Received 6 March 2020; revised 4 April 2020; accepted 16 April 2020. Date of publication 27 April 2020; date of current version 18 May 2020.

*Digital Object Identifier 10.1109/OJCOMS.2020.2989738*

# Learning-Assisted Eavesdropping and Symbol-Level Precoding Countermeasures for Downlink MU-MISO Systems

**ABDERRAHMANE MAYOUCHE (Student Member, IEEE), DANILO SPANO (Member, IEEE), CHRISTOS G. TSINOS (Member, IEEE), SYMEON CHATZINOTAS (Senior Member, IEEE), AND BJÖRN OTTERSTEN (Fellow, IEEE)**

Interdisciplinary Centre for Security Reliability and Trust (SnT), University of Luxembourg, L-1855 Luxembourg City, Luxembourg

CORRESPONDING AUTHOR: A. MAYOUCHE (e-mail: abderrahmane.mayouche@uni.lu)

This work was supported in part by the Engineering and Physical Sciences Research Council, in part by the Luxembourg National Research Fund Project, titled Exploiting Interference for Physical Layer Security in 5G Networks (CI-PHY), in part by the ECLECTIC FNR Project, Energy and Complexity Efficient Millimeter-Wave Large-Array Communications, and in part by the European Research Council under Horizon 2020 under Grant 742648, AGNOSTIC.

Part of this work has been accepted for publication in the *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Waikoloa, HI, USA, Dec. 2019.

**ABSTRACT** In this work, we introduce a machine-learning (ML) based detection attack, where an eavesdropper (Eve) is able to learn the symbol detection function based on precoded pilots. With this ability, an Eve can correctly detect symbols with a high probability. To counteract this attack, we propose a novel symbol-level precoding (SLP) scheme that enhances physical-layer security (PLS) while guaranteeing a constructive interference effect at the intended users. Contrary to conventional SLP schemes, the proposed scheme is robust to the ML-based attack. In particular, the proposed scheme enhances security by designing Eve's received signal to lie at the boundaries of the detection regions. This distinct design causes Eve's detection decisions to be based almost purely on noise. The proposed countermeasure is then extended to account for multi-antennas at the Eve and also for multi-level modulation schemes. In the numerical results, we validate both the detection attack and the countermeasures and show that this gain in security can be achieved at the expense of only a small additional power consumption at the transmitter, and more importantly, these benefits are obtained without affecting the performance at the intended user.

**INDEX TERMS** Multi-user interference, constructive interference, symbol-level precoding, physical-layer security, machine learning, convex optimization, MISO, and bit-error rate.

## I. INTRODUCTION

THE FIFTH generation (5G) of cellular networks aims at satisfying the wireless broadband demands of 2020 [1]. By 2022, there will be 28.5 billion connected devices [2]. In such a congested environment, unintended receivers (e.g., an eavesdropper (Eve)) may detect some sensitive information. Thus, security is of paramount importance to next generation networks. In particular, physical-layer security (PLS) has attracted much interest recently as a complement to security in higher layers of the network [3].

The essence of PLS is to use the randomness of the propagation channel to provide security at the physical layer, i.e., by minimizing the information leakage to the Eve. Namely, PLS is envisioned to be used as an additional layer of protection on top of the existing security methods based on cryptography. As the rise of quantum computing is threatening both symmetric and asymmetric cryptography [4], non-cryptographic methods are needed. Most literature on PLS utilize information theoretic metrics, such as secrecy rate [5], for performance analysis [6]–[11]. However, we find only few work in the literature [12]–[14] that tackles the problem from a signal processing point of view.

Meanwhile, in a downlink multiuser communication systems, where multiple users are simultaneously served with independent information over the same channel resource, interference among users can greatly limit the system throughput. Multi-user interference (MUI) leads to a deviation of the received symbols outside of their detection region, thus altering the correct detection of the transmitted symbols. A popular technique to tackle MUI is multiuser precoding. Block level precoding considers the MUI as harmful and should be mitigated [15]–[18]. In this situation, the precoding is limited to alleviate the interference along the whole frame as it uses only the knowledge of channel-state information (CSI). This results in reducing the average amount of interference in the frame. Contrary to block-level precoding, in symbol-level precoding (SLP), the interference can be controlled on a symbol-by-symbol basis. This way permits to rotate each interfering signal to be in the correct detection region, thus eliminating the inter-user interference at each symbol slot. Therefore, SLP techniques [19] ensures interference-free communication at the price of a higher switching rate at the precoder [20]–[26].

In the context of security, SLP has been proposed as a new way for physical-layer security [27]. Namely, this technique is inherently secure as the transmitted signal is strictly designed for an intended receiver based on both his CSI and DI, thus naturally making Eve's received signal quite different as the designed signal is a function of the intended user's channel and not Eve's channel. Likewise, in [14], the authors used the idea of a smart Eve that exploits the statistical characteristics of the received signal at the latter in order to improve its detection performance. To tackle this vulnerability, they presented a new design principle for secure SLP precoding and proposed two algorithms to generate the precoder. While their approach requires more transmit power, it can achieve an improved security. Similarly, we note that the concept of exploiting MUI was also employed to design artificial noise (AN) beamformers that is constructive to the intended user and destructive to the Eve [28].

Even thought SLP techniques can be considered secure for a common Eve which employs a conventional detector, yet it is not the case for the sophisticated ones. In other words, an advanced Eve may use machine learning (ML) based techniques to successfully detect the desired signal even in the case when a conventional symbol-level precoder is used. Notably, ML has drawn significant interest in the area of wireless communication. That is, machine learning, a main subset of artificial intelligence (AI), is the set of tools and algorithms used to make predictions or decisions through learning patterns from data [29]. Namely, based on a sample data, known as the training set, ML algorithms build a mathematical model in order to make predictions or decisions. In the context of next-generation wireless systems, ML can be used to model/solve various problems in large-scale multiple-input multiple-output (MIMO), device-to-device (D2D) networks, heterogeneous networks (HetNets), …, etc [30] [31]. More particularly, at the physical layer (PHY) of communication systems, deep learning (DL), a subclass of ML, has shown a promising potential. In [32], a new way of end-to-end system design was proposed using DL, where the system can learn the whole transmitter and receiver processes for a given channel model.

Nevertheless, in the context of PLS, only a few works that involve ML has been proposed. In [33], the authors proposed a ML-based scheme against an attacker that employs deep neural networks (DNNs) to determine the modulation scheme used. To reduce the accuracy of the intruder, a constellation perturbation is introduced at the encoder by using the same DNNs structure. This perturbation is designed in such a way to not confuse the intended receiver. In [34] however, the authors proposed a flexible wiretap code design for Gaussian channels under finite block length through autoencoders. To this end, Karl *et al.* formulated a multi-objective problem that takes into account the performance of both the intended receiver and the Eve. Thereafter, the authors solve this optimization problem using neural networks based autoencoders. This work falls in the same category as [35], which also exploited the power of autoencoders for wiretap code design.

In our work, on the other hand, ML is used in a different way. Namely, Eve can utilize the power of ML in order to improve its detection accuracy. Since most communications standards, such as 5G NR, WiFi, and DVBS, use both un-precoded and precoded pilots for purposes of CSI and signal-to-noise (SNR) estimation, as a result, an Eve can take advantage of this extra information to improve its detection accuracy.

Namely, we propose and validate the ML-based attack in the context of multi-user multiple-input single-output (MU-MISO) system by comparing different classifiers. We show that even SLP-based secure schemes [27] are vulnerable to such an attack. To counteract this attack, we propose a novel secure SLP-based precoder design as a countermeasure to this attack. The idea of the proposed scheme is to design the transmitted signal to simultaneously perform both constructive interference at the intended receivers and force Eve's received signal to lie at the boundary of its detection region. This distinct design of Eve's received signal makes its detection decision based mostly on the noise, which provides maximum equivocation. At the same time, it makes it an energy efficient scheme, as it employs only a small deviation of the received constellation point. Thereafter, we compare the different schemes using a new metric that combines both required transmit power and achievable BER at the Eve. Simulation results show the potency of the ML-based attack and the effectiveness of the proposed countermeasure. We note that we tackle this problem from a signal processing point of view rather than from an information theoretic one. The primary contributions of the paper are listed below:

1) We introduce the machine-learning based detection attack by considering both single and multi-antenna Eve, when SLP signals are employed. We design the ML framework of the attack to support both single-level and multi-level modulations. For this attack, we study several ML classifiers for symbol detection and compare their prediction accuracy.

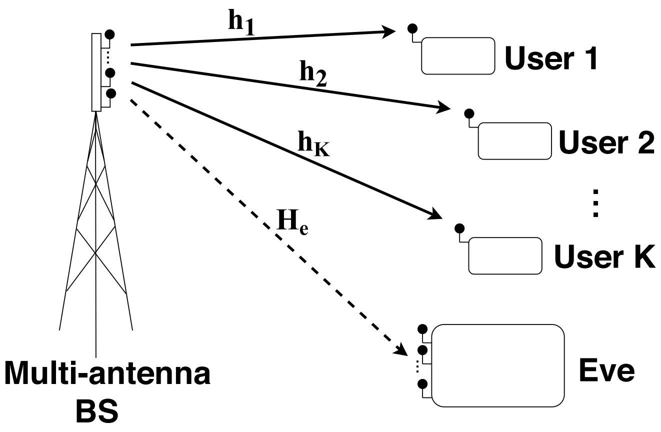


FIGURE 1. Downlink MU-MISO system with K single-antenna users and one multi-antenna eavesdropper.

2) As a countermeasure to this detection attack, we propose a novel precoding design principle that increases the achievable BER at Eve. We then formulate an optimization problem based on this design principle, that we call PLS scheme. We note that the proposed scheme assumes perfect knowledge of Eve's channel at the BS [28], which is the case when Eve is part of the system trying to Eavesdrop other users.
3) As the proposed problem is non-convex, we propose different convex formulations of the same problem, that provides varying tradeoffs between security, computational efficiency, and transmit power.
4) We compare the different PLS schemes with a benchmark scheme using a new metric that we propose, that takes into account both the secure bit-rate and the power consumption.
5) We finally investigate the performance of the proposed schemes under different receive SNR levels at Eve.

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

*Notations:* Upper and lower boldface symbols are used to denote matrices and column vectors, respectively. $\|\cdot\|$ represents the Euclidean norm. $\mathcal{CN}(\mathbf{m},\mathbf{Q})$ denotes the circular symmetric complex Gaussian distribution with mean $\mathbf{m}$ and covariance matrix $\mathbf{Q}$. $\mathcal{R}^{m\times n}$ and $\mathcal{C}^{m\times n}$ represent the set of $m\times n$ real matrices, and the set of $m\times n$ complex matrices, respectively. The expectation operator is denoted by $\mathbb{E}[\,\cdot\,]$ and the absolute value by $|\cdot|$.

