Profiling the Strength of Physical-Layer Security: A Study in Orthogonal Blinding

Yao Zheng
Complex Networks & Security Research Laboratory
Virginia Polytechnic Institute and State University
zhengyao@vt.edu

Matthias Schulz
Secure Mobile Networking Lab
Technische Universität Darmstadt
mschulz@seemoo.tu-darmstadt.de

Wenjing Lou
Complex Networks & Security Research Laboratory
Virginia Polytechnic Institute and State University
wjlou@vt.edu

Y. Thomas Hou
Complex Networks & Security Research Laboratory
Virginia Polytechnic Institute and State University
thou@vt.edu

Matthias Hollick
Secure Mobile Networking Lab
Technische Universität Darmstadt
mhollick@seemoo.tu-darmstadt.de

ABSTRACT

Physical layer security for wireless communication is broadly considered as a promising approach to protect data confidentiality against eavesdroppers. However, despite its ample theoretical foundation, the transition to practical implementations of physical-layer security still lacks success. A close inspection of proven vulnerable physical-layer security designs reveals that the flaws are usually overlooked when the scheme is only evaluated against an inferior, single-antenna eavesdropper. Meanwhile, the attacks exposing vulnerabilities often lack theoretical justification. To reduce the gap between theory and practice, we posit that a physical-layer security scheme must be studied under multiple adversarial models to fully grasp its security strength. In this regard, we evaluate a specific physical-layer security scheme, *i.e.* orthogonal blinding, under multiple eavesdropper settings. We further propose a practical "ciphertext-only attack" that allows eavesdroppers to recover the original message by exploiting the low entropy fields in wireless packets. By means of simulation, we are able to reduce the symbol error rate (SER) at an eavesdropper below 1% using only the eavesdropper's receiving data and a general knowledge about the format of the wireless packets.

Keywords

physical-layer security, information-theoretic security analysis, orthogonal blinding, cryptanalysis, ciphertext-only attack

WiSec'16 , July 18-22, 2016, Darmstadt, Germany
© 2016 ACM. ISBN 978-1-4503-4270-4/16/07…$15.00
DOI: http://dx.doi.org/10.1145/2939918.2939933

1. INTRODUCTION

Physical-layer security has been a long-standing security area that achieves confidentiality for data transmissions by exploiting the two fundamental characteristics of the wireless medium, which are *broadcast* and *superposition*. By stirring transmitted signals with synthesized noise, physical-layer security schemes can effectively corrupt the eavesdropper's reception and achieve secure communication in a broadcast system [1]. While theoretical study shows that this design philosophy holds a lot of promise, several practical physical-layer security schemes proposed for multiple input multiple output (MIMO) systems have been proven insecure over time. For instance, friendly jamming, proposed by Gollakota *et al.*, applying jamming techniques to prevent unauthorized access to implantable medical devices [2] or camouflage the transmission of a secret key [3], was later proven to be vulnerable when an attacker strategically places her antenna array to discern and cancel the jamming signals [4, 5]. Another example is orthogonal blinding [6], proposed by Anand *et al.*, which thwarts a eavesdropper by injecting artificial noise into channels orthogonal to the intended receiver's channels. The scheme was recently shown to be vulnerable against a multi-antenna eavesdropper with capabilities similar to those of the transmitter [7, 8]. In [7], the eavesdropper attacks orthogonal blinding by training an adaptive filter through known data symbols to separate transmitted signals from artificial noise.

The swift development of attack methods toward physical-layer security schemes has raised concerns about its practicality. The reasons behind those prompt attack methods are usually tri-fold: (1) The actual secrecy rate attained by a physical-layer security scheme can be significantly lower than the secrecy capacity of the MIMO wire-tap channel, and may depend on the MIMO configurations of the transmitter, the receiver, and the eavesdropper. (2) The evaluation of a physical-layer security scheme has been focusing on a single-antenna eavesdropper [3, 6] due to technology constrains, which lead to inconclusive results. For instance, in [6], the scheme considers the eavesdropper to be limited by singular antenna methods due to constrains of mobile devices. (3) While the assumption of a single-antenna eavesdropper might be realistic in the past, the rapid advancement of MIMO technology quickly obviates such an assumption by increasing the number of antennas for average devices.

To that end, we argue that physical-layer security schemes must be scrutinized under multiple MIMO configurations in order to gain comprehensive insights about their security strength and lifespan as the technology progresses. In this paper, we provide an extensive evaluation framework for physical-layer security by associating theoretical analysis with practical attack method under multiple MIMO configurations. In particular, we focus on profiling the security strength of orthogonal blinding based physical-layer security schemes. To identify vulnerabilities, we derive and compare the secrecy rates attained by orthogonal blinding under different MIMO configurations. Based on the theoretical analysis, we further present an attack showcase that allows a multi-antenna eavesdropper to effectively recover the transmitted data solely using the received signal. Our attack corresponds to the "ciphertext-only attack" model in cryptanalysis, where the eavesdropper exploits the nonuniform statistical profile of the transmitted data to infer its content.

Our results emphasize that, unlike conventional approaches such as contemporary cryptography, the level of information protection provided by a physical-layer security scheme is a dependent variable affected by practical conditions. A scheme that performs reasonably well against a single-antenna eavesdropper can have zero security incentive against a multi-antenna eavesdropper. In addition, the randomness of the input data, or the lack thereof, can deteriorate the performance of a physical-layer security scheme as well. In our case, it is the extremely regularized wireless packets that exposes a potential vulnerability of orthogonal blinding that is otherwise concealed. Our contributions in this paper are the followings:

- We provide an intuitive framework to study the security strength of orthogonal blinding based physical-layer security by comparing the secrecy capacity of the wire-tap channel with the secrecy rate attained by the scheme.

- We correlate the theoretical results with a cryptographic attack scenario, *i.e.* ciphertext-only attack. We show that the entropy contained in wireless packets is insufficient to prevent a powerful adversary from launching a brute force ciphertext-only attack toward orthogonal blinding.

- We design a practical, ciphertext-only attack scheme that allows an adversary to recover the transmitted data by exploiting the low entropy fields in wireless packets without knowing any transmitted data a priori.

- We implement our attack in MATLAB and evaluate its performance through extensive simulations.

In what follows, we show the motivation of our work by reviewing the theoretical foundation of physical-layer security in Sec. 2. In Sec. 3 we present the system model and the method of orthogonal blinding used for secure transmission. We analyze the performance of orthogonal blinding under various MIMO configurations using in Sec. 4. In Sec. 5, we channel our analysis results into a practical attack and present our ciphertext-only attack method against orthogonal blinding. We demonstrate our attack in Sec. 6. Finally, we discuss our findings in Sec. 7 and conclude in Sec. 8.

2. BACKGROUND

The theoretical foundation of physical-layer security was laid by Aaron Wyner, when he introduced the concept of the wire-tap channel [9] in 1975. In a basic wire-tap channel model, there are three terminals, one transmitter, one receiver, and one eavesdropper. The transmitter encodes a message M and broadcast it. Through the broadcast channel, the receiver and the eavesdropper observe Y and Z respectively. The goal is to exploit the channel such that the receiver can recover M from Y while the the eavesdropper cannot recover M from Z. Subsequent work extended this result to a basic Gaussian channel [10], that better models wireless communication systems. In the original framework, the channel must have two properties to permit secure communication: (1) Soundness: the error rate between transmitter and the receiver is asymptotically zero. (2) Completeness: the communication rate between the transmitter and the receiver is asymptotically zero. There two properties are formally defined by the *secrecy capacity*, which represent the maximum secrecy rate at which Alice and Bob can communicate while Eve receives an arbitrarily small amount of information.

