ROBin: Known-Plaintext Attack Resistant Orthogonal Blinding via Channel Randomization

***Abstract*—Orthogonal blinding based schemes for wireless physical layer security aim to achieve secure communication by injecting noise into channels orthogonal to the main channel and corrupting the eavesdropper's signal reception. These methods, albeit practical, have been proven vulnerable against multi-antenna eavesdroppers who can filter the message from the noise. The venerability is rooted in the fact that the main channel state remains stasis in spite of the noise injection, which allows an eavesdropper to estimate it promptly via known symbols and filter out the noise. Our proposed scheme leverages a reconfigurable antenna for Alice to rapidly change the channel state during transmission and a compressive sensing based algorithm for her to predict and cancel the changing effects for Bob. As a result, the communication between Alice and Bob remains clear, whereas randomized channel state prevents Eve from launching the known-plaintext attack. We formally analyze the security of the scheme against both single and multi-antenna eavesdroppers and identify its unique anti-eavesdropping properties due to the artificially created fast changing channel. We conduct extensive simulations and real-world experiments to evaluate its performance. Empirical results show that our scheme can suppress Eve's attack success rate to the level of random guessing, even if she knows all the symbols transmitted through other antenna modes.**

I. Introduction

The ever-expanding wireless technology is pushing the limit of the network security infrastructure. Many wireless devices need to secure the communication channels between each other without pre-shared security context. Orthogonal blinding based physical-layer security [1]–[3] has been widely considered as a promising candidate to provide confidentiality during wireless transmission without *a priori* key exchange. Instead of relying on pre-shared secrets, orthogonal blinding achieves secure communications by transmitting synthetic noise into the null-space of the receiver's channel and corrupting the eavesdropper's reception. Its practicality supersedes other theoretical physical-layer methods, such as zero-forcing beamforming, which relies on knowledge about the eavesdropper's channel. Security analysis proves that it can asymptotically approach the secrecy capacity of zero-force beamforming against single-antenna eavesdroppers. However, further studies show that orthogonal blinding is not effective against a multi-antenna eavesdropper, who has sufficient spatial dimensions to separate the message from the artificial noise. Schulz and Zheng et al. [4]–[6] demonstrated that an eavesdropper may leverage the known or low entropy symbols in the transmission to quickly train a decoding filter and recovers the rest of the transmission, an attack equivalent to the known-plaintext attack in cryptanalysis.

The root of this vulnerability is due to the fact that the synthetic noise only changes the quality of the receiving signal but not the state of the channel. Specifically, the noise injected by the transmitter (Alice) can lower the signal-to-noise ratio (SNR) of the eavesdropper's (Eve's) channel. But it cannot change the channel states between she and Eve or she and the legitimate receiver (Bob). This limitation opens up a window for the known-plaintext attack. Assuming the channel state remains ergodic with its coherent time. Due to the increasingly sophisticated digital modulation methods, Alice can transmit a sequence of tens or hundreds of symbols within such a short period. Although these symbols are buried deep under the synthetic noise, a fraction of known symbols among them would allow Eve with multiple antenna to compute the channel state information (CSI), using a common MIMO technique known as least square (LS) channel estimation, which is robust against channel noise. Once Eve estimated the CSI, she may use it to equalize the channel and remove the synthetic noise during the rest of the coherent period.

Follow this line of reasoning, there are two ways to defend against the known-plaintext attack, assuming Alice cannot avoid transmitting known symbols. She can limit the number of symbols to transmit within each coherent time period, which limits the communication throughput. Or she can reduce the coherent time to thwart the known-plaintext attack. However, the coherent time is an intrinsic condition that depends on the signal multipath and Doppler spread, both of which are not subject to the manipulation of transmitting content. Therefore, it would appear there are no cogent methods to defend against the known-plaintext attack.