## II. SYSTEM MODEL

As depicted in Fig. 1, we consider a single cell multi-user (MU) multiple-antenna multiple-input single-output (MISO) downlink system, where the base station (BS) is equipped with $N_t$ transmit antennas serving $K$ single-antenna users, with $K \leq N_t$, and one multi-antenna eavesdropper with $M$ antennas. We assume a block fading channel $\mathbf{h}_j \in \mathcal{C}^{1\times N_t}$ between the transmit BS antennas and the $j$-th user. The received signal at the $j$-th user can be expressed as:

$$y_j[n] = \mathbf{h}_j\mathbf{x}[n] + z_j[n] \tag{1}$$

where $y_j[n] \in \mathcal{C}$ is the received signal at the $j$-th user in the symbol slot $n$, $\mathbf{x}[n] \in \mathcal{C}^{N_t\times 1}$ is the transmitted vector from the $N_t$ transmit antennas, and $z_j[n] \in \mathcal{C}$ is the additive white Gaussian noise (AWGN) at the $j$-th user with variance $\sigma_z^2$.

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

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

where $\mathbf{H} = [\mathbf{h}_1^T \cdots \mathbf{h}_K^T]^T \in \mathcal{C}^{K\times N_t}$ represents the system channel matrix and $\mathbf{z}[n] \in \mathcal{C}^{K\times 1}$ gathers the independent AWGN components of all users, with a variance of $\sigma_z^2$ each. We note that $\mathbf{H}$ is assumed to be known at the BS through pilot-assisted channel estimation [36].

Similarly, the received signal at an Eve with $M$ antennas, $\mathbf{y}_e[n] \in \mathcal{C}^{M\times 1}$, can be expressed as follows

$$\mathbf{y}_e[n] = \mathbf{H}_e\mathbf{x}[n] + \mathbf{z_e}[n] \tag{3}$$

where $\mathbf{H}_e = [\mathbf{h}_{e,1}^T \cdots \mathbf{h}_{e,M}^T]^T \in \mathcal{C}^{M\times N_t}$ represents the system channel matrix between the BS and the multi-antennas Eve, and $\mathbf{z}_e[n] \in \mathcal{C}^{M\times 1}$ gathers the independent AWGN components at all $M$ antennas, with a variance of $\sigma_e^2$ each.

In conventional block-level precoding, the transmitted vector $\mathbf{x}[n]$ is modeled as $\mathbf{W}\mathbf{d}_a[n]$, with $\mathbf{W}$ being the precoding matrix and $\mathbf{d}_a[n] \in \mathcal{C}^{K\times 1}$ the data information intended for the K legitimate users. Specifically, the precoding matrix $\mathbf{W}$ is designed depending only on the CSI. For this reason, this type of precoding is commonly being referred to as channel-level or block-level precoding [19], [36]. Consequently, the precoder $\mathbf{W}$ changes only when the CSI changes and remains constant for several symbol slots, making the relation between $\mathbf{x}[n]$ and $\mathbf{d}_a[n]$ linear.

In symbol-level precoding approach, however, the precoding module directly designs the transmitted signal vector $\mathbf{x}[n]$ based on both the CSI $\mathbf{H}$ and the input data symbols $\mathbf{d}_a[n]$, hence the symbol-level nomenclature, i.e., the precoded signal $\mathbf{x}[n]$ changes at every symbol slot [37]. Therefore, this scheme optimizes the transmit vector $\mathbf{x}[n]$ without any intermediate steps (such as designing $\mathbf{W}$) while constructively exploiting the inter-user interference. As a result, the relation between the transmit vector $\mathbf{x}[n]$ and the input symbol vector $\mathbf{d}_a[n]$ is no longer linear, as in the case of block-level precoding, and is inherently embedded into the precoding module. We note that the data symbols, $\mathbf{d}_a[n]$, are assumed to be uncorrelated and drawn from a generic multi-level constellation having unit average power. We also assume that the channel to the Eve is known at the BS. This assumption is reasonable when the Eve is a legitimate user trying to eavesdrop other users. This assumption gives Eve the advantage to know the modulation and coding parameters used, while it provides the BS with the information of

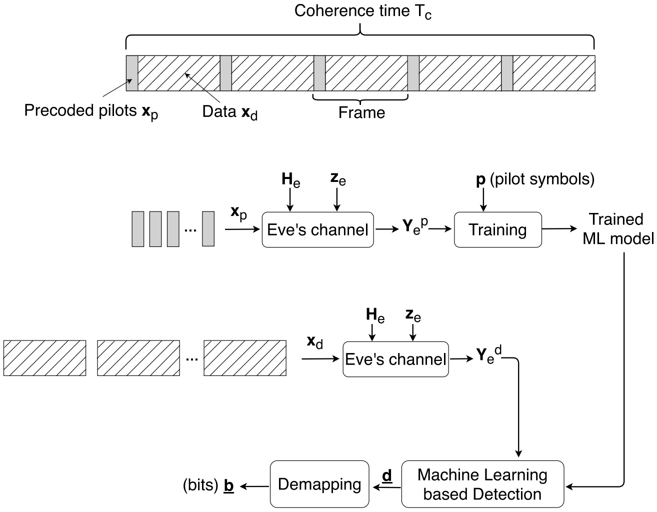


**FIGURE 2.** **Summary of the ML-based attack.**

his channel. For ease of notation, we drop the time index $n$ in the remainder of the paper.

## III. ML-BASED ATTACK

In this section, we introduce the ML-based attack, where an Eve can detect another user's symbols with a sufficiently low BER. Specifically, Eve would know the precoded pilot symbols used and their placement in the frame. This side information, which is usually publicly available in standards, can be exploited by the Eve and used to eavesdrop another user via the use of machine learning (ML) tools. This attack encompasses two phases i) training phase and ii) prediction phase. An overview of the attack is provided in Fig. 2. Alongside, we present the two phases of the attack followed by a formulation of it. We then conclude this section by presenting a practical example of the ML-based attack on a SLP benchmark scheme.

### A. TRAINING PHASE

As shown in Fig. 2, the BS sends multiple frames within one coherence time $T_c$, where at the beginning of each frame, we find precoded pilots, $\mathbf{x}_p \in \mathcal{C}^{N_t \times 1}$, for channel and SNR estimation. The received pilot signals at the $i$-th antenna of the Eve, $y^p_{e,i} \in \mathcal{C}$, can be written as follows

$$y^p_{e,i} = \mathbf{h}_{e,i}\mathbf{x}_p + z_{e,i} \tag{4}$$

where $\mathbf{h}_{e,i} \in \mathcal{C}^{1\times N_t}$ is the vector of the channel coefficients between the BS and the $i$-th antenna of the Eve and $z_{e,i} \in \mathcal{C}$ is the AWGN at the Eve with variance $\sigma^2_{e,i}$. The overall received pilot signal at Eve at all antennas, $\mathbf{y}^p_e \in \mathcal{C}^{1\times M}$, can be written as

$$\mathbf{y}^p_e = \mathbf{H}_e\mathbf{x}_p + \mathbf{z}_e. \tag{5}$$

As $y^p_{e,i}$ is Eve's received pilot signal, it knows beforehand the corresponding pilot symbol $p$ that was transmitted. We note that the transmitted signal $\mathbf{x}_p$ is a function of all user symbols, however the introduced attack targets a specific user, for which we know the transmitted pilot symbols in advance. In other words, the Eve is not trying to decode the data of all the users, it instead attempts to decode the data of a single user. As such, the Eve would create a mapping between the received signal $\mathbf{y}^p_e$ and the corresponding labels $p$. Thus, the Eve can exploit the knowledge of the precoded pilots, that are sent regularly according to communication standards for signal-to-noise ratio (SNR) estimation, in order to improve its detection performance.

We note that, as the number of antennas at Eve, $M$, increases, the number of input features increase accordingly, which often leads to better prediction accuracy. In essence, each antenna at Eve receives a different distorted copy of the same transmitted signal $\mathbf{x}_p$, the more different copies of $\mathbf{x}_p$ received by Eve, the better the machine-learning model performance will be, thus resulting in an improved symbol detection accuracy.

In the case of QPSK, there are only 4 possible pilot symbols, hence 4 classes. In the ML world, these classes are commonly being referred to as labels. As such, the corresponding machine learning problem is a supervised ML problem [38]. Meanwhile, since the labels are discrete, i.e., constellation points, the problem is categorised as a classification problem. Namely, the training set $D$ contains $N$ training points, i.e., $\{\mathbf{y}^p_{e,n}, p_n\}, n = 1, \ldots, N$, where $y^p_{e,n}$ represents the $n$-th received pilot signal at Eve, while $p_n$ is the corresponding constellation point (label) associated with the observations $\mathbf{y}^p_{e,n}$. We further define the training set $D$ as

$$\left\{\mathbf{y}^p_{e,n}, p_n\right\} \sim f(\mathbf{y}, p), n = 1, \ldots, N \tag{6}$$

where the operator $\sim$ signifies that the pairs $\{\mathbf{y}^p_{e,n}, p_n\}, n = 1, \ldots, N$ are i.i.d with probability distribution $f(\mathbf{y}, p)$. The training set $D$ can be written in a more compact form as below

$$D = \left\{\mathbf{Y}^p_e, \mathbf{p}\right\} \tag{7}$$

where $\mathbf{Y}^p_e \in \mathcal{C}^{N\times M}$ is the received pilot symbols at Eve and $\mathbf{p} \in \mathcal{C}^{N\times 1}$ are the corresponding transmitted pilot symbols.

For simplicity, we denote the real and imaginary parts of $\mathbf{Y}^p_e$ as two real numbers, called input features, while we represent each pilot symbol in $\mathbf{p}$ using four[1] decimal $c = \{0, 1, 2, 3\}$, with each class corresponding to one QPSK symbol. Hence, the training set becomes $\{\mathbf{Y}^{p,r}_e, \mathbf{Y}^{p,im}_e, \mathbf{c}_p\}$ with $\mathbf{Y}^{p,r}_e \in \mathcal{R}^{N\times M}$ being the real part of Eve's received pilot signals, $\mathbf{Y}^{p,im}_e \in \mathcal{R}^{N\times M}$ is its imaginary part, and $\mathbf{c}_p \in \mathcal{N}^{N\times 1}$ are their corresponding classes. Based on the training set $D$, we derive a predictor (the trained ML model) that predicts a class $l$ based on the observation $y_e$.