Wyner's original treatment inspires a flourishing area of research, which studies characterizations of physical-layer security for more complex wireless communication systems. In particular, there are several works that aim to derive the secrecy capacity of a MIMO wire-tap channel by extending a basic Gaussian wire-tap channel to the case when the terminals have multiple antennas [11, 12]. One of the important result from these works is that the attainable secrecy rate can be greatly affected by the ratio of eavesdropping antennas to transmitting antennas. The result, while significant, is not widely adapted when evaluating physical-layer security schemes in practice due to its complexity.

In parallel with the theoretical research, several practical physical-layer security schemes have been proposed in the literature. An interesting family of them is based on orthogonal blinding [6], otherwise known as masked beamforming. The idea of orthogonal blinding is to simultaneously transmit the message to the intended receiver's channel while transmitting synthesized noise in the orthogonal subspace to interfere with the eavesdropper's reception. Based on empirical measurements, these schemes have been shown to be effective against a single-antenna eavesdropper. However, due to lack of evaluation under other MIMO configurations, especially in the multi-antenna eavesdropper regime, these schemes are often found to be vulnerable when facing powerful eavesdroppers. For instance, in [7, 8], Schulz *et al.* presented an attack toward [6] under an multi-antenna eavesdropper setting. In [13], Tung *et al.* showed two active, single-antenna attacks toward MIMO systems protected by orthogonal blinding.

Despite its flaws, we still find orthogonal blinding an interesting case in physical-layer security designs, due to its practical assumption about the knowledge of channel state information (CSI). Specifically, The scheme performs reasonably well against a single-antenna eavesdropper even if the sender and the receiver have no knowledge the eavesdropper's channel, a quality desirable among physical layer security schemes. In addition, the weakness of orthogonal blinding against a multi-antenna eavesdropper is representative as mobile terminals progress from singular antenna to multiple antennas. To better understand its limitations, and limitations of physical-layer security schemes in general, we see a compelling reason to study the strength and weakness of orthogonal blinding, since the notions of secure and insecure are never absolute, and vary by the capabilities of the attacker and defender. Only by determining the boundary inbetween, we can better assess the usefulness of a security method. Unlike previous work that focus on specific attack method, our study aims to provide an intuitive framework for physical-layer security that incorporates both theoretical and practical machinery.

3. SYSTEM MODEL

In this section, we describe the communication system, the channel model and the secure transmission method. Our subject to study is based on MIMO transceivers using orthogonal frequency-division multiplexing (OFDM), a prevalent wireless technology adapted in 802.11ac Wi-Fi standard [14]. Using OFDM, we can split wide-band channels into narrow sub-channels to counter the problem of intersymbol interference (ISI) and channel fading. It allow us to describe the CSI using a linear model. Through MIMO, we allow the transmitter to apply orthogonal blinding based physical-layer security to protect data transmission. Our analysis focus on the case of slow fading, where the transmitted data block is short compared to the coherence time of the fading. But the result can be extended to the case of fast fading channels.

3.1 Communication System

Consider a multi-user MIMO-OFDM system, as shown in Fig. 1, with one transmitter Alice, $\mathcal{A}$ with $n_\mathcal{A}$ antennas, one receiver Bob $\mathcal{B}$ with $m_\mathcal{B}$ antennas, and one eavesdropper Eve $\mathcal{E}$ with $m_\mathcal{E}$ antennas. Due to OFDM, the downlink CSI from Alice's j-th antenna to a receiver's i-th antenna can be characterized by a single complex number per subcarrier in the frequency domain, *i.e. channel coefficient* $H_{i,j}[k] \in \mathbb{C}$. The full CSI can be represented by a three dimensional array, $H \in \mathbb{C}^{m \times n_\mathcal{A} \times k}$, in which the third dimension represents the number of sub-channels. The CSI of the k-th sub-channel is a two dimensional matrix, $H[k] \in \mathbb{C}^{m \times n_\mathcal{A}}$. At the k-th sub-channel, the relationship between the received signal, $R[k] \in \mathbb{C}^{m \times *}$, and the transmitted signal, $D[k] \in \mathbb{C}^{n_\mathcal{A} \times *}$, can be expressed as:

$$R[k] = H[k] \cdot D[k] + \mathcal{N}, \tag{1}$$

where $\mathcal{N} \in \mathbb{C}^{m \times *}$ represents additive white Gaussian noise. A specific CSI is only valid within the channel coherence time. Beyond that, a new CSI must be estimated to abstract the channel. A common approach for Alice to obtain CSIs of each receiver is through direct feedback from the receiver. For that, Alice broadcasts well known pilot symbols to all receivers. Each receiver then divides the reception by the pre-known pilot symbols to obtain its own CSI and reports it back to the Alice. Finally, the input $D[k]$ must satisfy the power constraint

$$\mathbf{E}\left[\|d[k]\|^2\right] \leq P, \tag{2}$$

where $d[k]$ represents a column in $D[k]$.

3.2 Secure Transmission

One of the key benefits of a multi-user MIMO-OFDM system is to avoid cross-talking and eavesdropping through transmitter-side precoding. As the eavesdropper, Eve attempts to overhear the message Alice sends to Bob. If Eve is *honest*, she would faithfully report her CSI, $H_\mathcal{E} \in \mathbb{C}^{m_\mathcal{E} \times n_\mathcal{A} \times k}$, to Alice. To secretly communicate with Bob, Alice can transmit within the null-space of Eve's CSI. Specifically, Alice precodes the transmitting data using the pseudo inverse of the block matrix consisting of Bob's and Eve's CSI,

$$D[k] = \begin{pmatrix} H_\mathcal{B}[k] \\ H_\mathcal{E}[k] \end{pmatrix}^H \left(\begin{pmatrix} H_\mathcal{B}[k] \\ H_\mathcal{E}[k] \end{pmatrix} \begin{pmatrix} H_\mathcal{B}[k] \\ H_\mathcal{E}[k] \end{pmatrix}^H \right)^{-1} \begin{pmatrix} D_\mathcal{B}[k] \\ D_\mathcal{E}[k] \end{pmatrix}, \tag{3}$$

where $H_\mathcal{B} \in \mathbb{C}^{m_\mathcal{B} \times n_\mathcal{A} \times k}$, $D_\mathcal{B} \in \mathbb{C}^{m_\mathcal{B} \times * \times k}$ and $D_\mathcal{E} \in \mathbb{C}^{m_\mathcal{E} \times * \times k}$ represent Bob's CSI and the transmitted signal intended for Bob and Eve. The precoding scheme, known as zero-forcing beamforming, prohibits cross-talk by nullifying the interference caused by other concurrent transmissions.