However, in this paper, we challenge this no-win scenario and propose an orthogonal blinding based physical-layer security method immune to the known-plaintext attack: Channel-**R**andomized **O**rthogonal **Blin**ding (ROBin). ROBin leverages a pattern reconfigurable antenna to vary the channel state at a per symbol or per frame rate, resulting in an artificially created fast-changing wireless channel unsuitable for the known-plaintext attack. To prevent the antenna reconfiguration from affecting Bob, we design a compressive sensing based algorithm for Alice to estimate the angle-of-departure (AoD) distribution of the multipath environment and predict the CSI for a given reconfigurable antenna pattern. Based on the predicted CSI, Alice can equalize the channel for Bob via digital pre-coding before transmitting. As a result, the main channel state appears stable in Bob's eye but randomly changing from Eve's perspective.

We formally analyze the security of ROBin, by comparing

the mutual information between Alice's transmission and Eve's reception, assuming the channel state has the Markov property and Eve knows the symbols transmitted via historical antenna modes but not the current one. The analysis shows that Eve gains little advantage from knowing previous symbols (as channel randomization reduces the channel correlation and makes the current channel state more unpredictable), regardless of the number of antennas she has. We implement the key components of ROBin; validate our theoretical analysis with extensive simulation and real-world experiments. Empirical results show that our scheme can suppress Eve's attack success rate to the level of random guessing, even if she knows all the symbols transmitted through other modes.

II. Related Work

Physical-layer security was pioneered by Wyner's work on the wiretap channel [7], which leverages the *channel advantage* for legitimate receivers over eavesdroppers (e.g. less noisy) to guarantee secure transmission over wireless channels. The rate of secret communications is characterized by *secrecy capacity*, which is shown to be the difference in the capacity of the receiver and the eavesdropper. Following Wyner's work, numerous studies based on various channel models ranging from basic Gaussian channels to complex MIMO wiretap channels have been proposed later [8]–[14]. In particular, Khisti et al. [12], [14] showed the secrecy capacity bounds in the large antenna limit with full channel state information (CSI) assumption. Their works reveal an important result that the achievable secrecy capacity can be significantly affected by the number of antennas of the eavesdropper. For instance, to block secret communication, Eve only needs three times as many antennas as transceivers have. However, since those theoretical works often make unrealistic assumptions such as channel advantage, full channel knowledge, or independent and identically channel distribution, they are rarely adopted to evaluate the secrecy of real-world schemes.

On the other hand, various practical physical-layer secret communication schemes have been proposed. One example is the friendly jamming approach. Gollakota et al. prevented unauthorized commands from being transmitted to implantable medical devices (IMDs) with a friendly jamming scheme in [1]. The security of their scheme relies on the assumption that the attacker equipped with MIMO is unable to separate the legitimate and jamming signal, due to the close proximity between the jammer and the data source. Similarly, Shen et al. [15] designed another jamming technique where jamming signals are controlled with secret keys, so that they are recoverable to authorized devices but unpredictably interfering to unauthorized ones. The jammer and the authorized device are very close to each other in both schemes, and this design is found as vulnerable by Tippenhauer et al. in [16]. When an attacker tactfully places her antenna array, the transmitted data signal can be recovered by exploiting the phase offsets between received signal components. Orthogonal blinding [3] proposed by Anand et al. is another example of physical-layer security schemes. To defend against a single-antenna eavesdropper, the transmitter injects artificial noise into channels orthogonal to the legitimate receiver's channel so that the original signal intended for the receiver cannot be recovered from the signal and noise mixture. However, when the eavesdropper has multiple antennas, by exploiting the known parts of the transmitted signal such as frame preambles, Schulz et al. [17] successfully implemented a known-plaintext attack against orthogonal blinding. With normalized least mean square algorithms, an adaptive filter was trained to separate transmitted messages from artificial noise.