### B. PREDICTION PHASE

As depicted in Fig. 2, the BS sends precoded data, $\mathbf{x}_d \in \mathcal{C}^{N_t\times 1}$, to the users. The received symbol at Eve in each

[1] The number of classes depends on the modulation order used. In the case of QPSK, the number of classes equals four.

symbol period, $\mathbf{y}_e^d \in \mathcal{C}^{M\times 1}$, can be written as follows

$$\mathbf{y}_e^d = \mathbf{H}_e \mathbf{x}_d + \mathbf{z}_e. \tag{8}$$

where $\mathbf{x}_d \in \mathcal{C}^{N_t \times 1}$ represents the transmitted precoded signal from the $N_t$ transmit antennas intended for all the users during one symbol period. If we assume that there are $L$ data symbols in one coherence time, $\mathbf{Y}_e^d \in \mathcal{C}^{L\times M}$ represents the collection of all received symbols at Eve during one coherence time $T_c$.

The goal of classification is to predict a label $d$ for a new, usually unobserved, received precoded signals, $\mathbf{y}_e^d$, that is outside the pilot signals. Namely, a machine learning-based detection can be performed over $\mathbf{Y}_e^d$ using the trained ML model, as shown in Fig. 2. The output of the ML-based detector block is the symbols vector $\underline{\mathbf{d}} \in \mathcal{C}^{L\times 1}$, which is an estimate of $\mathbf{d} \in \mathcal{C}^{L\times 1}$ (symbols intended for a specific user). Then, we perform demapping over $\underline{\mathbf{d}}$ to obtain the corresponding bit-vector $\underline{\mathbf{b}}$. Finally, we compare $\underline{\mathbf{b}}$ to $\mathbf{b}$ (the actual bits sent to a specific user) to obtain the BER at Eve.

### C. ML ATTACK FORMULATION

As stated above, the idea of supervised learning classification is to find a robust mapping $h$ between the input features $\mathbf{Y}_e^p$ and the classes $\mathbf{p}$ using the training dataset $D$. To further illustrate, we give the example of the support vector machine (SVM) classifier. The goal of SVM classifier is to separate the four[2] classes using lines that are usually hyperplanes.

The hyperplanes can be described using the below equation

$$\mathbf{w}\,\mathbf{y}_e + b = 0 \tag{9}$$

where $\mathbf{w}$ is the normal to the hyperplane and $\frac{b}{\|\mathbf{w}\|}$ is the perpendicular distance from the hyperplane to the origin. Support vectors, as their names imply, are the separating hyperplanes and the goal of the SVM algorithm is to orientate the hyperplanes in such a way to be as far as possible from the closest members of the different classes. Namely, implementing the SVM classifier boils down to selecting the parameters $\mathbf{w}$ and $b$ that best achieve the aforementioned goal through the use of the training data. Once these parameters are estimated, the trained ML model can be used to directly predict the transmitted symbols from observing any received signal at the Eve during the same coherence time $T_c$.

### D. ATTACK EXAMPLE ON A BENCHMARK SCHEME - CISPM

As a Benchmark, we use the approach in [37], which is commonly being referred to as constructive interference for sum power minimization (CISPM). This particular scheme is designed to exploit inter-user interference for power gains at the intended users, in other words, this scheme propels the intended users' received signals deeper into the correct detection region of the desired symbol for each user.

TABLE 1. Performance of different classifiers for SLP-based dataset.

| Classifier | Symbol detection accuracy |
|---|---|
| Support Vector Machines | 0.7 |
| Gradient Boosting Machine | 0.63 |
| Logistic Regression | 0.71 |
| K-Nearest Neighbors | 0.66 |
| XGBoost | 0.68 |
| Light GBM | 0.67 |

Although this scheme applies no processing towards Eve's received signal, it still provides security gains. Namely, since the transmitted signals are designed to have constructive interference (CI) only with the intended users channels, Eve's received signal would in all likelihood fall in a different region than the correct one, as his channel is different than the intended user's one. Hence, the benchmark scheme is inherently secure against a conventional eavesdropper. The corresponding optimization problem is defined as

$$\begin{aligned} \mathbf{x}(\mathbf{d},\mathbf{H},\gamma) = \arg\min_{x} \quad & ||\mathbf{x}||^2 \\ \text{subject to} \quad & Re\{\mathbf{h}_j\mathbf{x}\} \trianglelefteq \sigma_z\sqrt{\gamma_j}Re\{d_j\}, j = 1,\ldots,K \\ & Im\{\mathbf{h}_j\mathbf{x}\} \trianglelefteq \sigma_z\sqrt{\gamma_j}Im\{d_j\}, j = 1,\ldots,K \end{aligned} \tag{10}$$

where $\gamma_j$ is the target SINR for the $j$-th user, $\gamma = [\gamma_1,\ldots,\gamma_K] \in \mathcal{R}^{K\times 1}$ represents the target SINR for all users. This problem is convex as both objective function and constraints are convex and can be solved efficiently using second order cone programming [39].

Although the CISPM scheme is secure against conventional eavesdropper, it can not stand against a sophisticated Eve that employs machine learning for symbol detection. As we shall demonstrate subsequently, the CISPM is vulnerable to the ML-based attack as it uses no specific pre-processing for Eve's received signal.

The setup of the experiment is as follows. We consider a BS using the CISPM scheme to precode the transmit signal $\mathbf{x}$ intended to the $K$ users. Particularly, both transmit signals $\mathbf{x}_p$ and $\mathbf{x}_d$ are designed using the CISPM scheme. In Table 1, we show the symbol detection accuracy[3] of the different classifiers when the CISPM scheme is used. We note that, for this simulation we used QPSK modulation, $N_t = 10$, $K = 6$, and a single antenna Eve. In this particular experiment, we used 100 symbols as pilots and 1000 symbols as data. In this setting, we used MATLAB for data generation and Python for classification and performance analysis. We should mention that we did not use deep learning [40] in this context despite its high performance mainly because it requires considerable amount of training data that is not available in our case. Namely, in each coherence time, only one portion of the frame is dedicated to pilot symbols, which in turn serve as the training data, and since the channel and data change in each frame, training could be done only within the

[2] The number of classes depends on the modulation order. For QPSK, the number of classes equals four.

[3] This accuracy refers to the accuracy of the trained ML model, i.e., the learning block of the diagram in Fig. 2.

frame itself, hence the limitation of training data. We notice that the symbol detection accuracy is relatively high when using such a scheme. This is due to the fact that at the BS, there was no particular constraint or processing towards the received signal at Eve. Therefore, Eve is using the power of ML tools to be able to still discriminate between the intended symbols for a particular user, even though the precoded signal was specifically designed for channel vectors that are considerably different than Eve's one.

## IV. COUNTERMEASURE - PHYSICAL-LAYER SECURITY (PLS) SCHEME

In this section, we first present a novel secure principle for designing secure precoding schemes that counteract the ML-based Eve. Then, based on this principle, we propose a precoder that yields high achievable BER at the Eve. Since the formulation of the latter scheme is non-convex, we propose an equivalent convex formulation. As a tradeoff between security and transmit power, we propose three other convex secure precoding schemes that are more energy efficient.

### A. SECURE DESIGN PRINCIPLE

As presented in the earlier section, an Eve with multiple antennas can achieve a decent detection performance that allows it to detect most of the received symbols by using the power of machine leaning. In order to dramatically worsen its detection performance, we propose a novel design principle of the precoded signal. Namely, we deliberately force the received signal at the Eve to lie at the boundaries of the detection regions.

This specific design has two advantages 1) to increase PLS as the detection decisions at the Eve will be mostly made depending on noise and 2) for energy efficiency purposes since it involves only a small deviations of the received constellation point.

### B. PLS SCHEME

In this section, we introduce the SLP-based countermeasure, that we call subsequently PLS scheme. Similar to [12], the idea is to design the transmitted signal $\mathbf{x}$ so as to have constructive interference at the intended users, and at the same time, to confuse the Eve by maximizing its detection uncertainty using the above secure design principle.

The PLS scheme is demonstrated in Fig. 3. Herein, we adopt the example of QPSK modulation for illustration purposes, where the dark circles represent the constellation points. We design the transmitted signal in such a way to have constructive interference at the intended users, that is represented by the grey shared regions. The goal here is to push the received points deeper into the detection region in order to improve the intended users' detection accuracy. However, we design Eve's received signal to lie in the strapped region (boundary of the detection region), whose width is controlled by the parameter $\delta$. The lower the value of $\delta$, the sharper the strapped region, thus the higher the probability of falling into a different region after noised adds up, resulting in higher BER at Eve. It is worth noticing that this particular design makes Eve's detection decisions to be mostly based on noise.

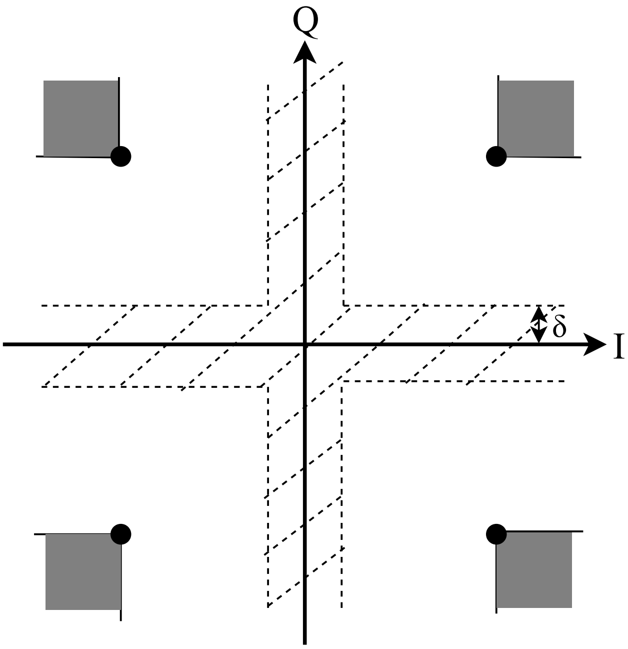


FIGURE 3. Example of PLS scheme using QPSK modulation.