If Eve is *dishonest*, she may choose to not report her CSI or report fake CSI to Alice. In case Eve's CSI cannot be trusted, Alice must change her communication strategy. To still achieve confidentiality, Alice transmits artificial noise, $\mathrm{AN} \in \mathbb{C}^{(n_\mathcal{A} - m_\mathcal{B}) \times * \times k}$, in the null-space of Bob's CSI to mislead Eve. For each sub-channel, Alice finds a random matrix, $H_r[k] \in \mathbb{C}^{(n_\mathcal{A} - m_\mathcal{B}) \times n_\mathcal{A}}$ that is orthonormal to $H_\mathcal{B}[k]$. To compute $H_r[k]$, Alice uses the projection matrix,

$$H_\mathcal{B}^H[k](H_\mathcal{B}[k]H_\mathcal{B}^H[k])^{-1}H_\mathcal{B}[k] \tag{4}$$

and a complex random uniform matrix, $\hat{H}_r[k] \in \mathbb{C}^{(n_\mathcal{A} - m_\mathcal{B}) \times n_\mathcal{A}}$. Alice subtracts the projected image of $\hat{H}_r[k]$ from $\hat{H}_r[k]$,

$$\hat{H}_r[k] - \hat{H}_r[k] \cdot \left(H_\mathcal{B}^H[k](H_\mathcal{B}[k]H_\mathcal{B}^H[k])^{-1}H_\mathcal{B}[k] \right) \tag{5}$$

and normalizes the result to obtain $H_r[k]$. Prior to transmitting, Alice precodes the data for Bob and artificial noise using the pseudo inverse of the block matrix consisting of $H_\mathcal{B}[k]$ and $H_r[k]$,

$$D[k] = \begin{pmatrix} H_\mathcal{B}[k] \\ H_r[k] \end{pmatrix}^H \left(\begin{pmatrix} H_\mathcal{B}[k] \\ H_r[k] \end{pmatrix} \begin{pmatrix} H_\mathcal{B}[k] \\ H_r[k] \end{pmatrix}^H \right)^{-1} \begin{pmatrix} D_\mathcal{B}[k] \\ \mathrm{AN}[k] \end{pmatrix}. \tag{6}$$

Since the artificial noise in the null-space of Bob's CSI, it degrades Eve's channel and leaves Bob's channel unaffected.

In both cases (with the honest and with the dishonest eavesdropper), the overall communication system is modeled by a wire-tap channel model

$$\begin{pmatrix} R_\mathcal{B}[k] \\ R_\mathcal{E}[k] \end{pmatrix} = \begin{pmatrix} H_\mathcal{B}[k] \\ H_\mathcal{E}[k] \end{pmatrix} \cdot D[k] + \mathcal{N}, \tag{7}$$

where the channel between Alice and Bob is the main channel, and the channel between Alice and Eve is the wire-tap channel. The linear precoding allows Alice to thwart eavesdroppers by inhibiting information leakage due to the cross-talk in a MIMO-OFDM system. Physical-layer security systems like this were proposed as an alternative or as an extension to high-layer encryption since the overhead of such an approach is small and no pre-shared secret is required. However, in Sec. 4 we show that the secrecy level of the scheme varies depending on the assumptions about Eve.

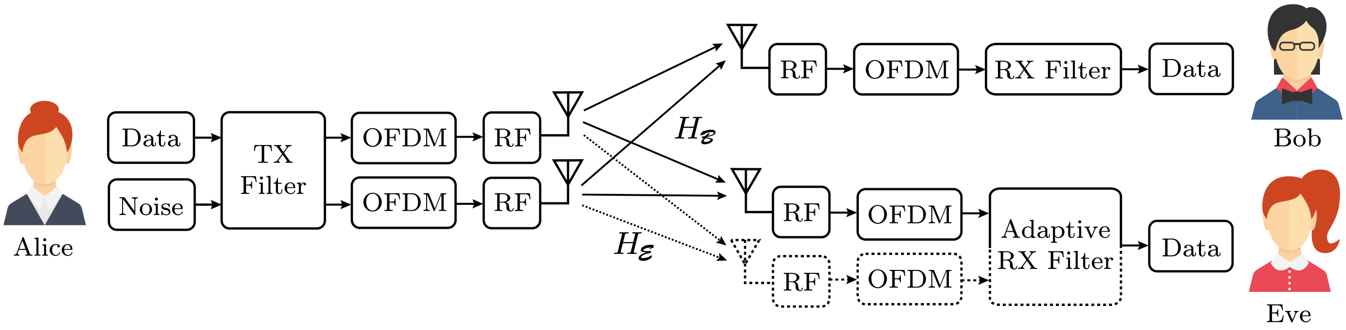

Figure 1: Our system model illustrating the transmitter Alice, the intended receiver Bob and the eavesdropper Eve.

4. SECURITY PROFILING

Here we present a comprehensive security evaluation of orthogonal blinding under different MIMO configurations. For convenience, we restrict our attention to two typical cases: (1) *inferior eavesdropper*: $m_{\mathcal{B}} + m_{\mathcal{E}} < n_{\mathcal{A}}$; (2) *superior eavesdropper*: $m_{\mathcal{B}} \leq n_{\mathcal{A}} \leq m_{\mathcal{E}}$. In both cases, we consider $H_{\mathcal{B}}$, $H_{\mathcal{E}}$, and H_r to be full rank. We further categorize our result based on the eavesdropper's behavior: (1) Eve is *honest* and faithfully reports her CSI. (2) Eve is *dishonest* and chooses to not report her CSI or report fake CSI. Finally, we profile the security strength of the scheme based on the soundness and completeness of the security system. Analogous to a logical proof, we consider the system to be sound if the wire-tap channel supports secure communication, *i.e.*, it has a positive secrecy capacity. We consider the system to be complete if the communication protocol can achieve the optimal capacity. The overall analysis results are summarized in Table 1. Our result is based on a MIMO Gaussian wire-tap channel but can be extend to other channel types with orthogonal blinding.

4.1 Preliminary

Here we review properties of generalized singular value decomposition (GSVD) in preparation for our analysis. The GSVD is a matrix decomposition that simultaneously diagonalizes a pair of matrices. In particular, by applying GSVD, we can transform Eq. 7 into a diagonal form,

$$\begin{pmatrix} \tilde{R}_{\mathcal{B}}[k] \\ \tilde{R}_{\mathcal{E}}[k] \end{pmatrix} = \begin{pmatrix} \Sigma_{\mathcal{B}}[k] \\ \Sigma_{\mathcal{E}}[k] \end{pmatrix} \cdot \tilde{D}[k] + \tilde{\mathcal{N}}, \tag{8}$$

Table 1: Summary of security profiling.

	Honest	Dishonest
Eve shares ...	... correct CSI	... incorrect or no CSI
Inferior $m_{\mathcal{B}} + m_{\mathcal{E}} < n_{\mathcal{A}}$	sound; complete	unsound; incomplete
Superior $m_{\mathcal{B}} \leq n_{\mathcal{A}} \leq m_{\mathcal{E}}$	sound; incomplete	unsound; incomplete

where

$$\Sigma_{\mathcal{B}}[k] = \begin{array}{c c} & \begin{array}{ccc} q-r-s & s & r \end{array} \\ \begin{array}{c} s \\ r \end{array} & \begin{pmatrix} \mathbf{0} & \mathbf{D}_{\mathcal{B}} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} \end{pmatrix} \end{array} \tag{9}$$

$$\Sigma_{\mathcal{E}}[k] = \begin{array}{c c} & \begin{array}{ccc} q-r-s & s & r \end{array} \\ \begin{array}{c} q-r-s \\ s \end{array} & \begin{pmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{D}_{\mathcal{B}} & \mathbf{0} \end{pmatrix} \end{array}, \tag{10}$$

are two block diagonal matrices with

$$\mathbf{D}_{\mathcal{B}} = \mathrm{diag}(\alpha_1, \ldots, \alpha_s), \quad \mathbf{D}_{\mathcal{E}} = \mathrm{diag}(\beta_1, \ldots, \beta_s). \tag{11}$$

