A Product Channel Attack to Wireless Physical Layer Security

Gonzalo J. Anaya-Lopez, Gerardo Gomez and F. Javier Lopez-Martinez

***Abstract*—We propose a novel attack that compromises the physical layer security of downlink (DL) communications in wireless systems. This technique is based on the transmission of a slowly-varying random symbol by the eavesdropper during its uplink transmission, so that the equivalent fading channel observed at the base station (BS) has a larger variance. Then, the BS designs the secure DL transmission under the assumption that the eavesdropper's channel experiences a larger fading severity than in reality. We show that this approach can lead the BS to transmit to Bob at a rate larger than the secrecy capacity, thus compromising the system secure operation. Our analytical results, corroborated by simulations, show that the use of multiple antennas at the BS may partially alleviate but not immunize against these type of attacks.**

***Index Terms*—Attacks, fading, physical layer security, secrecy capacity, wireless security.**

I. Introduction

During the last decade, the research on wireless security has experienced a paradigm-shift due to the advent of physical layer security (PLS) techniques. Even though the broadcast nature of wireless transmission could be thought to be detrimental for security, the seminal works in [1, 2] paved the way to leverage the random nature of wireless channels to provide information-theoretic security to communications in the presence of eavesdroppers. Similarly to conventional techniques for security provision in higher layers, PLS in wireless environments is also sensitive to attacks, with the ultimate goal of precluding a secure communication between the legitimate peers Alice and Bob.

In addition to malicious jamming [3], which affects the ability of Alice to acquire the channel state information (CSI) from Bob (thus degrading the achievable secure rate), there are other approaches proposed in the literature to perform attacks from a PLS perspective. For instance, in massive multiple-input multiple-output (MIMO) contexts, a pilot-contamination attack can be used to influence the base station's beamforming design [4]. In this strategy, usually referred to as *pilot spoofing* [5], an eavesdropper (Eve) transmits the same pilot sequence as Bob's during the uplink training phase, in a perfectly synchronized fashion. By doing so, the equivalent channel for the eavesdropper improves as the number of antennas is increased, which causes the secrecy capacity not to be increased as the number of antennas grows.

In this work, we propose a new type of attack aimed at compromising the physical layer security in scenarios on which the potential eavesdroppers are system agents; this is the case, for instance, of wireless communication systems served by a base station (BS). In our scheme, the eavesdropper designs its uplink (UL) transmission in a way that the equivalent channel observed by the BS is the product[1] of the actual fading and a slowly-varying random sequence – i.e, a *synthetic* fading coefficient. By doing so, the BS designs its downlink (DL) transmission to the legitimate user under the premise that the eavesdropper experiences a more severe fading than the actual one, thus choosing a secrecy rate larger than the *true* secrecy capacity. The efectiveness of this technique is verified both theoretically and by simulation, showing that multiple antennas at the BS does not suffice to improve robustness against the attack.

This strategy differs from the random beamforming or artificial fast fading scheme in [6] in several aspects: (*a*) our scheme is intended to operate in scenarios on which Eve is a part of the system, so that Eve's CSI is available at Alice; (*b*) we implement the artificial *slow* fading technique at the eavesdropper's side, aiming to deceive Alice into assuming that Eve's channel has a larger variance; (*c*) the artificial fast fading proposed in [6] changes at a faster rate that the actual fading channel, so that Eve is unable to estimate the CSI; in our case, the synthetic fading generated by Eve changes at the same rate as the actual fading, so that Alice cannot separate the effects of both sources of randomness.

The remainder of this letter is organized as follows. The system model under analysis is described in Section II, and the product channel attack technique is described in Section III. The derivation of the relevant secrecy metrics are carried out in Section IV. Performance results are evaluated and discussed in Section V. Finally, we draw the main conclusions in Section VI.

II. System Model

Let us assume a wireless communication system where a BS transmits information to a set of users $\mathcal{V}$ on its coverage area. Without loss of generality, we consider that the BS is equipped with M antennas whereas users are equipped with single-antenna devices. We assume that the system operates

Manuscript received May xx, 2020; revised XXX. This work has been funded by the Spanish Government and the European Fund for Regional Development FEDER (projects TEC2016-80090-C2-1-R and TEC2017-87913-R), by Junta de Andalucia (project P18-RT-3175, TETRA5G) and by University of Málaga. The review of this paper was coordinated by XXXX.

The authors are with Departmento de Ingenieria de Comunicaciones, Universidad de Malaga - Campus de Excelencia Internacional Andalucia Tech., Malaga 29071, Spain (e-mail: {gjal, ggomez, fjlopezm}@ic.uma.es).

Digital Object Identifier 10.1109/XXX.2020.XXXXXXX

[1]Hence, we propose the term *product channel attack* to denote this technique.

on a time-division duplexing (TDD) mode, so that CSI for each user can be estimated during the UL transmission phase. We consider that all radio channels are subject to independent quasi-static Rayleigh fading, and remain constant along the transmission of each codeword.