For a downlink MU-MISO system, with $N_t$ transmit antennas and $K$ users, the aforementioned precoder design problem can be formulated as a power minimization problem as

$$\mathbf{x}(\mathbf{d}, \mathbf{H}, \mathbf{h}_e, \gamma, \delta) = \arg\min_{x} \|\mathbf{x}\|^2 \tag{11}$$

$$\text{subject to } \; Re\{\mathbf{h}_j\mathbf{x}\} \trianglelefteq \sigma_z\sqrt{\gamma_j} Re\{d_j\}, \quad j = 1, \cdots, K \tag{12}$$

$$Im\{\mathbf{h}_j\mathbf{x}\} \trianglelefteq \sigma_z\sqrt{\gamma_j} Im\{d_j\}, \quad j = 1, \cdots, K \tag{13}$$

$$Re\{\mathbf{h}_e^i\mathbf{x}\} \lesseqgtr \mp\delta, \;\; i = 1, \ldots, M \tag{14}$$

$$Im\{\mathbf{h}_e^i\mathbf{x}\} \lesseqgtr \mp\delta, \;\; i = 1, \ldots, M \tag{15}$$

where $\mathbf{h}_j\mathbf{x}$ is the $j$-th user's noiseless received signal, $\mathbf{h}_e\mathbf{x}$ is the noiseless received signal at the Eve, $\trianglelefteq$ denotes the correct detection region [22], $\delta$ is the distance parameter controlling the width of the strapped region, the operator $\lesseqgtr \mp$ refers to $\leq +$ and $\geq -$ simultaneously, while $Re$ and $Im$ denotes real and imaginary parts, respectively. The above problem[4] is non-convex because of the non-convexity of target region of Eve's received signal.The physical meaning of constraints in the PLS scheme are of two types. Constructive interference (CI) at the legitimate users, achieved by constraints (12)

[4] We note that the formulation in (11) is valid for a generic multi-level constellation, such as M-QAM, however it can be tailored to other constellations as APSK.

**Algorithm 1** PLS - Square Scheme

```
Input: $\mathbf{d}, \mathbf{H}, \mathbf{H}_e, \gamma, \sigma_z^2, \delta$;
Do: Solve problem (11) as follows:
    Satisfy CI constraints in (12) and (13)
    Satisfy constraints (14) and (15) simultaneously.
Output: $\mathbf{x}_s$
```

**Algorithm 2** PLS - Two-Steps Nearest

```
Input: $\mathbf{d}, \mathbf{H}, \gamma, \sigma_z^2$;                              ▷ Step 1
Solve problem (10)
Output: $\mathbf{x}_{CI}$
Input: $\mathbf{d}, \mathbf{H}, \mathbf{H}_e, \gamma, \sigma_z^2, \delta, \mathbf{x}_{CI}$;      ▷ Step 2
Do: Solve problem (11) as follows:
    Satisfy CI constraints in (12) and (13)
    if $|Re\{\mathbf{h}_e^i\mathbf{x}_{CI}\}| < |Im\{\mathbf{h}_e^i\mathbf{x}_{CI}\}|$ then
        return Satisfy constraint (14)
    else
        Satisfy constraint (15)
Output: $\mathbf{x}_n$
```

**Algorithm 3** PLS Scheme - Two-Steps Farthest

```
Input: $\mathbf{d}, \mathbf{H}, \gamma, \sigma_z^2$;                              ▷ Step 1
Solve problem (10)
Output: $\mathbf{x}_{CI}$
Input: $\mathbf{d}, \mathbf{H}, \mathbf{H}_e, \gamma, \sigma_z^2, \delta, \mathbf{x}_{CI}$;      ▷ Step 2
Do: Solve problem (11) as follows:
    Satisfy CI constraints in (12) and (13)
    if $|Re\{\mathbf{h}_e^i\mathbf{x}_{\mathbf{CI}}\}| > |Im\{\mathbf{h}_e^i\mathbf{x}_{CI}\}|$ then
        return Satisfy constraint (14)
    else
        Satisfy constraint (15)
Output: $\mathbf{x}_f$
```

and (13). The CI effect results in increased power gains at the legitimate users. However, constraints (14) and (15) are intended to have destructive interference at Eve to increase the uncertainty during symbol detection. Particularly, making his received signal lie at the boundary regions, so that the noise will move it in either direction of the detection regions and hence increase the BER at the latter. We note that the quality of service of the users, exhibited by constraints (12) and (13), does not affect constraints (14) and (15) of the boundary regions.

Namely, in problem (11), the non-convex constraints are the ones related to the Eve, they are as follows

$$Re\{\mathbf{h}_e^i\mathbf{x}\} \underset{>}{\leq} \mp\delta, i = 1, \dots, M \tag{16}$$

$$Im\{\mathbf{h}_e^i\mathbf{x}\} \underset{>}{\leq} \mp\delta, i = 1, \dots, M. \tag{17}$$

Given these constraints, the feasibility region of Eve's received signal is non-convex, as shown in Fig. 3 (the strapped region). In the following, we propose four convex implementations of the problem in (11), with varying security and energy efficiency trade-offs.

### 1) PLS - SQUARE SCHEME

In this scheme, we take the intersection of the vertical boundary region and the horizontal one, characterized by constraints (16) and (17), respectively. The intersection of the two form a square, hence the name. With this, the problem in (11) becomes convex and could be solved efficiently using convex solvers such as CVX. This scheme designs Eve's received signal to lie in the square whose center is the origin and side is $2\delta$. When noise is added, the received signal at Eve will lie on any of the 4 detection regions (in case of QPSK), thus providing high security. Algorithm 1 explains the process of signal design of the PLS - Square scheme.

We note that Algorithm 1 is executed for every symbol slot.

### 2) PLS - TWO-STEPS NEAREST SCHEME

In this scheme, as its name implies, the transmit signal $\mathbf{x}$ is designed in two steps. In the first step, we aim to determine the region in which Eve's received signal would lie when CISPM scheme is used (we name the transmit signal inhere $\mathbf{x}_{CI}$). Once we identify the coordinates of Eve's received signal, $\mathbf{H}_e\mathbf{x}_{CI}$, we feed this information into the second problem as an input. Herein, we execute problem (11) with the formulation of nearest. Namely, depending on where Eve's signal would land, we design it to fall into the nearest boundary region, either vertical one or horizontal one. The detailed steps of the procedure are found in Algorithm 2, where condition $|Re\{\mathbf{h}_e^i\mathbf{x}_{\mathbf{CI}}\}| < |Im\{\mathbf{h}_e^i\mathbf{x}_{CI}\}|$ implies that Eve's received signal is closer to the vertical boundary region, hence in this scheme we design Eve's received signal to lie in the vertical boundary region (constraint (characterized by 14)). Otherwise, we design Eve's received signal to lie in the horizontal boundary region instead (represented by constraint (15)).

### 3) PLS - TWO-STEPS FARTHEST SCHEME

This scheme can be considered as opposite of the PLS - Two-steps nearest scheme, i.e., instead of picking the closest boundary region, it always chooses the farthest one. Intuitively, this scheme would provide higher security gains than the nearest scheme (as it pushes the constellation point even farther, leading to higher chances of falling into the wrong region), however, it would consume more transmit power, the bigger the introduced deviation by the constraint, the higher power required to move it. Below we formulate the algorithm for the PLS - Two-steps farthest scheme.

Algorithm 3, where condition $|Re\{\mathbf{h}_e^i\mathbf{x}_{CI}\}| > |Im\{\mathbf{h}_e^i\mathbf{x}_{CI}\}|$ indicates that Eve's received constellation point is closer to the horizontal boundary region, and since this is farthest scheme, we design Eve's received signal to fall into vertical boundary region (constraint (characterized by 14)). However, if the condition is not fulfilled, we design Eve's

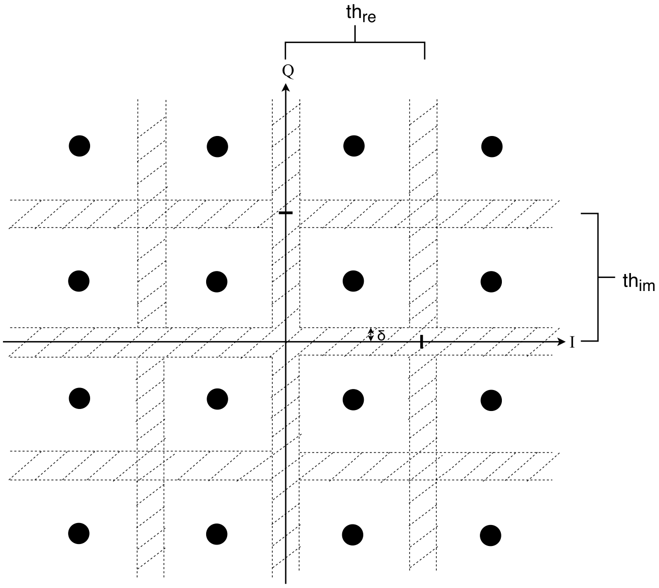


FIGURE 4. 16-QAM constellation showing the 6 lines boundary regions.

received signal to lie in the horizontal boundary region instead (represented by constraint (15)).

### 4) PLS - TWO-STEPS 6-LINES SCHEME

This scheme is also a two-step scheme, however, this particular scheme is designed for higher order modulation such as 16-QAM, where the detection regions are numerous. Fig. 4 depicts the 6-lines that define the 6 boundary regions (the region where Eve's received signal should lie) for this scheme. Namely, this scheme consist of designing Eve's received signal to lie in one of these lines by choosing the closest boundary region to it. Below we define the different constraints characterizing the 6 boundary regions:

$$Re\{\mathbf{h}_e^i\mathbf{x}\} \lesseqgtr \mp\delta, i = 1, \ldots, M \quad (18)$$

$$Re\{\mathbf{h}_e^i\mathbf{x}\} + th_{re} \lesseqgtr \mp\delta, i = 1, \ldots, M \quad (19)$$

$$Re\{\mathbf{h}_e^i\mathbf{x}\} - th_{re} \lesseqgtr \mp\delta, i = 1, \ldots, M \quad (20)$$

$$Im\{\mathbf{h}_e^i\mathbf{x}\} \lesseqgtr \mp\delta, i = 1, \ldots, M. \quad (21)$$

$$Im\{\mathbf{h}_e^i\mathbf{x}\} + th_{im} \lesseqgtr \mp\delta, i = 1, \ldots, M. \quad (22)$$

$$Im\{\mathbf{h}_e^i\mathbf{x}\} - th_{im} \lesseqgtr \mp\delta, i = 1, \ldots, M \quad (23)$$

where $th_{re}$ and $th_{im}$ denotes the threshold that determines the boundary regions of both real and imaginary parts, respectively, as depicted in Fig. (4).

Naturally, this scheme would require less power than all the aforementioned PLS schemes, considering that it introduces the smallest deviation of the constellation point. Algorithm 4 shows the details of this scheme.

We note that the above-mentioned implementations of the optimization problem in (11) are convex, and thus their global optimum can be obtained using standard convex optimization tools [39].