The values, q, r, and s, correspond to the dimension of the subspaces of the entire wire-tap channel, the sub-channels that go only to the Bob, and the subspaces that go to both the Bob and Eve. The generalized singular values are defined as

$$\sigma_i = \frac{\alpha_i}{\beta_i}, \quad i = 1, 2, \ldots, s. \tag{12}$$

4.2 Inferior, Honest Eavesdropper

Consider the first scenario that Eve reports her CSI honestly and is *inferior* to Alice in terms of number of antennas, *i.e.* $m_{\mathcal{B}} + m_{\mathcal{E}} < n_{\mathcal{A}}$. Since $H_{\mathcal{E}}$ is full rank, *i.e.* $\mathrm{rank}(H_{\mathcal{E}}) = m_{\mathcal{E}} < n_{\mathcal{A}}$, we have $r > 0$, $s \geq 0$[1] in Eq. 9 and Eq. 10. Hence, the sub-channels that allow Alice to securely communicate with the Bob are: (1) The r sub-channels that solely go to the Bob and (2) The subset of $s' < s$ sub-channels that go to both Bob and Eve and have σs greater than one. The wire-tap channel's secrecy capacity is positive. Because Alice has full knowledge of the channel, she can achieve the secrecy capacity by transmitting through the top $m_{\mathcal{B}}$ of the $r + s'$ viable sub-channels with proper wiretap codes. The security of the system is therefore sound and complete.

4.3 Superior, Honest Eavesdropper

Consider the second scenario that Eve reports her CSI honestly and is *superior* to Alice in terms of number of antennas, *i.e.* $m_{\mathcal{B}} \leq n_{\mathcal{A}} \leq m_{\mathcal{E}}$. Observe that $\mathrm{rank}(H_{\mathcal{E}}) = n_{\mathcal{A}}$, and we have $r = 0$ and $s = m_{\mathcal{B}}$ in Eq. 9 and Eq. 10. Hence, the sub-channels that allow Alice to securely communicate with Bob are the subset of $s' < s$ sub-channels that go to

[1] Technically, we have $r \geq 0$ and $s \geq 0$. However, unless $H_{\mathcal{B}}$ is extremely unfortunate, we can assume $r > 0$.

both Bob and Eve and have σs greater than one. The wire-tap channel's secrecy capacity is not guaranteed to be positive. Formally, the secrecy capacity of this scenario is [12]

$$\sum_{j:\sigma_j \geq 1} \log \sigma_j^2, \tag{13}$$

which is only positive if

$$\sigma_{\max} > 1. \tag{14}$$

Given that Alice has full knowledge of the channel, she can achieve the secrecy capacity of the wire-tap channel by transmitting through the top $m_{\mathcal{E}}$ of the s' sub-channels with proper wiretap codes. The security of the system is therefore unsound but complete.

4.4 Inferior, Dishonest Eavesdropper

Consider the third scenario that Eve reports her CSI dishonestly and is *inferior* to Alice in terms of number of antennas, *i.e.* $m_{\mathcal{B}} + m_{\mathcal{E}} < n_{\mathcal{A}}$. The secrecy capacity of the wire-tap channel is the same as what we show in Sec. 4.2. Since Alice does not know Eve's CSI, She cannot identify the sub-channels that support secure transmission. Instead, Alice transmits artificial noise in the null space of $H_{\mathcal{B}}[k]$. It is equivalent to Alice randomly selecting $m_{\mathcal{B}}$ sub-channels from the total $r + s$ sub-channels, and hoping to avoid the ones that have σs smaller or equal to one. Obviously, Alice's choice is, in general, suboptimal. However, the probability for Alice to avoid unsuitable sub-channels is non-diminishing,

$$0 < \binom{m_{\mathcal{B}}}{m_{\mathcal{B}} + m_{\mathcal{E}}} \leq \binom{m_{\mathcal{B}}}{r + s - s'} \leq 1, \tag{15}$$

when Eve is inferior,*i.e.*,

$$m_{\mathcal{B}} \leq r + s - s' \leq m_{\mathcal{B}} + m_{\mathcal{E}}. \tag{16}$$

Hence, orthogonal blinding can guarantee that the *stochastic* secrecy loss of the wire-tap channels is at most $\binom{m_{\mathcal{B}}}{m_{\mathcal{B}}+m_{\mathcal{E}}}$ of the optimal secrecy capacity. The security of the system is therefore sound but incomplete.

4.5 Superior, Dishonest Eavesdropper

Consider the last scenario that Eve reports her CSI dishonestly and is *superior* to Alice in terms of number of antennas, *i.e.* $m_{\mathcal{B}} \leq n_{\mathcal{A}} \leq m_{\mathcal{E}}$. The secrecy capacity of the wire-tap channel is the same as what we show in Sec. 4.3. However, when Alice applies orthogonal blinding, the the probability for Alice to avoid unsuitable sub-channels can be arbitrarily close to zero,

$$0 \leq \binom{m_{\mathcal{B}}}{r + s - s'} \leq 1, \tag{17}$$

When Eve is superior, *i.e.*,

$$r + s - s' = s - s' \leq m_{\mathcal{B}}. \tag{18}$$

Therefore, Alice's choice can be arbitrarily far from optimal. The security of the system is therefore neither sound nor complete.

5. CIPHERTEXT-ONLY ATTACK

The previous information theoretic analysis give us an overall picture about the security level of the physical-layer security system against eavesdroppers with different capabilities. In particular, when facing a superior, dishonest eavesdropper, the security system is unsound and incomplete, which renders it vulnerable to various attacks. In [7], Schulz *et al.* demonstrated that the system is subject to attack analogous to a known-plaintext attack in the cryptography domain. In this work, we extend that idea and show that the system is also vulnerable to attack analogous to a ciphertext-only attack by exploiting the low entropy fields in wireless packets.

5.1 Entropy Analysis

We can compare the physical-layer security system to a cryptography system, where the transmitted data, $D_{\mathcal{B}}[k]$, equals to the plaintext, $\mathcal{M}$[2], Eve's received data, $R_{\mathcal{E}}[k]$, equals to the ciphertext, $\mathcal{C}$, and Bob's CSI, $H_{\mathcal{B}}[k]$, equals to the key, $\mathcal{K}$. By using sufficiently many antennas, Eve can effectively weaken the secure communication between Alice an Bob and be able to decode a nonvanishing fraction of any sent message. From a cryptographic perspective, it is analogous to the case when $\mathrm{H}(\mathcal{M} \mid \mathcal{C})$ is arbitrarily small, and the system is not cryptographically secure due to the nonzero mutual information between $\mathcal{C}$ and $\mathcal{M}$.

Due to the linearity of the precoding mechanism, we have

$$\mathrm{H}(\mathcal{K} \mid \mathcal{M}, \mathcal{C}) = \mathrm{H}(\mathcal{K} \mid \mathcal{C}) - \mathrm{H}(\mathcal{M} \mid \mathcal{C}) = 0.$$

Eve, therefore, can uniquely identify the key from the ciphertext if the entropy of the plaintext is low,

$$\mathrm{H}(\mathcal{K} \mid \mathcal{C}) = \mathrm{H}(\mathcal{M} \mid \mathcal{C}) \leq \mathrm{H}(\mathcal{M}).$$

Intuitively, $\mathrm{H}(\mathcal{M} \mid \mathcal{C})$ is upper bounded by $\mathrm{H}(\mathcal{M})$. Hence, a smaller $\mathrm{H}(\mathcal{M})$ decreases the unicity distance of the cryptographic system, which reduces the amount of ciphertext needed to learn the key. When Eve knows the exact plaintext, we have $\mathrm{H}(\mathcal{M}) = 0$, and the attack model reduces to a known-plaintext attack as shown in [7].