The BS operates in two modes for DL transmission, referred to as *standard* and *secure* modes. Under *standard* operation, the BS beamforms a set of messages z_v with $\mathbb{E}\{|z_v|^2\} = 1$ and $v \in \mathcal{V}$ to each intended user through a maximal ratio transmission (MRT) scheme [7]. Under *secure* operation, the BS wishes to establish a secure communication with a legitimate user $v_{\rm i} = {\rm B}$, now assuming that a (different) illegitimate user $v_{\rm j} = {\rm E}$ aims to eavesdrop the communication.

During the UL phase, the signal received by the BS at the i-th receive antenna can be expressed as:

$$y_u^{(i)} = \sqrt{P_u L_u} x_u h_u^{(i)} + n^{(i)}, \tag{1}$$

where now $u = \{{\rm B}, {\rm E}\}$ is used to denote the parameters corresponding to the transmission from the legitimate (B) or eavesdropper (E) users, respectively. The transmitted symbols x_u are normalized so that $\mathbb{E}\{|x_u|^2\} = 1$; P_u represents the transmission power for user u; L_u is the path loss measured at a reference distance R_u, computed as $R_u^{-\alpha}$, where α is the path-loss exponent; and the channel coefficients $h_u^{(i)}$ are circularly symmetric complex Gaussian random variables with $\mathbb{E}\{|h_u^{(i)}|^2\} = 1$. Finally, $n^{(i)}$ represents the additive white Gaussian noise (AWGN) samples at the i-th receive antenna. We assume that the BS is able to perfectly estimate all the channel coefficients $h_u^{(i)}$, in order to recover the UL messages, as well as to use such CSI to design the DL transmission.

During the DL transmission in secure mode, the BS beamforms the message $z_{\rm B}$ with $\mathbb{E}\{|z_{\rm B}|^2\} = 1$ through a MRT scheme [7]. In this case, the beamforming vector $\mathbf{w}_{\rm B} \in \mathbb{C}^{M\times 1}$ is adapted to Bob's instantaneous channel; using the notation in [8], we have $\mathbf{w}_{\rm B}^{\mathcal{H}} = \frac{\mathbf{h}_{\rm B}^{\mathcal{H}}}{||\mathbf{h}_{\rm B}||} = \frac{[h_{\rm B}^{(1)},\ldots,h_{\rm B}^{(M)}]^*}{\sqrt{\sum_{i=1}^{M}|h_{\rm B}^{(i)}|^2}}$, where $^{\mathcal{H}}$ denotes the Hermitian transpose and $\mathbf{h}_{\rm B} \in \mathbb{C}^{M\times 1}$ is the vector representation of the legitimate channel. Therefore, assuming a transmission power P_T for the BS, the signal received at Bob from the BS in the DL transmission after the MRT processing is given by

$$y_{\rm B}^{\rm MRT} = \sqrt{P_T R_{\rm B}^{-\alpha}} \underbrace{\mathbf{h}_{\rm B}^{\mathcal{H}} \mathbf{w}_{\rm B}}_{h_{\rm B}^{\rm eq}} z_{\rm B} + n_{\rm B}, \tag{2}$$

whereas the signal received at the eavesdropper is given by

$$y_{\rm E}^{\rm MRT} = \sqrt{P_T R_{\rm E}^{-\alpha}} \underbrace{\mathbf{h}_{\rm E}^{\mathcal{H}} \mathbf{w}_{\rm B}}_{h_{\rm E}^{\rm eq}} z_{\rm B} + n_{\rm E}, \tag{3}$$

where $n_{\rm B}$ and $n_{\rm E}$ are the AWGN noise components at each receiver, with $\mathbb{E}\{|n_u|^2\} = N_0$. In (2) and (3), the signal arriving at each receiver is affected by an equivalent scalar channel denoted as $h_{\rm B}^{\rm eq}$ and $h_{\rm E}^{\rm eq}$, respectively. Thanks to the MRT scheme, $|h_{\rm B}^{\rm eq}|^2$ is Gamma distributed with scale and shape parameters M and M, respectively, whereas $|h_{\rm E}^{\rm eq}|^2$ is exponentially distributed with unitary mean [9].

Hence, the instantaneous signal-to-noise ratio (SNR)s at the legitimate and eavesdropper's sides can be expressed as

$$\gamma_{\rm B} = \frac{P_T R_{\rm B}^{-\alpha}}{N_0} |h_{\rm B}^{\rm eq}|^2 |z_{\rm B}|^2 \tag{4}$$

and

$$\gamma_{\rm E} = \frac{P_T R_{\rm E}^{-\alpha}}{N_0} |h_{\rm E}^{\rm eq}|^2 |z_{\rm B}|^2, \tag{5}$$

with average SNRs $\overline{\gamma}_{\rm B} = \mathbb{E}\{\gamma_{\rm B}\} = \frac{M P_T R_{\rm B}^{-\alpha}}{N_0} = M\overline{\gamma}_0$, being $\overline{\gamma}_0$ the average SNR in the case of a single-antenna transmitter and $\overline{\gamma}_{\rm E} = \mathbb{E}\{\gamma_{\rm E}\} = \frac{P_T R_{\rm E}^{-\alpha}}{N_0}$. Note that $\overline{\gamma}_{\rm E}$ is not influenced by the number of antennas M since the beamforming vector $\mathbf{w}_{\rm B}$ is not adapted to Eve's instantaneous channel.