**Algorithm 4** PLS Scheme - Two-Steps 6 Lines

```
Input: $\mathbf{d}, \mathbf{H}, \gamma, \sigma_z^2$;                      ▷ Step 1
1: Solve problem (10)
Output: $\mathbf{x}_{CI}$
Input: $\mathbf{d}, \mathbf{H}, \mathbf{H}_e, \gamma, \sigma_z^2, \delta, \mathbf{x}_{CI}$;   ▷ Step 2
2: Do: Solve problem (11) as follows:
3:     Satisfy CI constraints in (12) and (13)
4:     Determine the closest line to $\mathbf{h}_e^i\mathbf{x}_{CI}$
5:     Apply the corresponding constraint from (18,19,20,21,22,23)
Output: $\mathbf{x}_{6l}$
```

TABLE 2. Performance of different classifiers for countermeasure SLP-based dataset.

| Classifier | Symbol detection accuracy |
|---|---|
| Support Vector Machines | 0.28 |
| Gradient Boosting Machine | 0.3 |
| Logistic Regression | 0.28 |
| K-Nearest Neighbors | 0.26 |
| XGBoost | 0.28 |
| Light GBM | 0.27 |

### C. ATTACK EXAMPLE ON PLS SCHEME

As demonstrated in Section III-D, a sophisticated eavesdropper that employs ML can predict a precoded signal to a user with high accuracy. However, in the case of the PLS scheme (we used Random scheme implementation in this experiment), the prediction accuracy is quite low compared to the CISPM scheme. In fact, these values are close to $\frac{1}{4}$, which is the lower bound when Eve has no side information and is randomly picking symbols out of the QPSK set. The main reason for this behavior is because we are forcing Eve's received signal to lie at the boundary region. Hence the received signal at the latter will be randomly distorted because of noise, thus making it very difficult for the ML algorithm to map the received signals to the pilot symbols. Similarly, we compared many classifiers, where their prediction accuracy is summarised in Table 2.

## V. NUMERICAL RESULTS

In the numerical results, we define the considered performance metrics. First, the total transmit power by the BS antennas is defined as $P_{tot} = ||\mathbf{x}||^2$. In the simulations, we take the average of the above quantity over a large number of symbol slots, i.e., $\mathbb{E}_{\mathbf{d}_n,\mathbf{H}}[P_{tot}]$, to obtain the frame-level total transmit power, which is then averaged over a large number of channel realizations. We also compute the effective BER at the Eve, by detecting the received signal at the latter. In addition, we compute the BER at the intended users in order to investigate the impact of the countermeasure scheme on the intended user performance.

Consequently, we define the metric that we call effective rate, $\overline{R}_a$, that quantifies the error-free part of the total rate, and can be written as in [26] as

$$\overline{R}_a = WR_c(1 - BER_a) \quad (24)$$

where $W$ is the bandwith, $R_c$ is the rate (equals 2 in the case of QPSK), and $BER_a$ is the effective BER, where $a$ can be either intended user or Eve.

Similar to the performance metric used in [41], we define the secure rate as

$$R_{sec} = \overline{R}_{int} - \overline{R}_{eve} \tag{25}$$

where $\overline{R}_{int}$ is the effective rate at the intended user and $\overline{R}_{eve}$ is the one at the Eve.

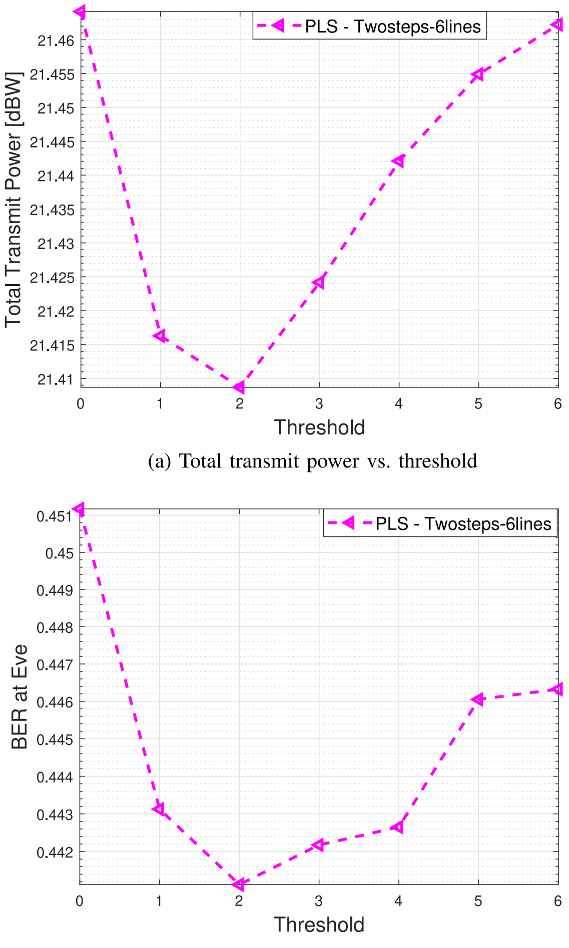
Last but not least, we define a new metric that we call Energy Efficiency for Secure Transmission (EEST) $\eta_{eest}$ that combines both the secure bits transmitted and the transmit power consumed, so it will be $[secure - bits/Joule]$, and defined as

$$\eta_{eest} = \frac{R_{sec}}{\mathbb{E}_{\mathbf{d}_n,\mathbf{H}}[P_{tot}]}. \tag{26}$$

We note that we have devised this metric to compare the overall performance of the PLS schemes, by taking into account simultaneously security and transmit power. The EEST increases either by increasing the secure rate and/or by decreasing the power consumption, and thus, higher values of it indicate either better security and/or lower power consumption. Therefore, if an $A$ scheme provides higher EEST than another scheme $B$, then scheme $A$ is providing higher security with respect to its consumed power. We note that the metric for secure transmission is the secure rate, in the numerator of the EEST, the higher the secure rate, the more secure the scheme will be. Particularly, we can observe a very high EEST that was due to very low power consumption and little security. As a result, there is no value of it that can guarantee secure transmission.

In the below figures, we used the SVM classifier for the ML-based attack as it possesses one of the highest prediction accuracies, thus making the Eve as sophisticated as possible. Moreover, all results have been averaged over 100 channel realisations and using 1000 symbols in each realizations, in order to give an accurate performance analysis of the proposed precoders. The simulated MU-MISO system comprises of $N_t = 15$ antennas at the BS, $K = 6$ single-antenna intended users, $M = \{1, 3, 6\}$ number of antennas at Eve depending on the simulation, $\sigma_z^2 = 1$, and $\sigma_e^2 = \{0, 0.2, \ldots, 1\}$ depending on the figure. MATLAB was used as the main software for simulations, embedded with CVX as the convex optimization solver. We note that since the proposed schemes and the benchmark scheme pertain to the same class of optimization convex problems, they are of comparable complexity.

For the numerical results, a value for the thresholds $th_{re}$ and $th_{im}$ has to be chosen. For that, we investigate the impact of the thresholds on both the total transmit power and the BER at Eve. We note that these threshold values are relevant only for the Two-steps 6-lines scheme, where we set $th_{re} = th_{im}$ because of the symmetry of the 16-QAM constellation. As shown in Figure 5, part (a) plots the total transmit power vs. the threshold while part (b) depicts the BER at Eve vs. the threshold.



(a) Total transmit power vs. threshold

(b) BER at Eve vs. threshold

**FIGURE 5. 16-QAM with $N_t$ = 15, $K$ = 6, 15 dB target SINR, and 1 antennas at the Eve.**

As expected, and in accordance with the SLP schemes behavior in this section, higher security (BER at Eve) comes at the cost of higher power consumption. In Fig. 5, part (a), the transmit power shows a minimum, corresponding to the position of the threshold close to the original position of the received symbols, i.e., the constraints are not too stringent, hence the consequent power saving. Before reaching this minimum, we observe a decrease of the power, due to the constraints becoming less and less strict. However, after reaching the minimum, the total power starts increasing because of constraints getting more stringent, but going in the opposite direction. As for the behavior of the BER at Eve depicted in part (b) of Fig. 5, the stricter the constraints, the more distant are the boundary regions from the original position of the received symbols, the more likely for Eve to make wrong detection decisions, hence the increase in the BER at Eve.

Finally, we have picked the value of $th_{re} = th_{im} = \frac{6}{\sqrt(2)}$ as a trade-off value between the total power consumed and

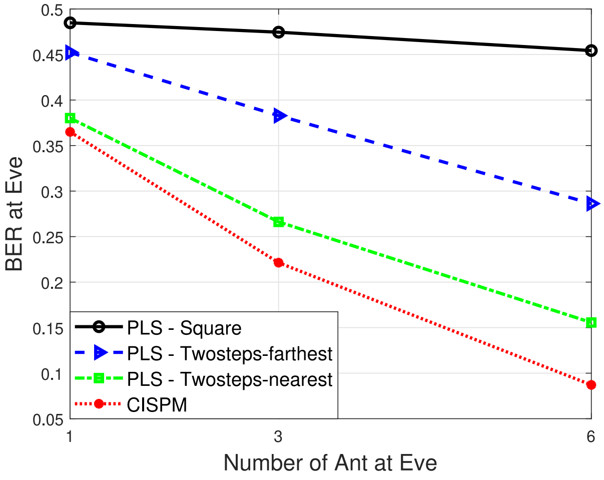


**FIGURE 6.** QPSK - BER vs. number antennas at Eve, with $N_t = 15$, $K = 6$, $\delta = 0.1$, and 10dB of target SINR at intended user.

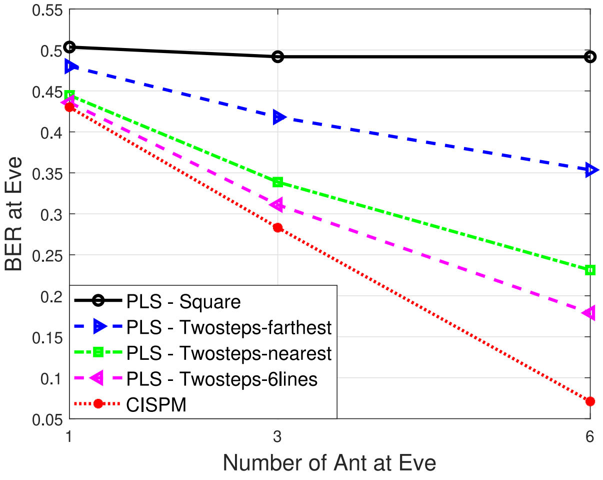


**FIGURE 7.** 16-QAM - BER vs. number antennas at Eve, with $N_t = 15$, $K = 6$, $\delta = 0.1$, $thre = th_{im} = \frac{6}{\sqrt{2}}$, and 20dB of target SINR at intended user.

security. But after all, varying the threshold barely affects the performance, as shown in Figure 5, values of transmit power and BER vary slightly with the change of the threshold. We note that the suggested fixed value of the threshold is for the selected parameters used in this section.