Note that this vulnerability is unique to the orthogonal blinding based physical-layer security schemes. In a strong cryptography system, the adversary should not be able to learn the key, $\mathcal{K}$, from the cyphertext, $\mathcal{C}$, even if the entropy of the plaintext, $\mathcal{M}$, is low. However, the coding method of orthogonal blinding is complete deterministic and linear, which makes it vulnerable to various cryptography attacks.

Of course, the requisite of breaking orthogonal blinding with ciphertext-only attack is the existence of some low entropy segments in the plaintext. To investigate the likeliness of low entropy data, we analyzed WiFi frames. Thereto, we captured 10^5 raw frames with a minimal length of 103 bytes using a MacBook Pro in monitor mode in our office environment. We observed up to 123 individual MAC addresses in management frames with correct FCSs. For each byte, starting at the MAC header, we calculated the entropy and divided by 8 bits/byte to get the *information efficiency.*

The results are illustrated in Fig. 2. In the MAC header (bytes 1 to 24 resp. 32 (enc.)), we observe high entropy at the sequence number field (bytes 23 to 24), medium entropy at the destination MAC address field (bytes 5 to 10) and low entropy in the beginning (vendor fields) of the transmitter and source MAC addresses (bytes 11 to 14 and 17 to 20). Those medium and low entropy fields significantly reduce

[2] In practice, $\mathcal{M}$ refers to the part of the transmitted data Eve uses to launch the attack.

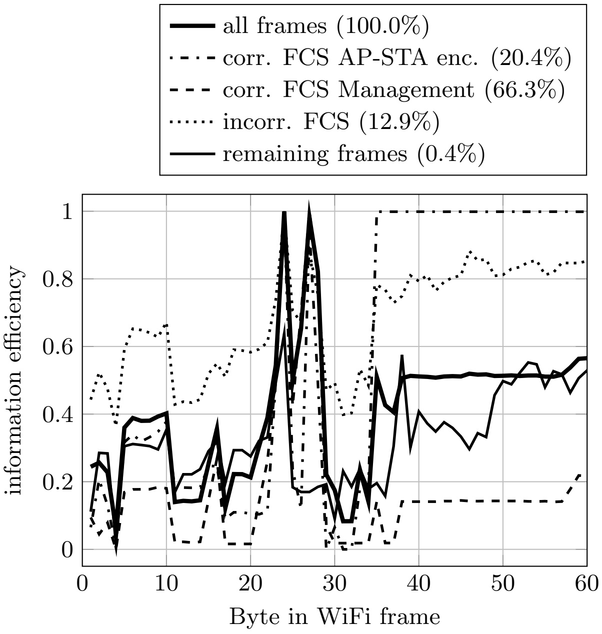

Figure 2: Information efficiency measurement for different bytes in Wi-Fi frames.

Eve's search space while training her receive filter presented in this work, while the high entropy fields are useless for us. Regarding the payload section (starting roughly at byte 36), encrypted frames offer the highest amount of entropy, while management frames have a very low entropy considering receptions with correct FCSs. In case of damaged frames, indicated by incorrect FCSs, the entropy increases which renders those frames less useful for our filter training.

5.2 Adversary Model

In [7], Schulz *et al.* present a known-plaintext attack against orthogonal blinding, in which Eve trains an adaptive filter, $F_{\mathcal{E}} \in \mathbb{C}^{m_{\mathcal{B}} \times m_{\mathcal{E}} \times k}$, using known plaintext and the corresponding ciphertext to separate the data from artificial noise,

$$\begin{pmatrix} D[k] \\ \mathrm{AN}[k] \end{pmatrix} = F_{\mathcal{E}}[k] \cdot R_{\mathcal{E}}[k].$$

The attack requires Eve to know the exact plaintext during training. Based on our analysis, we see that physical-layer security is limping when operating against superior eavesdropper and handling low entropy input. Hence, we can relax the adversary model to a ciphertext-only attack, where Eve knows only $R_{\mathcal{E}}$ and has a general knowledge about the format of the wireless packets. We shall see that, even in such a scenario, Eve can still successfully train the adaptive filter by locating the low entropy fields in the unknown plaintext.

5.3 Attack Algorithm

Here we present how Eve can launch the ciphertext-only attack by formulating and solving an optimization problem. From our previous entropy analysis, we see that the transmitted data is bound to have low entropy fields either in the header of the physical-layer or in the headers of the higher layers. In particular, consider that the transmitted data can be divided into three parts

$$D_{\mathcal{B}}[k] = \begin{pmatrix} \overleftarrow{D}_{\mathcal{B}}[k] & \bar{D}_{\mathcal{B}}[k] & \overrightarrow{D}_{\mathcal{B}}[k] \end{pmatrix},$$

where $\overleftarrow{D}_{\mathcal{B}}[k]$ and $\bar{D}_{\mathcal{B}}[k]$ contain low entropy, and $\overrightarrow{D}_{\mathcal{B}}[k]$ contains high entropy. In practice, $\overleftarrow{D}_{\mathcal{B}}[k]$ and $\bar{D}_{\mathcal{B}}[k]$ represents the low entropy fields in various headers, and $\overrightarrow{D}_{\mathcal{B}}[k]$ represents the payload. The three-way partition is analogous to the training, validating and testing set in machine learning. Correspondingly, Eve's reception can be divided into three parts,

$$R_{\mathcal{E}}[k] = \begin{pmatrix} \overleftarrow{R}_{\mathcal{E}}[k] & \bar{R}_{\mathcal{E}}[k] & \overrightarrow{R}_{\mathcal{E}}[k] \end{pmatrix},$$

where $\overleftarrow{R}_{\mathcal{E}}[k]$, $\bar{R}_{\mathcal{E}}[k]$, and $\overrightarrow{R}_{\mathcal{E}}[k]$ are the corresponding superposition of data and artificial noise.

To launch the attack, Eve aims at finding $F_{\mathcal{E}}$ to minimize

$$\|F_{\mathcal{E}}[k] R_{\mathcal{E}}[k] - D_{\mathcal{B}}[k]\|_F^2.$$

However, since Eve does not know $D_{\mathcal{B}}$, the problem appears to be unsolvable. Instead, Eve may attempt to solve an alternative problem,

$$\begin{array}{ll} \text{minimize} & \mathrm{H}\left(F_{\mathcal{E}}[k] \begin{pmatrix} \overleftarrow{R}_{\mathcal{E}}[k] & \bar{R}_{\mathcal{E}}[k] \end{pmatrix}\right) \\ \text{subject to} & F_{\mathcal{E}}[k] F_{\mathcal{E}}^H[k] \succ 0 \\ & \mathbf{E}\left(F_{\mathcal{E}}[k] \overrightarrow{R}_{\mathcal{E},c}[k] \overrightarrow{R}_{\mathcal{E},c}^H[k] F_{\mathcal{E}}^H[k]\right) \geq G \end{array}, \quad (19)$$

where the objective function gives the entropy of the decoded data, $\overrightarrow{R}_{\mathcal{E},c}[k]$ represents each column in $\overrightarrow{R}_{\mathcal{E}}[k]$, and G is the average modulation gain. The constrains prevent any trivial solution such as $F_{\mathcal{E}}[k] = \mathbf{0}$. Intuitively, if the filter is optimal, the objective function gives the entropy of $\begin{pmatrix} \overleftarrow{D}_{\mathcal{B}}[k] & \bar{D}_{\mathcal{B}}[k] \end{pmatrix}$. Otherwise, the residual noise should increase the total entropy.