III. The product channel attack

As previously indicated, the BS designs its DL transmission using a MRT scheme for each user, using the CSI acquired in the UL phase. We consider that the BS transmit with constant power, and adapts the rate and coding schemes for each user in order to operate close to capacity (in *standard* mode), or to secrecy capacity (in *secure* mode). Because the BS has perfect CSI for every user in the system (including the eavesdropper E, or Eve), it is feasible to adapt the wiretap coding scheme to every realization of the fading channels. As indicated in [1], any average secrecy rate below the average secrecy capacity is achievable. Hence, the secure performance is captured by the average secrecy capacity (ASC) of the link between the legitimate peers (the BS, which plays the role of Alice, and Bob) in the presence of an eavesdropper E, defined as

$$\overline{C}_{\rm S} = \mathbb{E}\{C_{\rm S}(\gamma_{\rm B}, \gamma_{\rm E})\}, \tag{6}$$

where $\gamma_{\rm B}$ and $\gamma_{\rm E}$ denote the instantaneous SNRs at Bob and Eve, respectively, and $C_{\rm S}(\gamma_{\rm B}, \gamma_{\rm E})$ is the instantaneous secrecy capacity defined as

$$C_{\rm S}(\gamma_{\rm B}, \gamma_{\rm E}) \underset{\gamma_{\rm B}>\gamma_{\rm E}}{=} \log_2(1+\gamma_{\rm B}) - \log(1+\gamma_{\rm E}). \tag{7}$$

The physical layer security attack proposed in this work is formulated as follows: let us assume that during the UL phase the eavesdropper transmits a modified symbol $\tilde{x}_{\rm E} = x_{\rm E} \cdot \theta_{\rm E}$ with $\mathbb{E}\{|\tilde{x}_{\rm E}|^2\} = 1$. The synthetic variable $\theta_{\rm E}$ is generated so that it varies at the same rate as the actual fading channel, and multiplies Eve's UL transmission symbols and pilot sequences. In this situation, the CSI information acquired by the BS is modified as follows: the CSI estimated by the BS in the UL for Eve is now $\hat{\mathbf{h}}_{\rm E} = \theta_{\rm E}\mathbf{h}_{\rm E}$, whereas Bob's channel estimation (and hence the beamforming design) remains unaltered. Thus, the BS is deceived into thinking that the equivalent channel observed by E after MRT is now

$$\hat{h}_{\rm E}^{\rm eq} = \hat{\mathbf{h}}_{\rm E}^{\mathcal{H}} \mathbf{w}_{\rm B} = \theta_{\rm E}^* \mathbf{h}_{\rm E}^{\mathcal{H}} \mathbf{w}_{\rm B} = \theta_{\rm E}^* h_{\rm E}^{\rm eq}, \tag{8}$$

so that Eve's instantaneous SNR estimation available at the BS becomes $\hat{\gamma}_{\rm E} = |\theta_{\rm E}|^2 \gamma_{\rm E}$. However, the average SNR estimated by the BS is not modified with respect to the case on which the attack is not performed, i.e. $\hat{\overline{\gamma}}_{\rm E} = \mathbb{E}\{\hat{\gamma}_{\rm E}\} = \overline{\gamma}_{\rm E}$. Note that the average SNR is chiefly determined by the path loss due to the distance between each user and the BS, which can also

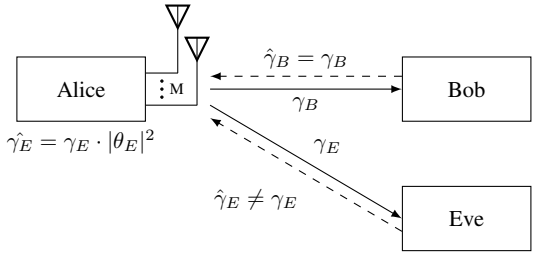

Fig. 1. CSI availability at the BS (Alice) for the system model under consideration. For simplicity, only the users of interest are represented.

be determined through timing alignment strategies. Thus, the eavesdopper avoids the risk that the BS detects an abnormal variation in the average SNR estimated from this user. With all the above considerations, the overall CSI availability at the BS can be summarized as in Fig. 1.