Fig. 6 and 7 plots the BERs at Eve as a function of the number of antennas at Eve, for case of QPSK and 16-QAM modulations, respectively. We compare the benchmark scheme (CISPM) with the PLS schemes. The parameters used in the simulation are $N_t = 15$, $K = 6$, $\delta = 0.1$, and 10dB of target SINR at intended user. In both QPSK and 16-QAM, all PLS schemes outperform the CISPM one with PLS Random providing the highest security gains. We also observe that the more antennas at Eve, the higher the prediction accuracy (more samples of same signal), and ultimately the lower the BER. However, we notice that PLS - Random scheme is not affected much by this increase in the number of antennas at Eve, and it is due to nature of this scheme, in particular, it randomly assigns Eve's received signal to either the horizontal boundary region or vertical one, and hence making it super hard for the ML engine to find a relationship, as it is practically impossible to predict something random, thus it provides the highest security. On the other hand, the other PLS schemes still provide better security gains than the CISPM one, but not as good as the Random one, mainly because in their design is inherently deterministic, hence the ML engine would often find ways to find the relationship between the observed precoded symbols and the actual symbols intended for a specific user, thus the decrease of the BER as the number of antennas at Eve increase, i.e., more training data. We also observe that in the case of 16-QAM.

Fig. 8 and 9 depicts the BERs at Eve as a function of the target SINR at the intended user, that we set to the same value for all users for simplicity, for case of QPSK and 16-QAM modulations, respectively. We compare the benchmark scheme (CISPM) with the PLS schemes. The parameters used in the simulation are $N_t = 15$, $K = 6$, $\delta = 0.1$, and 3 antennas at the Eve. Similarly, for all precoding schemes, the higher the target SINR at the intended user, the lower the BER at the Eve, except for the PLS - Random scheme, where its performance is not affected by the target SINR due it its invulnerability to ML-based attack, given the employed randomness in the design. We also observe that all PLS schemes outperform the CISPM one as they include some Eve-related constraints in their formulation, with the same behavior in both QPSK and 16-QAM.

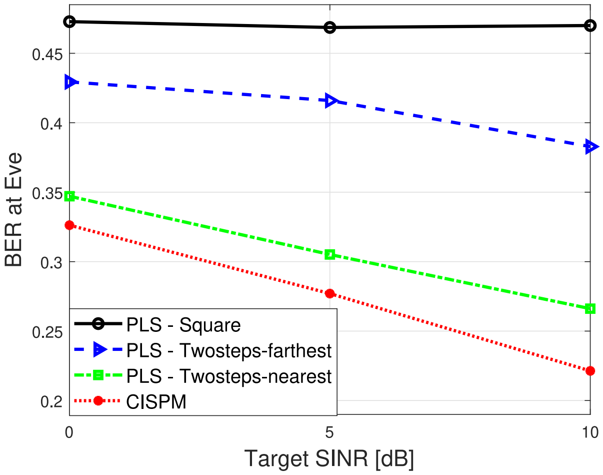


**FIGURE 8.** QPSK - BER vs. target SINR, with $N_t = 15$, $K = 6$, $\delta = 0.1$, and 3 antennas at the Eve.

Fig. 10 and 11 plots the BERs at intended user as a function of the target SINR at the intended user, that we set to the same value for all users for simplicity, for case of QPSK and 16-QAM modulations, respectively. We compare the benchmark scheme (CISPM) with the PLS schemes. The parameters used in the simulation are $N_t = 15$, $K = 6$, $\delta = 0.1$, and 3 antennas at the Eve. As expected, for all the schemes and both modulations, the BER at the intended user

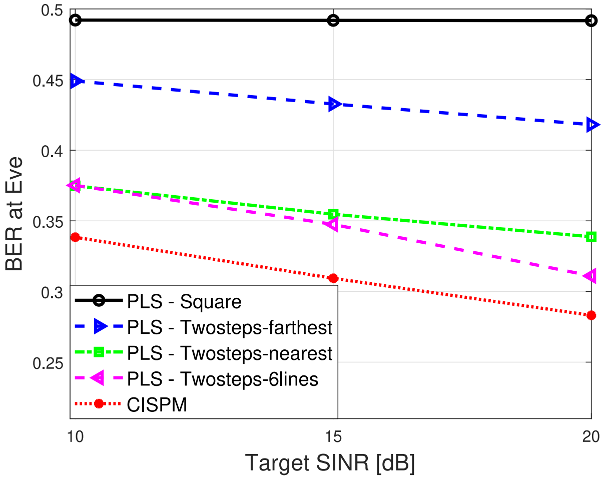


**FIGURE 9.** 16-QAM - BER vs. target SINR, with $N_t = 15$, $K = 6$, $\delta = 0.1$, $thre = th_{im} = \frac{6}{\sqrt{2}}$, and 3 antennas at the Eve.

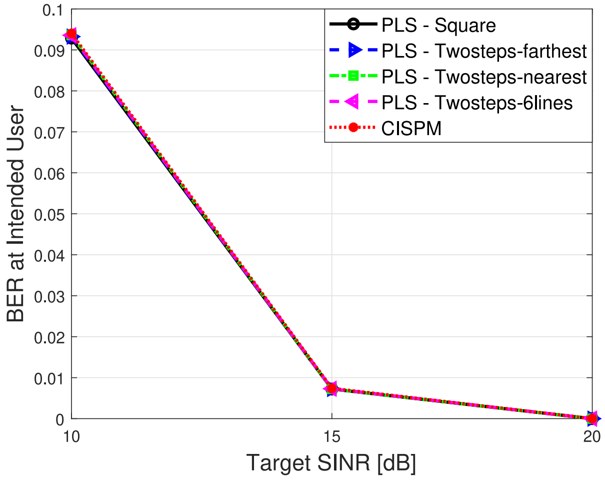


**FIGURE 11.** 16-QAM - BER at intended user vs. target SINR, with $N_t = 15$, $K = 6$, $\delta = 0.1$, $thre = th_{im} = \frac{6}{\sqrt{2}}$, and 3 antennas at the Eve.

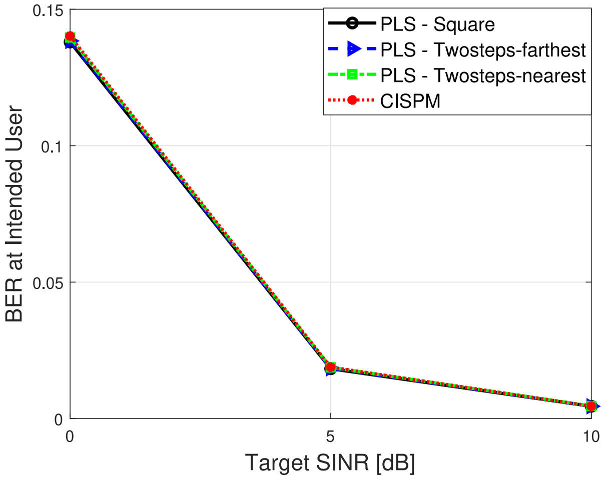


**FIGURE 10.** QPSK - BER at intended user vs. target SINR, with $N_t = 15$, $K = 6$, $\delta = 0.1$, and 3 antennas at the Eve.

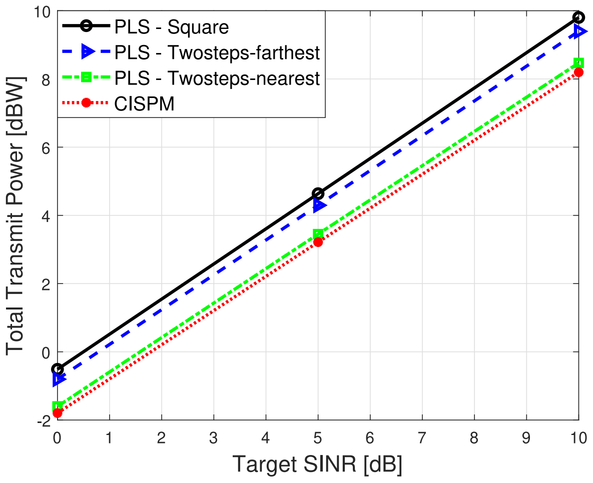


**FIGURE 12.** QPSK - Total transmit power vs. target SINR, with $N_t = 15$, $K = 6$, $\delta = 0.1$, and 3 antennas at the Eve.

decreases as the target SINR at the latter increases. Namely, higher target SINR implies higher transmit power, hence better SNR at intended, that leads to an improved BER. We also note that all the schemes have the same performance at the intended user, a match is observed among all schemes, both PLS and CISPM, consequently, we can conclude that despite the security gains offered by the PLS schemes, their use does not impact the performance at the intended user.

Fig. 12 and 13 show the total transmit power, in dBW, as a function of the target SINR, that we set to the same value for all users for simplicity, for case of QPSK and 16-QAM modulations, respectively. We compare the benchmark CISPM with the PLS schemes. The parameters used in the simulation are $N_t = 15$, $K = 6$, $\delta = 0.1$, and 3 antennas at the Eve. As expected, the power consumption increases linearly with target SINR, with benchmark scheme consuming a bit less power than the PLS ones. In particular, the PLS - Random scheme consumes more than PLS - Twosteps-farthest which consumes more than PLS - Twosteps-nearest. This is intuitive in the sense that the Twosteps-nearest consumes less than the Twosteps-farthest as it incur a smaller deviation of the target received signal. To illustrate more, this behavior is due to the fact that, the more we constrain our signal design problem, the more power is required. Moreover, the more antennas at the Eve, the higher the transmit power for the PLS schemes, i.e., number of constraints increase with the number of antennas at Eve. For 16-QAM alone, the Twosteps-6lines consuming the least among all PLS schemes, as it requires the smallest deviation of the Eve's received constellation point, i.e., it moves it to the closest line among the 6 lines (boundary regions). We also observe that the power consumption difference between the two scheme is only of 1 dB in the case of 3 antennas at Eve. Thus, only a small additional power consumption is required to provide such high security.

Fig. 14 and 15 plots the energy efficiency for secure transmission $\eta_{eest}$, in [Secure bits/Joule], as a function of

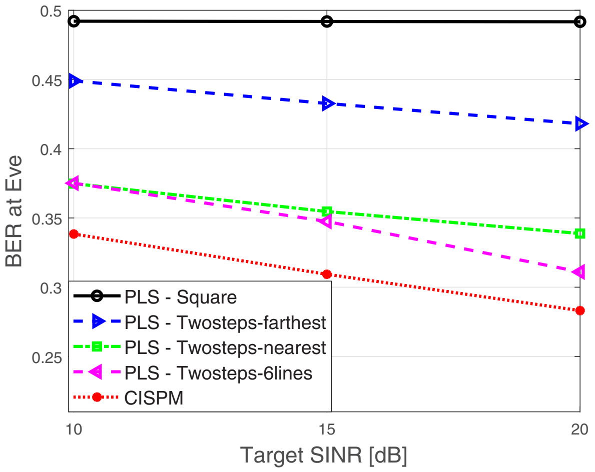


FIGURE 13. 16-QAM - Total transmit power vs. target SINR, with $N_t = 15$, $K = 6$, $\delta = 0.1$, $th_{re} = th_{im} = \frac{6}{\sqrt{2}}$, and 3 antennas at the Eve.