Unfortunately, since entropy is a concave function, it can be shown that Eq. 19 is NP-hard [15]. To still solve the problem, Eve may exploit the low entropy fields and apply a greedy hill climbing approach. Let $\{\overleftarrow{d}_{\mathcal{B}}[k]\}$ be a set of frequent columns in $\overleftarrow{D}_{\mathcal{B}}[k]$[3]. Eve cycles through the columns in $\overleftarrow{R}_{\mathcal{E}}[k]$ and iteratively update the filter by randomly sampling $\overleftarrow{d}_{\mathcal{B}}[k] \in \{\overleftarrow{d}_{\mathcal{B}}[k]\}$ and solving

$$\text{minimize} \quad \|F_{\mathcal{E}}^{i+1}[k] \overleftarrow{R}_{\mathcal{E},c}[k] - \overleftarrow{d}_{\mathcal{B}}[k]\|_2^2 + \|F_{\mathcal{E}}^{i+1}[k] - F_{\mathcal{E}}^{i}[k]\|_2^2, \quad (20)$$

where the proximal operator $\|F_{\mathcal{E}}^{i+1}[k] - F_{\mathcal{E}}^{i}[k]\|_2^2$ is used to confine the solution close to the previous filter and within the feasible region. There are two possible outcomes for such update: (1) Eve's guess is correct and the update moves the current filter closer to the optimal one. (2) Eve's guess is incorrect and the update moves the current filter farther from the optimal one or outside of the feasible region. Eve can check which outcome it is by applying the filter to $\bar{R}_{\mathcal{E}}[k]$ and comparing the resulting entropy, $\mathrm{H}\left(F_{\mathcal{E}}^{i+1}[k] \bar{R}_{\mathcal{E}}[k]\right)$. If the entropy decreases, Eve accepts the update and vise versa. Note that Eve's guesses do not need to fully match the actual plaintext. Due to the robustness of Eq. 20, Eve can make progress as long as a majority of symbols in her guesses match the plaintext. Once the algorithm converges, Eve can apply the filter to $\overrightarrow{R}_{\mathcal{E}}[k]$ to obtain the content of the payload.

[3] In practice, low entropy fields may occupy multiple columns or a fraction of columns. The iterative approach still applies since Eve knows the beginning of the packet through pilot symbols, and is able to locate the low entropy fields.

6. EXPERIMENTAL EVALUATION

Here, we present the performance of the ciphertext-only attack against orthogonal blinding. In Sec. 6.1 we briefly review the simulation parameters we use for our experiments. We consider three parameters that could affect the attack algorithm, *i.e.*, channel signal-to-noise ratio (SNR), Alice's noise-to-data ratio (NDR), and information efficiency of the transmitted data. In Sec. 6.2, we show the signal reception at Bob's side under a variety of channel SNR and NDR. In Sec. 6.3, we show the convergence behavior and effectiveness of our attack algorithm. In Sec. 6.4, we discuss how the attack algorithm performs against blinded data with different information efficiency. In Sec. 6.5 and Sec. 6.6, we analyze the effect of channel SNR and Alice's NDR. Finally, we summarize our finding in Sec. 6.7.

6.1 Technical Parameters

As we described in Sec. 3, our three nodes Alice, Bob and Eve are multi-antenna nodes using OFDM transmitters. In particular, our evaluation setup considers Alice and Eve having two antennas, and Bob having one. We use synthetic wireless packets with predefined information efficiency as transmitted data. To create the synthetic packets, we randomly generate a set of 16-bit binary vectors and perform rejection sampling to collect samples that have H distinct values. This way, the corresponding wireless packets have an overall information efficiency of H/16. To transmit the data, We use OFDM to split a 40 MHz wide additive white Gaussian noise (AWGN) channel into 64 equally spaced sub-channels. The OFDM frames consist of pilot symbols for channel sounding and 500 data symbols for each sub-channel.

We use normalized quadrature phase shift keying (QPSK) as our primary modulation scheme. To generate the data symbols for each sub-channel, we encode the synthetic wireless packets trough a 2 bit Gray code encoder, and modulate the gray codes into QPSK data symbols. We assign every 8 successive data symbols to one sub-channel such that every sub-channel carries a parallel string of packets. To measure the effect of Alice's artificial noise, we vary the ratio between artificial noise and transmitted data signal, *i.e.* NDR. Since Alice's total transmit power is fixed, a higher NDR reduces the amount of power to transmit the data signal,

$$\frac{1}{\mathrm{NDR}+1}\begin{pmatrix} D[k] \\ \mathrm{NDR}\cdot\mathrm{AN}[k] \end{pmatrix}.$$

To measure the effect of channel noise, we also vary the channel's SNR referenced by Alice's transmit power. Finally, we use Eve's symbol error rate (SER) to measure the progress and performance of the attack algorithm. The following results are based on 50 Monte Carlo simulations for each configuration.

6.2 Bob's Signal Reception

To evaluate the performance of our ciphertext-only attack, We first show Bob's SER under orthogonal blinding. As shown in Fig. 3, Bob's SER is affected by both the channel's SNR and Alice's NDR. As Alice increases the NDR, she dedicates more power to transmit the artificial noise instead of data symbols, which increases Bob's SER. As the channel's SNR decreases, the channel noise also increases Bob's SER. Note that under the same setting as in Fig. 4, where NDR = 4 and SNR = 30 dB Bob can achieve an average SER of 1.1×10^{-3}.

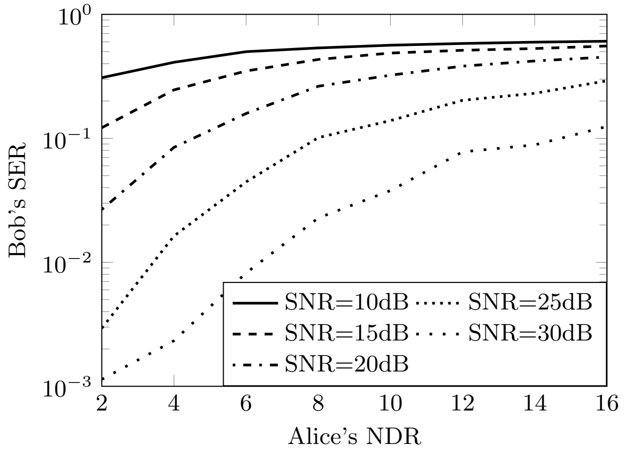

Figure 3: Bob's SER over Alice's NDR for different SNRs.

6.3 Convergence Behavior

In Fig. 4, we show how Eve's SER reduces over the number of iterations. Since the performance of the hill climbing algorithm varies with the initial conditions, the result is obtained by averaging over 50 Monte Carlo simulations. From Fig. 4, we see that minimizing the entropy of the decoded message serves as a good searching oracle. When the information efficiency equals 0.4, the hill climbing algorithm is able to converge within 5 iterations[4], which corresponds to 40 symbols in the received data. Due to the robustness of the least-square solution and proximal operator, Eve can always make progress as long as her guesses are not completely wrong. When the algorithm converges, Eve can reduce her SER to approximately 0.1. Note that the result is achieved without knowing the exact plaintext symbols transmitted by Alice. Yet, the SER achieved through ciphertext-only attack is only 1.3% higher than the SER achieved through the optimal filter, $H_B^{\dagger}[k]$.