Now, the transmission rate from A to B is decided by A based on the SNRs $\hat{\gamma}_{\mathrm{B}}$ and $\hat{\gamma}_{\mathrm{E}}$, and the latter differs from the actual SNRs at Eve due to the fact that the attack does not affect the legitimate channel. With the CSI availability at A, the transmission rate towards B is then designed to maximize the following metric:

$$\begin{aligned} R_{\mathrm{S}}(\gamma_{\mathrm{B}}, \hat{\gamma}_{\mathrm{E}}) &\underset{\gamma_{\mathrm{B}} > \hat{\gamma}_{\mathrm{E}}}{=} C_{\mathrm{B}}(\gamma_{\mathrm{B}}) - \hat{C}_{\mathrm{E}}(\hat{\gamma}_{\mathrm{E}}) \\ &\underset{\gamma_{\mathrm{B}} > \hat{\gamma}_{\mathrm{E}}}{=} \log_2(1+\gamma_{\mathrm{B}}) - \log(1+\hat{\gamma}_{\mathrm{E}}) > 0. \end{aligned} \tag{9}$$

From the BS perspective, the metric R_{S} corresponds to the secrecy capacity of the legitimate link. However, comparing (7) and (9) it is evident that such rate does not coincide with the secrecy capacity; in the following, we will refer to R_{S} as *compromised secrecy rate*. Using the definition in (9), the average compromised secrecy rate can be computed as

$$\overline{R}_{\mathrm{S}} = \mathbb{E}\{R_{\mathrm{S}}\left(\gamma_{\mathrm{B}}, \hat{\gamma}_{\mathrm{E}}\right)\}. \tag{10}$$

Now, when the average SNR at Bob is sufficiently large, the average secrecy capacity is tightly approximated by [10]

$$\overline{C}_{\mathrm{S}} \underset{\overline{\gamma}_{\mathrm{B}} \to \infty}{\approx} \mathbb{E}\{C_{\mathrm{B}}\left(\gamma_{\mathrm{B}}\right)\} - \mathbb{E}\{C_{\mathrm{E}}\left(\gamma_{\mathrm{E}}\right)\}, \tag{11}$$

and hence, we also have that

$$\overline{R}_{\mathrm{S}} \underset{\overline{\gamma}_{\mathrm{B}} \to \infty}{\approx} \mathbb{E}\{C_{\mathrm{B}}\left(\gamma_{\mathrm{B}}\right)\} - \mathbb{E}\{\hat{C}_{\mathrm{E}}\left(\hat{\gamma}_{\mathrm{E}}\right)\}. \tag{12}$$

Because the equivalent channel $\hat{h}_{\mathrm{E}}^{\mathrm{eq}}$ has a larger variance that $h_{\mathrm{E}}^{\mathrm{eq}}$, then $\mathbb{E}\{C_{\mathrm{E}}\left(\gamma_{\mathrm{E}}\right)\} > \mathbb{E}\{\hat{C}_{\mathrm{E}}\left(\hat{\gamma}_{\mathrm{E}}\right)\}$ and hence $\overline{R}_{\mathrm{S}} > \overline{C}_{\mathrm{S}}$. Thus, when the BS considers that E is experiencing a larger fading severity than the actual one, then A is deceived into assuming that the eavesdropper channel has a lower capacity than in reality. This causes that the BS can select a rate $\overline{R}_{\mathrm{S}}$ that exceeds the secrecy capacity, which compromises physical layer security.

IV. Analytical results

We now provide analytical expressions to give mathematical support to the performance degradation due to the proposed attack. We use the formulation of the average secrecy capacity introduced in [10, eq. (29)]:

$$\overline{C}_{\mathrm{S}}(\overline{\gamma}_{\mathrm{B}}, \overline{\gamma}_{\mathrm{E}}) = \overline{C}_{\mathrm{B}}(\overline{\gamma}_{\mathrm{B}}) - \mathcal{L}\left(\overline{\gamma}_{\mathrm{B}}, \overline{\gamma}_{\mathrm{E}}\right), \tag{13}$$

where $\overline{C}_{\mathrm{B}}(\overline{\gamma}_{\mathrm{B}}) = \mathbb{E}\{C_{\mathrm{B}}\left(\gamma_{\mathrm{B}}\right)\}$ is the average capacity of the legitimate link, and the term $\mathcal{L}\left(\overline{\gamma}_{\mathrm{B}}, \overline{\gamma}_{\mathrm{E}}\right) \geq 0$ can be regarded as an average secrecy capacity loss, defined as [10, eq. (30)]:

$$\mathcal{L}\left(\overline{\gamma}_{\mathrm{B}}, \overline{\gamma}_{\mathrm{E}}\right) \triangleq \frac{1}{\log 2} \int_0^{\infty} \frac{\overline{F}_{\mathrm{E}}(x)\overline{F}_{\mathrm{B}}(x)}{1+x} dx, \tag{14}$$

where $\overline{F}_{\mathrm{B}}(\cdot)$ and $\overline{F}_{\mathrm{E}}(\cdot)$ represent the complementary cumulative distribution function (cCDF) of γ_{B} and γ_{E}, respectively, and $\log$ denotes the natural logarithm. As discussed in Section II, the legitimate SNR γ_{B} is Gamma distributed with scale parameter $\overline{\gamma}_{\mathrm{B}}$ and shape parameter M:

$$\overline{F}_{\mathrm{B}}(x) = e^{-\frac{Mx}{\overline{\gamma}_{\mathrm{B}}}} \sum_{n=0}^{M-1} \left(\frac{Mx}{\overline{\gamma}_{\mathrm{B}}}\right)^n \frac{1}{n!} \tag{15}$$