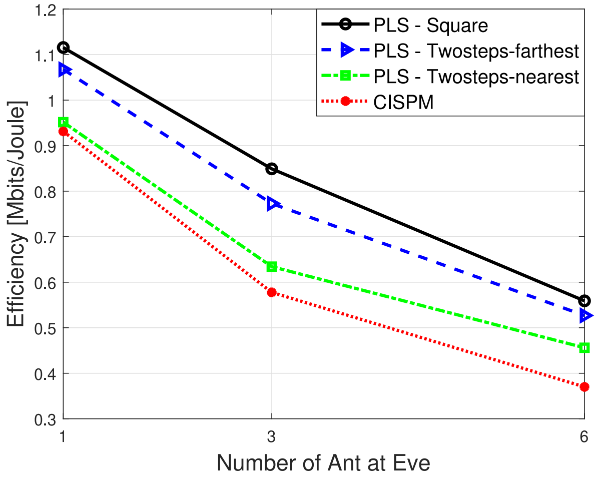


FIGURE 14. QPSK - Rate/power efficiency vs. number of antennas at Eve, with $N_t = 15$, $K = 6$, $\delta = 0.1$, and 5 dB target SINR.

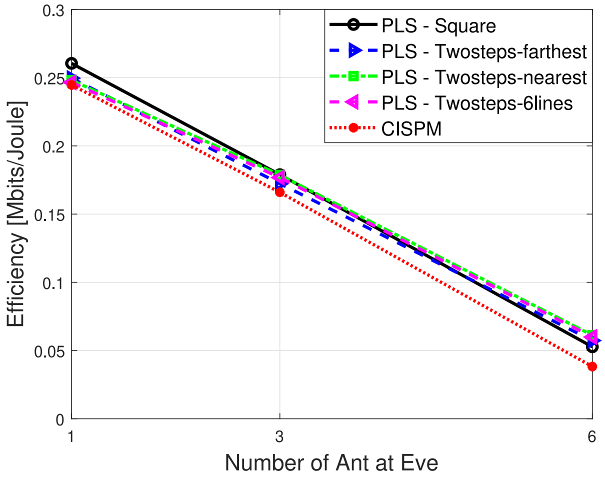


FIGURE 15. 16-QAM - Rate/power efficiency vs. number of antennas at Eve, with $N_t = 15$, $K = 6$, $\delta = 0.1$, $th_{re} = th_{im} = \frac{6}{\sqrt{2}}$, and 15 dB target SINR.

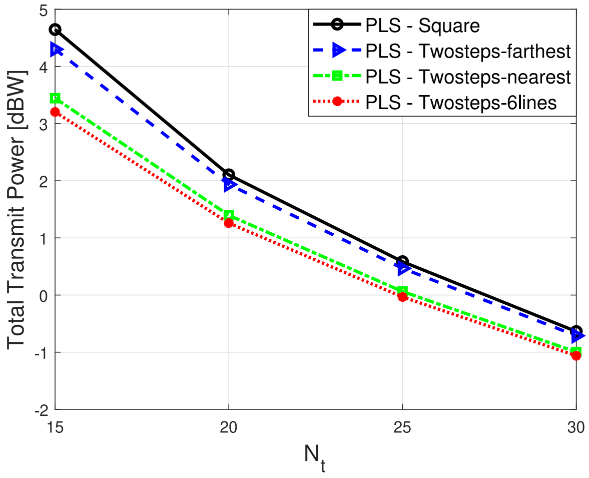


FIGURE 16. QPSK - Total transmit power vs. $N_t$, with $K = 6$, $\delta = 0.1$, 5 dB target SINR, and 3 antennas at the Eve.

the number of antennas at Eve, for case of QPSK and 16-QAM modulations, respectively. We compare the benchmark scheme with the PLS schemes. The parameters used in the simulation are $N_t = 15$, $K = 6$, $\delta = 0.1$, and 5 dB target SINR for QPSK and 15 dB for 16-QAM. In the case of QPSK, Fig. 10, it turns out that, when taking into account both total transmit power and secure rate, PLS schemes still outperform CISPM scheme. This is due to the fact that the difference in power consumption is relatively smaller than the difference in secure bits, hence keeping the same ranking, with PLS Random scheme providing the highest efficiency. For 16-QAM on the other hand, we see the same pattern when Eve has 1 antennas, however, as the number of antennas at Eve increases, the ranking among PLS schemes changes accordingly, and this is due to the difference in power consumption that becomes relatively higher than the difference in secure rate, thus the change in the ranking. Despite this small change in ranking among PLS schemes, PLS schemes still outperform CISPM scheme in all the cases.

Fig. 16 and 17 depicts the total transmit power, in dBW, as a function of the number of antennas $N_t$, for a fixed target SINR of 5 dB for QPSK and 15 dB for 16-QAM, respectively. We compare the CISPM scheme with the PLS schemes. The parameters used in the simulation are $N_t = 15$, $K = 6$, $\delta = 0.1$, and 3 antennas at the Eve. We observe that, for all the schemes, the power consumption decreases with the number of antennas. Namely, increasing the number of antennas, Nt, leads to higher power gains at the receivers, hence the less required power by the transmitter. In other words, increasing $N_t$ leads to stronger inter-user interference, hence higher power gains. Similarly to Fig. 8 and 9, PLS schemes consumes more power than CISPM scheme, where increasing the number of antennas at Eve leads to even higher power consumption, i.e., more antennas at Eve imply more constraints given that the constraints are applied on a per-antenna basis, hence the more power required.

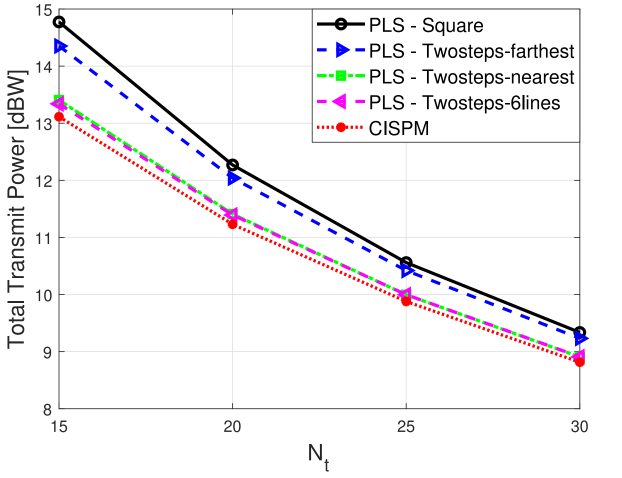


**FIGURE 17.** 16-QAM - Total transmit power vs. $N_t$, with $K = 6$, $\delta = 0.1$, 15 dB target SINR, $thre = th_{im} = \frac{6}{\sqrt{2}}$, and 3 antennas at the Eve.

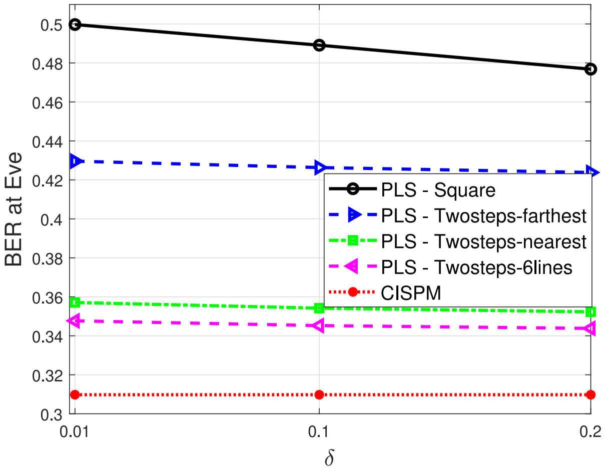


**FIGURE 19.** 16-QAM - BER vs. $\delta$, with $N_t = 15$, $K = 6$, 15 dB target SINR, $thre = th_{im} = \frac{6}{\sqrt{2}}$, and 3 antennas at the Eve.

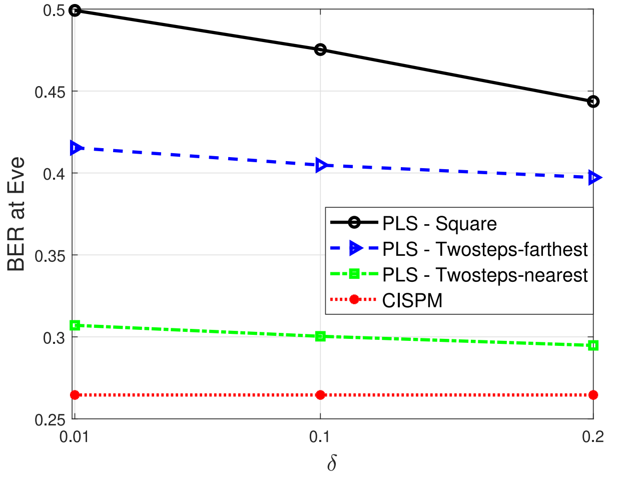


**FIGURE 18.** QPSK - BER vs. $\delta$, with $N_t = 15$, $K = 6$, 5 dB target SINR, and 3 antennas at the Eve.

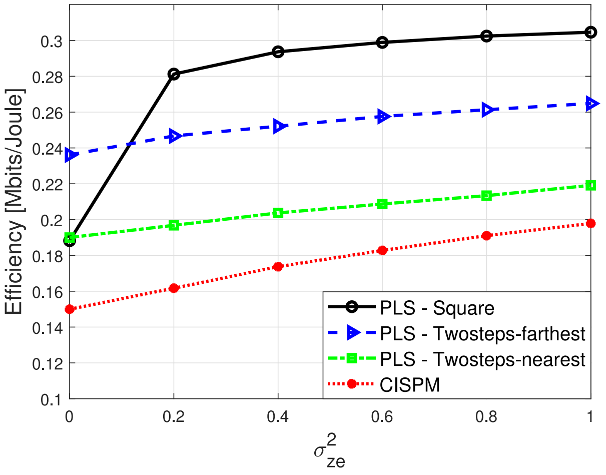


**FIGURE 20.** QPSK - Rate/power efficiency vs. $\sigma^2_{ze}$, with $N_t = 15$, $K = 6$, $\delta = 0.1$, 10 dB target SINR, and 3 antennas at the Eve.