6.4 Effect of Information Efficiency

In Fig. 5, we illustrate how information efficiency of the training data affects the algorithm's rate of convergence and Eve's SER. The information efficiency practically correlates to Eve's guessing space. A high information efficiency reduces the probability for Eve to obtain a correct guess. In addition, a high information efficiency reduces the number of accidental matching symbols when Eve's guess is wrong. Due to the two factors, the algorithm's rate of convergence increases as the information efficiency increases. In our simulation, when the information efficiency increases from 0 to 0.6, the algorithm's rate of convergence increases from 1 iteration to 17 iterations. However, the information efficiency has no dramatic effect toward Eve's optimal SER. The reason is because, unlike channel SNR and NDR, the information efficiency does not introduce additional noise into Eve's reception. In our simulation, when the information efficiency increases from 0 to 0.6, Eve's SER merely increases by 3.1%.

[4] We define the algorithm convergence as the iteration when the objective value is within 10% of the optimal value.

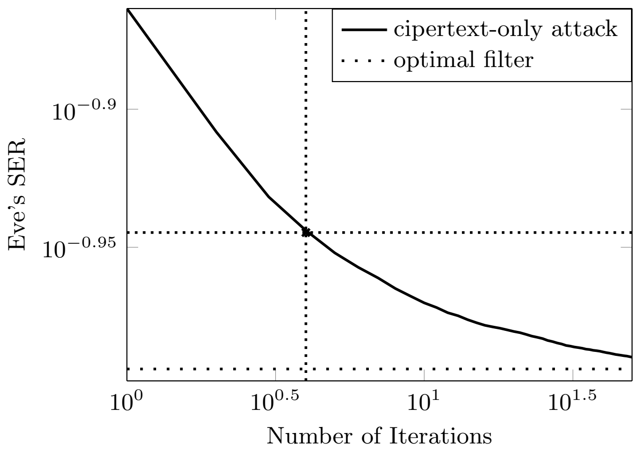

Figure 4: Eve's SER over the number of iterations. SNR = 30 dB; NDR = 4; information efficiency = 0.4. The dotted line marks Eve's SER when applying the optimal filter.

6.5 Effect of Channel Noise

In Fig. 6, we illustrate how channel SNR affects the algorithm's rate of convergence and Eve's SER. By increasing the channel noise, we can decrease the channel SNR, which affects both Eve and Bob. As shown in Fig. 3 and Fig. 5, a low channel SNR increase Bob's SER as well as Eve's optimal SER during the ciphertext-only attack. In our simulation, when the channel SNR decreases from 30 dB to 10 dB, Eve's optimal SER increases from 0.11 to 0.54. The channel SNR also affects algorithm's rate of convergence since low channel SNR reduces the algorithm's sensitivity. When the channel SNR is low, there is a high chance that the transmitted data is distorted even without orthogonal blinding. Therefore, the algorithm tends to quickly converge to a high SER instead of slowly converging to a low SER. In our simulation, when the channel SNR efficiency decreases from 30 dB to 10 dB, the rate of convergence decreases from 10 iterations to 4 iterations.

6.6 Effect of Artificial Noise

In Fig. 7, we show how Alice's NDR affects the performance of the attack algorithms. Same as Bob's signal reception, Eve's SER decreases as Alice increases her NDR. The reason is because the high NDR reduces the amount of power to transmit the data signal. In our simulation, when Alice's NDR increases from 2 to 10, Eve's optimal SER increases from 0.09 to 0.21. However, Alice's NDR has little effect on the algorithm's rate of convergence. In our simulation, when Alice's NDR increases from 2 to 10, the algorithm's rate of convergence stays between 8 to 10 iterations.

6.7 Summary

In Table 2, we summarize the findings of our experiments. In particular, when Eve is powerful and dishonest, she can effectively reduce her SER using the ciphertext-only attack. By minimizing the entropy of the decoded message, our hill climbing method allows Eve to estimate the channel between Alice and Bob, and find the optimal filter to separate the data and the artificial noise within 20 iterations. Our method can handle a wide range of channel SNR, Alice's NDR, and a variety of transmitted data with different information efficiency. The only side channel knowledge that Eve uses to breach the system is a general knowledge about the format of the wireless packets.

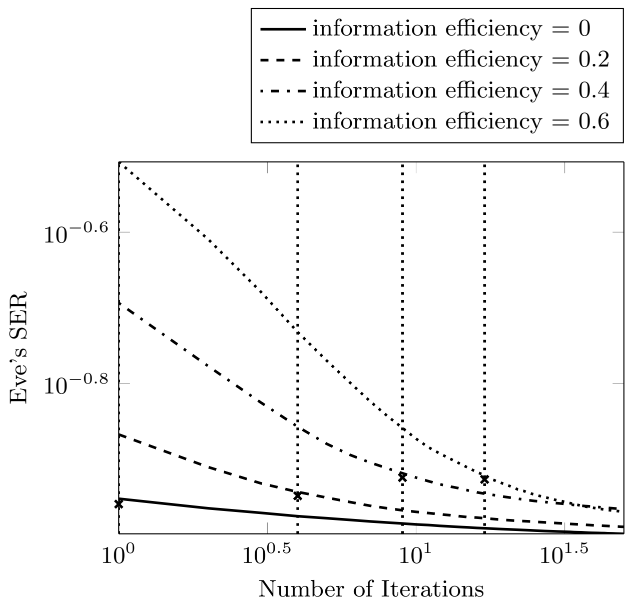

Figure 5: Eve's SER over the number of iterations. SNR = 30 dB; NDR = 4; various information efficiencies.

7. DISCUSSION

In the previous sections, we analyzed the security level of orthogonal blinding under different MIMO configurations. Our attack showcase further proves that orthogonal blinding vulnerable against ciphertext-only attack launched by multi-antenna eavesdropper. We now reflect on the limitation of physical-layer security in general and discuss how our analysis framework can be applied to other physical-layer security schemes.

Unlike higher-layer security measures, physical-layer security approaches are usually "keyless" methods that operate within the principles of wireless communication. The sole purpose of communication is to allow receivers to recover the transmitted message as much as possible. Hence, the operations applied at transmitter's side must be reversible by the receiver. In addition, the wireless medium only permits linear combination between various signals. These two prior conditions significantly limits the level of confusion and diffusion a physical-layer security method can achieve. In fact, most physical-layer security methods do not employ any one-way operation, but rely on interference to thwart the eavesdropper. As a result, the strength of physical-layer security methods is bound to be lower that higher-layer security measures, such as encryption.

Despite of its limitations, physical-layer security may still achieve "practical security" depending on its application scenarios. For instance, we have shown that a user cannot use orthogonal blinding to transmit long, regular messages with low information efficiency. However, the method is still relatively secure when it transmits random bits in short burst, given that the length of the bit string is smaller than the number of transmitting antennas. Such feature can be

Table 2: Summary of the major findings in simulations.

Experiment	Section	Conclusion
Convergence behavior	Sec. 6.3	The algorithm is able to converge within 10 iterations (160 symbols) and achieves comparable SER as the optimal filters.
Effect of information efficiency	Sec. 6.4	A high information efficiency increases the algorithm's rate of convergence but does not affect Eve's optimal SER.
Effect of channel noise	Sec. 6.5	A low channel SNR increases the algorithm's rate of convergence and Eve's optimal SER.
Effect of artificial noise	Sec. 6.6	A high NDR increases Eve's optimal SER but does not affect the algorithm's rate of convergence.