and γ_{E} is exponentially distributed with average $\overline{\gamma}_{\mathrm{E}}$. Using the cCDF of the Gamma distribution, the *true* secrecy capacity in (13) can be evaluated as

$$\overline{C}_{\mathrm{B}}\left(\overline{\gamma}_{\mathrm{B}}\right) = \frac{1}{\log 2} e^{\frac{M}{\overline{\gamma}_{\mathrm{B}}}} \sum_{n=0}^{M-1} E_{n+1}\left(\frac{M}{\overline{\gamma}_{\mathrm{B}}}\right), \tag{16}$$

where $E_m(\cdot)$ is the generalized Exponential Integral, and

$$\mathcal{L}\left(\overline{\gamma}_{\mathrm{B}}, \overline{\gamma}_{\mathrm{E}}\right) = \frac{e^{\frac{M}{\overline{\gamma}_{\mathrm{B}}} + \frac{1}{\overline{\gamma}_{\mathrm{E}}}}}{\log 2} \sum_{n=0}^{M-1} \left(\frac{M}{\overline{\gamma}_{\mathrm{B}}}\right)^n \Gamma\left(-n, \frac{M}{\overline{\gamma}_{\mathrm{B}}} + \frac{1}{\overline{\gamma}_{\mathrm{E}}}\right), \tag{17}$$

using the same procedure as in [11], where $\Gamma(\cdot,\cdot)$ is the upper incomplete Gamma function.

Analogously, the average compromised secrecy rate can be defined as:

$$\overline{R}_{\mathrm{S}}(\gamma_{\mathrm{B}}, \hat{\gamma}_{\mathrm{E}}) = \overline{C}_{\mathrm{B}}(\overline{\gamma}_{\mathrm{B}}) - \hat{\mathcal{L}}\left(\overline{\gamma}_{\mathrm{B}}, \overline{\gamma}_{\mathrm{E}}\right) \tag{18}$$

where now $\hat{\mathcal{L}}\left(\overline{\gamma}_{\mathrm{B}}, \overline{\gamma}_{\mathrm{E}}\right)$ is given by

$$\hat{\mathcal{L}}\left(\overline{\gamma}_{\mathrm{B}}, \overline{\gamma}_{\mathrm{E}}\right) \triangleq \frac{1}{\log 2} \int_0^{\infty} \frac{\overline{F}_{\hat{\mathrm{E}}}(x)\overline{F}_{\mathrm{B}}(x)}{1+x} dx, \tag{19}$$

and $\overline{F}_{\hat{\mathrm{E}}}(\cdot)$ represents the cCDF of $\hat{\gamma}_{\mathrm{E}}$. With these definitions, the condition for a successful attack (i.e., making A transmit at a larger rate than $\overline{C}_{\mathrm{S}}$) is given by

$$\mathcal{D}(\mathrm{bps/Hz}) \triangleq \mathcal{L}\left(\overline{\gamma}_{\mathrm{B}}, \overline{\gamma}_{\mathrm{E}}\right) - \hat{\mathcal{L}}\left(\overline{\gamma}_{\mathrm{B}}, \overline{\gamma}_{\mathrm{E}}\right) > 0, \tag{20}$$

which is measured in excess of bps/Hz.

The distribution of $\hat{\gamma}_{\mathrm{E}}$ is that of a composite random variable (RV) built as $\hat{\gamma}_{\mathrm{E}} = |\theta_{\mathrm{E}}|^2 \gamma_{\mathrm{E}}$, and its cCDF can be computed as

$$\overline{F}_{\hat{\mathrm{E}}}(z) = \int_0^{\infty} \overline{F}_{\mathrm{E}}\left(\frac{z}{y}\right) f_{\mathrm{y}}\left(y\right) dy, \tag{21}$$

where $f_{\mathrm{y}}\left(y\right)$ is the probability density function (PDF) of the variable $y = |\theta_{\mathrm{E}}|^2$. We will now exemplify how the choice of the distribution of the synthetic symbol θ_{E} impacts the physical layer security performance.

Let us first consider that $|\theta_{\mathrm{E}}|$ is drawn from a Rayleigh distribution, similar to the fading channel under consideration.

Hence, the power random variable $y = |\theta_{\rm E}|^2$ follows an exponential distribution with unitary power. The cCDF of $\hat{\gamma_{\rm E}}$ is therefore a special case of the distribution of the product of two Gamma random variables [12]:

$$\overline{F}_{\hat{\rm E}}^{\rm Ray}(z) = 2\sqrt{\frac{z}{\overline{\gamma}_{\rm E}}}K_1\left(\sqrt{\frac{4z}{\overline{\gamma}_{\rm E}}}\right), \tag{22}$$

where $K_1(\cdot)$ is the modified Bessel function of the second kind and first order. Plugging (22) and (15) and the well-known expression of the Gamma distribution into (19) and (18), the average compromised secrecy rate is obtained using (16) as

$$\hat{\mathcal{L}}^{\rm Ray}(\overline{\gamma}_{\rm B}, \overline{\gamma}_{\rm E}) \triangleq \frac{1}{\log 2}\int_0^\infty \frac{\overline{F}_{\hat{\rm E}}^{\rm Ray}(x)\overline{F}_{\rm B}(x)}{1+x}dx, \tag{23}$$

which can be easily evaluated numerically with standard mathematical packages.