Fig. 18 and 19 represent the BER at Eve, as a function of $\delta$, for a fixed target SINR of 5 dB for case of QPSK and 15 dB for 16-QAM, respectively. We compare the CISPM scheme with the PLS schemes. The parameters used in the simulation are $N_t = 15$, $K = 6$, and 3 antennas at the Eve. Similarly, PLS schemes outperform CISPM scheme, with PLS Random providing highest security gains. We observe that for all PLS schemes, the BER at Eve decreases as $\delta$ gets smaller. This can be explained intuitively as follows. The larger the $\delta$, the thicker the boundary region, hence the more chances for constellations points to fall into a deeper position inside the detection region, in this case, noise will have a smaller chance on pushing this to the opposite region as opposed to the case where the boundary region is very thin, thus the smaller the $\delta$, the higher the BER (more security gains). We note that same pattern is observed for both constellations, QPSK and 16-QAM.

In all of the below results, we considered a noisy channel of Eve. In the below simulation, however, we investigate the case where Eve has different SNR levels. For instance, in the case where Eve is very close to the BS, the received signal at the later will be strong, and vice-versa in the case when Eve is far from the BS. Similarly, if Eve uses sophisticated radio-frequency (RF) hardware, then the noise variance at the latter might be negligible.

Fig. 20 and 21 plots the energy efficiency for secure transmission $\eta_{eest}$, in [Secure bits/Joule], as a function of the noise variance at Eve $\sigma^2_{ze}$, for the case of QPSK and 16-QAM modulations, respectively. We compare the benchmark scheme with the PLS schemes. The parameters used in the simulation are $N_t = 15$, $K = 6$, $\delta = 0.1$, and 10 dB target SINR for QPSK and 20 dB for 16-QAM. It turns out that in the case where Eve has almost noiseless receive signal, the PLS - two-step-farthest scheme outperforms the PLS - Square scheme in both BER and $\eta_{eest}$, and even consumes less power. This behavior can be explained in the sense that the boundary schemes strength lies in the assumption that the noise at Eve would push it to either detection regions

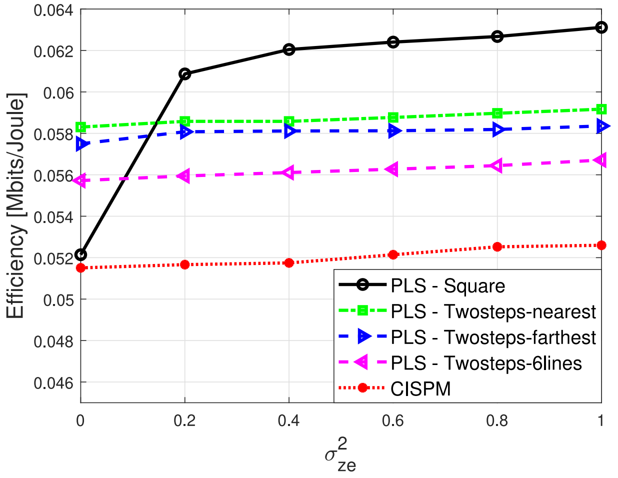


**FIGURE 21.** QAM-16 - Rate/power efficiency vs. $\sigma^2_{ze}$, with $N_t = 15$, $K = 6$, $\delta = 0.1$, 20 dB target SINR, and 3 antennas at the Eve.

with almost equal probability, therefore in the case of noiseless Eve, noise is no longer there to move the receive signal, and by design the PLS - two-step-farthest scheme feasible region is bigger than the PLS - Square scheme, therefore it is harder for the ML algorithm to track the Two-steps-farthest than the Square scheme. However, in the case of noisy Eve, the Square scheme performs better in BER and $\eta_{eest}$ because noise will push it not only to the opposite detection region but also the other neighbouring ones, hence the increase in security. Concurrently, in all schemes we observe that $\eta_{eest}$ increases with the increase of $\sigma^2_{ze}$ as a result of noise moving the received signals. More noise makes it harder for the ML algorithm to track the mapping, hence the higher BER at Eve and consequently higher $\eta_{eest}$.

## VI. CONCLUSION

In this paper, we proposed a new ML-based attack that permits a sophisticated eavesdropper to detect a message in a downlink MU-MISO system with a decent accuracy. The Eve learns patterns from the sent precoded pilots and predicts data symbols accordingly, where this sophisticated Eve employs several antennas and has ability to detect multi-level modulation schemes. We showed that this vulnerability is valid even when conventional SLP based precoding is employed. Still, these conventional precoders, such as CISPM scheme, have the advantage of not requiring the knowledge of Eve's channel. As a countermeasure to this attack, we propose novel SLP-based precoders. In general, the Square scheme provides the highest security gains and also computationally wise, it consumes almost half of the computation time than the other two-steps schemes, however it consumes the highest transmit power. However, as shown in the numerical results, depending on the modulation used, the number of antennas at Eve and the noise power at the latter, both Two-steps-farthest and nearest can outperform the Square scheme. Therefore, the proposed PLS schemes provide different tradeoffs between security, computation time, and transmit power, which would give the BS options to choose the most suitable scheme depending on level of security required and/or transmit power needed and parameters used. Notably, despite all the security gains offered by the PLS schemes, their use does not affect the performance at the intended user. Numerical results validate both the attack as well as the countermeasures, where the proposed PLS precoders achieve drastic security gains at the expense of only a small additional power consumption at the transmitter. Future research topics would be to extend this work to the case of non-perfect CSI and also where the channel to the Eve is unknown to the BS.

## REFERENCES

[1] I. Parvez, A. Rahmati, I. Guvenc, A. I. Sarwat, and H. Dai, "A survey on low latency towards 5G: RAN, core network and caching solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3098–3130, 4th Quart., 2018.

[2] Cisco VNI Forecast, "Cisco visual networking index: Forecast and trends, 2017–2022," San Jose, CA, USA, Cisco Public Inf., White Paper, Feb. 2019.

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

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

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[6] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[7] S. Asaad, A. Bereyhi, A. M. Rabiei, R. R. Müller, and R. F. Schaefer, "Optimal transmit antenna selection for massive MIMO wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 817–828, Apr. 2018.

[8] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[9] A. Subramanian, A. Thangaraj, M. Bloch, and S. W. McLaughlin, "Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 585–594, Sep. 2011.

[10] D. Chen, N. Zhang, N. Cheng, K. Zhang, Z. Qin, and X. S. Shen, "Physical layer based message authentication with secure channel codes," *IEEE Trans. Depend. Secure Comput.*, early access, Jun. 12, 2018, doi: 10.1109/TDSC.2018.2846258.

[11] D. Chen, N. Zhang, R. Lu, N. Cheng, K. Zhang, and Z. Qin, "Channel precoding based message authentication in wireless networks: Challenges and solutions," *IEEE Netw.*, vol. 33, no. 1, pp. 99–105, Jan./Feb. 2019.

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

[13] A. Mayouche, D. Spano, C. G. Tsinos, S. Chatzinotas, and B. Ottersten, "Machine learning assisted PHYSEC attacks and SLP countermeasures for multi-antenna downlink systems," in *Proc. IEEE Global Comm. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[14] Q. Xu, P. Ren, and A. L. Swindlehurst, "Rethinking secure precoding via interference exploitation: A smart eavesdropper perspective," 2019. [Online]. Available: arXiv:1908.03174.

[15] T. 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, Mar. 2006.

[16] W. Yu and T. Lan, "Transmitter optimization for the multi-antenna downlink with per-antenna power constraints," *IEEE Trans. Signal Process.*, vol. 55, no. 6, pp. 2646–2660, Jun. 2007.

[17] G. Dartmann, X. Gong, W. Afzal, and G. Ascheid, "On the duality of the max–min beamforming problem with per-antenna and per-antenna-array power constraints," *IEEE Trans. Veh. Technol.*, vol. 62, no. 2, pp. 606–619, Feb. 2013.

[18] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt, "Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels," *IEEE Trans. Signal Process.*, vol. 52, no. 2, pp. 461–471, Feb. 2004.

[19] M. Alodeh *et al.*, "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, 3rd Quart., 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] C. Masouros, "Correlation rotation linear precoding for MIMO broadcast communications," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 252–262, Jan. 2011.

[22] M. Alodeh, S. Chatzinotas, and B. Ottersten, "Symbol-level multiuser MISO precoding for multi-level adaptive modulation," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 5511–5524, Aug. 2017.

[23] D. Kwon, W.-Y. Yeo, and D. K. Kim, "A new precoding scheme for constructive superposition of interfering signals in multiuser MIMO systems," *IEEE Commun. Lett.*, vol. 18, no. 11, pp. 2047–2050, Nov. 2014.

[24] P. V. Amadori and C. Masouros, "Constant envelope precoding by interference exploitation in phase shift keying-modulated multiuser transmission," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 538–550, Jan. 2017.

[25] M. Alodeh, S. Chatzinotas, and B. Ottersten, "Energy-efficient symbol-level precoding in multiuser MISO based on relaxed detection region," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 3755–3767, May 2016.

[26] C. G. Tsinos, S. Domouchtsidis, S. Chatzinotas, and B. Ottersten, "Symbol level precoding with low resolution DACs for constant envelope OFDM MU-MIMO systems," *IEEE Access*, vol. 8, pp. 12856–12866, 2020.

[27] 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.

[28] M. R. A. Khandaker, C. Masouros, and K.-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, Sep. 2018.

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

[30] M. Chen, U. Challita, W. Saad, C. Yin, and M. Debbah, "Artificial neural networks-based machine learning for wireless networks: A tutorial," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3039–3071, 4th Quart., 2019.

[31] M. Min *et al.*, "Learning-based privacy-aware offloading for healthcare IoT with energy harvesting," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4307–4316, Jun. 2019.

[32] T. O'Shea and J. Hoydis, "An introduction to deep learning for the physical layer," *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no. 4, pp. 563–575, Dec. 2017.

[33] M. Z. Hameed, A. Gyorgy, and D. Gunduz, "Communication without interception: Defense against deep-learning-based modulation detection," 2019. [Online]. Available: arXiv:1902.10674.

[34] 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*, early access, Oct. 4, 2019, doi: 10.1109/TIFS.2019.2945619.

[35] R. Fritschek, R. F. Schaefer, and G. Wunder, "Deep learning for the Gaussian wiretap channel," 2018. [Online]. Available: arXiv:1810.12655.

[36] D. Spano, M. Alodeh, S. Chatzinotas, and B. Ottersten, "Symbol-level precoding for the nonlinear multiuser MISO downlink channel," *IEEE Trans. Signal Process.*, vol. 66, no. 5, pp. 1331–1345, Mar. 2018.

[37] 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.

[38] S. Shalev-Shwartz and S. Ben-David, *Understanding Machine Learning: From Theory to Algorithms*. Cambridge, U.K.: Cambridge Univ. Press, 2014.

[39] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[40] L. Deng, "A tutorial survey of architectures, algorithms, and applications for deep learning," *APSIPA Trans. Signal Inf. Process.*, vol. 3, Jan. 2014.

[41] J. Krivochiza, J. M. 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. 15509–15520, 2019.