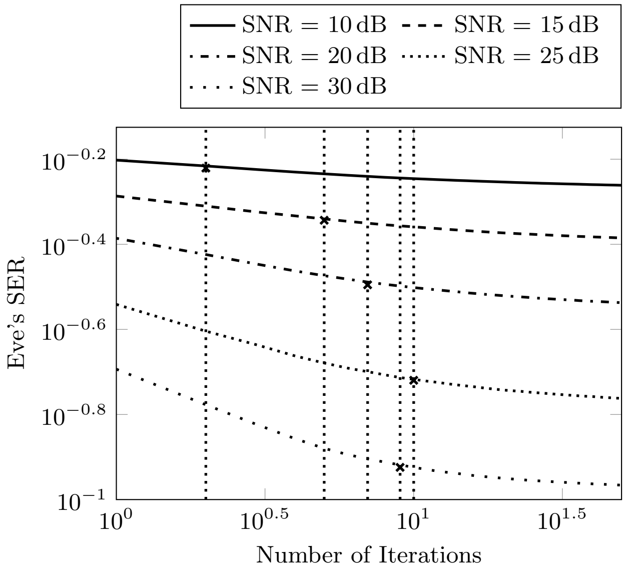

Figure 6: Eve's SER over the number of iterations, NDR = 4; information efficiency = 0.4; various SNRs.

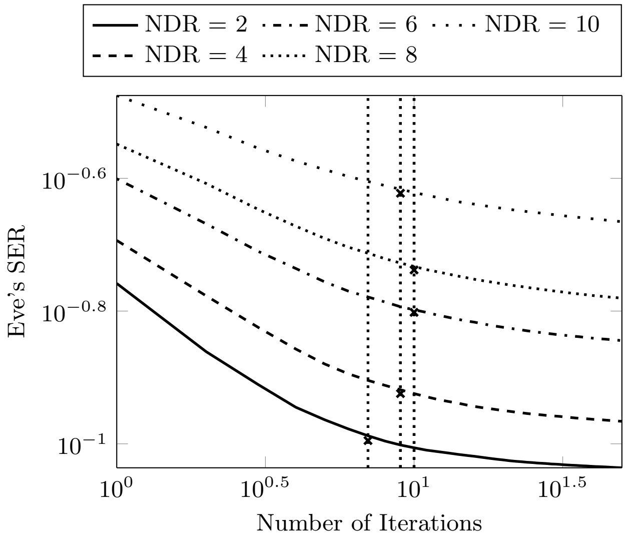

Figure 7: Eve's SER over the number of iterations. SNR = 30 dB; information efficiency = 0.4; various NDRs.

found useful in key exchange protocols. However, these application scenarios can only be identified after a thorough security analysis, which physical-layer security designer often neglect to do.

In our framework, we mainly rely on information theoretic analysis to determine the secrecy levels of linear precoding based physical-layer security method. The technique can also be extended when assessing physical-layer security schemes in general. The reason is because the obfuscation functions employed by physical-layer security are relatively simple and easy to handle mathematically. In most cases, these functions are linear or affine in nature, which makes theoretical analysis an ideal tool to determine the correlation between the received signal and the transmitted signal. Moreover, by categorizing eavesdroppers according to their capacities, we can better analyze the secrecy level of a physical-layer security method and provide a clearer picture about the its strength and weakness. For future work, we aim to apply our framework upon other physical-layer security schemes to help identify the application scenarios that are within their limitations.

8. CONCLUSION

In this work, we studied the strength of physical-layer security by means of theoretical analysis and practical attack. we evaluated a specific physical layer security scheme, *i.e.* orthogonal blinding, under multiple eavesdropper settings. We identified the weakness of orthogonal blinding by channeling the concepts from information theory into cryptanalysis. We discovered that, due to the linearity and the low entropy contents in the transmitted data, the system is vulnerable against attack equivalents to the "ciphertext-only attack" in the cryptography domain against a multi-antenna eavesdropper. We presented a practical attack method that allows eavesdroppers to recover the original message by exploiting the low entropy fields in wireless packets. By means of simulation, we demonstrated the effectiveness of the attack by reducing the eavesdropper's SER below 1% using only the eavesdropper's receiving data and a general knowledge about the wireless packets.

Acknowledgment

This work has been funded by the German Research Foundation (DFG) in the Collaborative Research Center (SFB) 1053 "MAKI – Multi-Mechanism-Adaptation for the Future Internet", by LOEWE CASED, and BMBF/HMWK CRISP. Zheng and Hou's work was partially supported by the National Science Foundation under grants CNS-1446478, CNS-1405747, CNS-1443889, and CNS-1343222. Lou's work was supported by (while serving at) the National Science Foundation. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] Xiangyun Zhou, Lingyang Song, and Yan Zhang. *Physical layer security in wireless communications.* Crc Press, 2013.

[2] Shyamnath Gollakota et al. "They can hear your heartbeats: non-invasive security for implantable medical devices". In: *ACM SIGCOMM Computer Communication Review* 41.4 (2011), pp. 2–13.

[3] Shyamnath Gollakota and Dina Katabi. "Physical layer wireless security made fast and channel independent". In: *INFOCOM, 2011 Proceedings IEEE.* IEEE. 2011, pp. 1125–1133.

[4] Nils Ole Tippenhauer et al. "On limitations of friendly jamming for confidentiality". In: *Security and Privacy (SP), 2013 IEEE Symposium on.* IEEE. 2013, pp. 160–173.

[5] Daniel Steinmetzer, Matthias Schulz, and Matthias Hollick. "Lockpicking Physical Layer Key Exchange: Weak Adversary Models Invite the Thief". In: *Proceedings of the 2015 ACM Conference on Security and Privacy in Wireless Mobile Networks.* WiSec '15. 2015.

[6] N. Anand, Sung-Ju Lee, and E.W. Knightly. "STROBE: actively securing wireless communications using Zero-Forcing Beamforming". In: *Proc. INFOCOM'12.* 2012, pp. 720–728.

[7] Matthias Schulz, Adrian Loch, and Matthias Hollick. "Practical Known-Plaintext Attacks against Physical Layer Security in Wireless MIMO Systems". In: *Proc. NDSS'14.* 2014.

[8] Yao Zheng et al. "Highly Efficient Known-Plaintext Attacks Against Orthogonal Blinding Based Physical Layer Security". In: *IEEE Wireless Communications Letters* 4.1 (Feb. 2015), pp. 34–37.

[9] Aaron D Wyner. "The wire-tap channel". In: *Bell System Technical Journal, The* 54.8 (1975), pp. 1355–1387.

[10] S. Leung-Yan-Cheong and M. Hellman. "The Gaussian wire-tap channel". In: *IEEE Transactions on Information Theory* 24.4 (July 1978), pp. 451–456.

[11] Ashish Khisti and Gregory W Wornell. "Secure transmission with multiple antennas I: The MISOME wiretap channel". In: *Information Theory, IEEE Transactions on* 56.7 (2010), pp. 3088–3104.

[12] Ashish Khisti and Gregory W Wornell. "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel". In: *Information Theory, IEEE Transactions on* 56.11 (2010), pp. 5515–5532.

[13] Yu-Chih Tung et al. "Vulnerability and Protection of Channel State Information in Multiuser MIMO Networks". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security.* CCS '14. 2014.

[14] The Institute of Electrical and Inc. Electronic Engineers. "IEEE Standard 802.11-2013". English. In: *IEEE Standard for Information technology* (2013).

[15] Mladen Kovacevic, Ivan Stanojevic, and Vojin Senk. "On the hardness of entropy minimization and related problems". In: *Information Theory Workshop (ITW),*