Taking a deeper look into the assumption of $|\theta_{\rm E}|$ to be Rayleigh distributed, it could be argued that such choice would require an arbitrary instantaneous power budget at Eve's side because of the semi-infinite support for the domain of the RV $|\theta_{\rm E}|$. Hence, we also consider the case on which $|\theta_{\rm E}|$ is drawn from an uniform distribution. In this situation, the power constraint $\mathbb{E}\{|\theta_{\rm E}|^2\} = 1$ is translated into a support for the RV given by $|\theta_{\rm E}| \in [0, \sqrt{3}]$. Integrating the exponential distribution over the support of $|\theta_{\rm E}|$ using (21) yields

$$\overline{F}_{\hat{\rm E}}^{\rm Uni}(z) = e^{-\frac{z}{3\overline{\gamma}_{\rm E}}} - \sqrt{\frac{z\pi}{3\overline{\gamma}_{\rm E}}}\,\mathrm{erfc}\left(\sqrt{\frac{z}{3\overline{\gamma}_{\rm E}}}\right), \tag{24}$$

where $\mathrm{erfc}(\cdot)$ is the complementary error function. Hence, we can compute the ASC loss in this case as

$$\hat{\mathcal{L}}^{\rm Uni}(\overline{\gamma}_{\rm B}, \overline{\gamma}_{\rm E}) \triangleq \frac{1}{\log 2}\int_0^\infty \frac{\overline{F}_{\hat{\rm E}}^{\rm Uni}(x)\overline{F}_{\rm B}(x)}{1+x}dx, \tag{25}$$

respectively. Again, this ASC loss metric can be evaluated with accuracy using standard numerical integration routines. Alternatively, exponential-like approximations to the erfc function can be used to obtain approximate expressions for the ASC loss in a similar functional form as that in (17).

V. Numerical Results

We now evaluate the performance metrics introduced in the previous section for a number of scenarios of interest. In all instances, Monte Carlo (MC) simulations have been included to double-check the validity of the analytical results.

In Fig. 2, the average secrecy capacity and the average compromised secrecy rate are evaluated for different antenna configurations. The eavesdropper's SNR is set to $\overline{\gamma}_{\rm E} = 5$dB, and the synthetic symbol $|\theta_{\rm E}|$ is drawn from a Rayleigh distribution. We observe that in all instances the compromised secrecy rate $\overline{R}_{\rm S}$, which is the secrecy metric available at Alice after the attack to design the DL transmission, exceeds the *true* secrecy capacity $\overline{C}_{\rm S}$. Hence, any transmission rate within the gray-shaded area is sensitive to be decoded by the eavesdropper.

In Fig. 3, we now represent the average secrecy capacity and the average compromised secrecy rate for different values of $\overline{\gamma}_{\rm E}$. A multi-antenna transmitter with $M = 4$ and a synthetic symbol $|\theta_{\rm E}|$ now drawn from a uniform distribution are considered. We see that the difference between the compromised secrecy rate $\overline{R}_{\rm S}$ and the *true* secrecy capacity $\overline{C}_{\rm S}$ grows as $\overline{\gamma}_{\rm E}$ is increased. Hence, for a given system set-up, the attack is more harmful as Eve is closer to Alice.

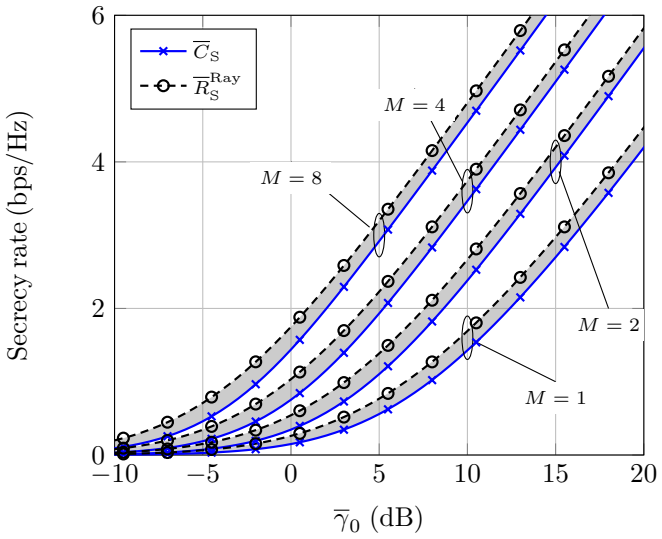

Fig. 2. Average secrecy capacity ($\overline{C}_{\rm S}$) vs. average compromised rate ($\overline{R}_{\rm S}$) as a function of $\overline{\gamma}_0$, with $\overline{\gamma}_{\rm E} = 5$ dB and $M = 1, 2, 4, 8$. Markers correspond to MC simulations.

