *IEEE Access*, vol. 9, pp. 30 698–30 711, 2021.

[50] N. Samuel, T. Diskin, and A. Wiesel, "Learning to detect," *IEEE Trans. Signal Process.*, vol. 67, no. 10, pp. 2554–2564, 2019.

[51] J. Yuan, *A practical guide to error-control coding using MATLAB*. Boston: Artech House, 2010.

[52] A. J. Viterbi, "A personal history of the Viterbi algorithm," *IEEE Signal Process. Magazine*, vol. 23, no. 4, pp. 120–142, July 2006.

[53] P. Popovski, K. F. Trillingsgaard, O. Simeone, and G. Durisi, "5G wireless network slicing for eMBB, URLLC, and mMTC: A communication-theoretic view," *IEEE Access*, vol. 6, pp. 55 765–55 779, 2018.

[54] A. Lozano and N. Jindal, "Optimum pilot overhead in wireless communication: A unified treatment of continuous and block-fading channels," *European Wireless Conf.*, pp. 725–732, 2010.