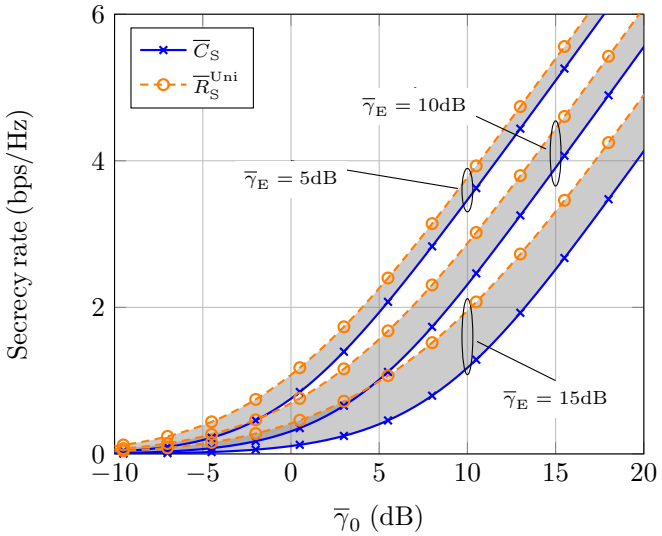

Fig. 3. Average secrecy capacity ($\overline{C}_{\rm S}$) vs. average compromised rate ($\overline{R}_{\rm S}$) as a function of $\overline{\gamma}_0$, with $M = 4$ and $\overline{\gamma}_{\rm E} = \{5, 10, 15\}$ dB. Markers correspond to MC simulations.

Finally, in Fig. 4 we evaluate the metric $\mathcal{D}$ in (20), which captures the difference between the compromised secrecy rate $\overline{R}_{\rm S}$ and the *true* secrecy capacity $\overline{C}_{\rm S}$. In this case, the x-axis now corresponds to the average SNR at Bob, i.e. $\overline{\gamma}_{\rm B}(\mathrm{d}B) = \overline{\gamma}_0(\mathrm{d}B) + 10\log_{10} M$. Hence, this means that in order to achieve a target $\overline{\gamma}_{\rm B}$ at Bob, the transmit power can be decreased by a factor of M compared to the case of using

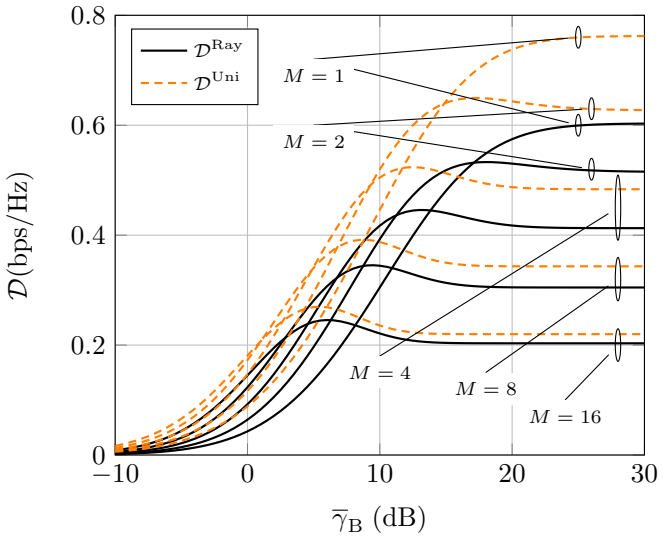

Fig. 4. Excess secrecy rate $\mathcal{D}$ as a function of $\overline{\gamma}_{\mathrm{B}}$, for different numbers of antennas and different distributions for the synthetic symbol θ_{E}; $\overline{\gamma}_{\mathrm{E}} = 15$ dB for $M = 1$ and then reduced by $10 \log_{10} M$ (dB).

a single antenna[2]. In other words, setting a fixed value of $\overline{\gamma}_{\mathrm{B}}$ ideally makes $\overline{\gamma}_{\mathrm{E}}$ to be decreased by a factor of M. We can extract several important insights from the observation of Fig. 4: (*i*) the use of a uniformly distributed synthetic symbol seems the better choice from the perspective of the eavesdropper, as it can be generated in an easier form while at the same time allowing for a larger average compromised secrecy rate; (*ii*) the use of a larger number of antennas at Alice allows for reducing $\mathcal{D}$ for high SNR at Bob, chiefly because of the effective reduction in $\overline{\gamma}_{\mathrm{E}}$ for a fixed $\overline{\gamma}_{\mathrm{B}}$; however, as previously discussed the scaling of $\overline{\gamma}_{\mathrm{B}}$ with M does not hold when the size of the antenna array grows [13]. This implies that the excess secrecy rate $\mathcal{D}$ cannot be eliminated in practice by letting $M \to \infty$; (*iii*) we see that in the low-SNR regime, increasing the number of antennas at Alice is actually detrimental since the excess secrecy rate grows in this region with M; finally, (*iv*) as $\overline{\gamma}_{\mathrm{B}}$ is increased the excess secrecy rate $\mathcal{D}$ saturates, so that no benefit is obtained by moving the legitimate user closer to Alice in terms of reducing $\mathcal{D}$. This behavior is well-explained by (11) and (12), which make $\mathcal{D}$ to depend only on the distribution of Eve's channel, i.e.

$$\mathcal{D} \underset{\overline{\gamma}_{\mathrm{B}} \to \infty}{\approx} \overline{C}_{\mathrm{E}} - \hat{\overline{C}}_{\mathrm{E}}, \tag{26}$$

where $\overline{C}_{\mathrm{E}}$ and $\hat{\overline{C}}_{\mathrm{E}}$ are the average capacity and the average rate estimated by Alice for Eve's link, respectively.

With all the previous considerations, we see that for a fixed system set-up, i.e. a given number of antennas at Alice, a fixed power budget P_T and a certain distance for the users acting as legitimate and eavesdropper agents R_{B} and R_{E}, the average compromised secrecy rate will always exceed the *true* secrecy capacity under this type of attack.

[2]We note that the scaling of $\overline{\gamma_{\mathrm{B}}}$ with M does not hold in practice for arbitrarily large M. Hence, while it is useful to analyze the behavior of antenna arrays in practice, it should not be used for asymptotic purposes as $M \to \infty$ [13].

VI. Conclusions

We presented a new type of attack against wireless physical layer security, that could affect secrecy performance in scenarios where one of the system agents acts as a potential eavesdropper. The generation by the eavesdropper on the UL phase of a synthetic symbol that varies at the same rate as the channel fading coefficients is shown to deceive the legitimate transmitter into selecting a secrecy rate that exceeds the secrecy capacity.

Since the attack becomes more effective as $\overline{\gamma}_{\mathrm{E}}$ grows, the use of secure areas in the proximity of Alice could help to partially mitigate the attack. Apart from this, the only choice for the BS is to reduce the transmission rate (ideally by the same amount as the excess secrecy rate $\mathcal{D}$) so that the actual transmission rate is below the *true* average secrecy capacity.

The proposed attack has shown to be effective even when considering eavesdroppers with the same capabilities as the legitimate agents, and without the need for using additional techniques such as jamming, multi-antenna reception or eavesdropper collusion. The impact of product channel attacks on physical layer security in more sophisticated scenarios, and the design of techniques to detect or mitigate these type of attacks seem to be interesting directions for future research activities.

References

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[2] P. K. Gopala, L. Lai, and H. El-Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[3] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Network*, vol. 27, pp. 28–33, May 2013.

[4] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag*, vol. 53, pp. 21–27, June 2015.

[5] J. K. Tugnait, "Pilot Spoofing Attack Detection and Countermeasure," *IEEE Trans. Commun.*, vol. 66, pp. 2093–2106, May 2018.

[6] H. Wang, T. Zheng, and X. Xia, "Secure MISO Wiretap Channels With Multiantenna Passive Eavesdropper: Artificial Noise vs. Artificial Fast Fading," *IEEE Trans. Wirel. Commun.*, vol. 14, pp. 94–106, Jan 2015.

[7] T. K. Lo, "Maximum ratio transmission," in *1999 IEEE International Conference on Communications (Cat. No. 99CH36311)*, vol. 2, pp. 1310–1314, IEEE, 1999.

[8] E. Björnson, M. Bengtsson, and B. Ottersten, "Optimal Multiuser Transmit Beamforming: A Difficult Problem with a Simple Solution Structure [Lecture Notes]," *IEEE Signal Process. Mag.*, vol. 31, no. 4, pp. 142–148, 2014.

[9] A. Shah and A. M. Haimovich, "Performance analysis of maximal ratio combining and comparison with optimum combining for mobile radio communications with cochannel interference," *IEEE Trans. Veh. Technol.*, vol. 49, pp. 1454–1463, July 2000.

[10] J. M. Moualeu, D. B. da Costa, F. J. Lopez-Martinez, W. Hamouda, T. M. N. Nkouatchah, and U. S. Dias, "Transmit Antenna Selection in Secure MIMO Systems Over α-μ Fading Channels," *IEEE Trans. Commun.*, vol. 67, no. 9, pp. 6483–6498, 2019.

[11] M.-S. Alouini and A. J. Goldsmith, "Capacity of Rayleigh fading channels under different adaptive transmission and diversity-combining techniques," *IEEE Trans. Veh. Technol.*, vol. 48, no. 4, pp. 1165–1181, 1999.

[12] G. K. Karagiannidis, N. C. Sagias, and P. T. Mathiopoulos, "$N*$Nakagami: A Novel Stochastic Model for Cascaded Fading Channels," *IEEE Trans. Commun.*, vol. 55, no. 8, pp. 1453–1458, 2007.

[13] E. Björnson and L. Sanguinetti, "Power scaling laws and near-field behaviors of massive MIMO and intelligent reflecting surfaces," *arXiv preprint arXiv:2002.04960*, 2020.