The root cause of the vulnerability in orthogonal blinding is that the channel is assumed to be stable during the whole transmission period, so that the attacker is able to gather enough plaintexts for filter training, and this flaw can be amended with channel randomization approach. In the literature, the channel randomization approach has been used for key generation, message confidentiality, and integrity protection. Aono et al. [18] proposed a key generation and agreement scheme that blocks the eavesdropper from generating the same key as transceivers by increasing the fluctuation of the wireless channel with a smart antenna. Hassanieh et al. [19] presented a secret transmission scheme for RFIDs randomizing both modulation and channel by rotating several directional antennas at the transmitter. Different from this work, their scheme is only applicable to single-antenna transmitters and does not use pre-coding. To defend against active man-in-the-middle attacks, Hou el al. [20] and Pan et al. [21] randomized the wireless channel with a fan and a reconfigurable antenna respectively to prevent online signal cancellation. All these works show that channel randomization approach can be a powerful tool to enhance physical-layer security. However, the studies are still preliminary and a comprehensive scheme that is MIMO-compatible and secure against multi-antenna attackers is lacking.

III. System and Threat Models

Consider a MIMO-OFDM system shown in Fig. 1, where the transmitter Alice aims at confidentially communicating with the receiver Bob through a wireless channel $\mathbf{H}_{AB}$, with the existence of a passive eavesdropper Eve. Denote the number of antennas for Alice, Bob and Eve as n_a, n_b and n_e respectively. The legitimate receiver Bob is equipped with regular omnidirectional antenna(s) (OAs) while the eavesdropper Eve can possess any types of antennas, including OAs, reconfigurable antenna(s) (RAs) and etc.. In particular, the transmitter Alice is equipped with RAs for channel randomization purpose, where an RA is an antenna capable of dynamically reconfiguring its antenna currents or radiating edges in a controlled and reversible manner [22]. Typically, an RA can swiftly reconfigurable its antenna profile including radiation pattern, polarization, frequency, and combinations of them. For example, Rodrigo et al. [23] presented an RA that has thousand of antenna modes and can be electronically switched within microseconds. From the receiver's perspective, the effect of the antenna profile is part of the CSI. Hence we can incorporate the impact of RA on the wireless into the channel model.

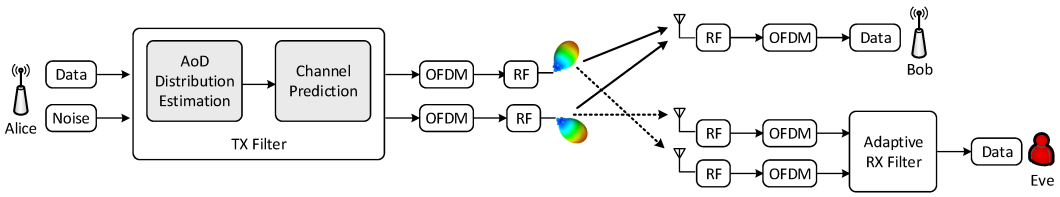

Fig. 1: Our system model illustrating the transmitter Alice, the legitimate receiver Bob and the passive eavesdropper Eve, where Alice is equipped with RA(s).

The wireless channel from Alice's j-th antenna to a receiver's i-th antenna ((i,j)-th receive-transmit pair) can be captured by a single complex number in the frequency domain, i.e. $h_{i,j}$, and the full CSI of transceivers can be represented by an array $\mathbf{H}$ with dimension $n_b \times n_a$. Then the received signal $\mathbf{R}$ with dimension $n_b \times *$ can be expressed as:

$$\mathbf{R} = \mathbf{H} \cdot \mathbf{D} + \mathbf{N} \tag{1}$$

where $\mathbf{D}$ and $\mathbf{N}$ represents the transmitted data and the additive white Gaussian noise (AWGN), with dimension $n_a \times *$ and $n_b \times *$ respectively. For the channel model, we consider a multipath channel. Recall that the effect of the antenna profile is also part of the CSI, to distinguish, we separate the CSI into the channel coefficient decided by the physical channel itself and the antenna part. Assuming that the channel is composed with P multipaths, denote the physical channel coefficient part of $h_{i,j}$ as $h_{i,j}^{(phy)}$, then

$$h_{i,j}^{(phy)} = \sum_{l=1}^{P} L_l \alpha_l e^{-j\phi_l} \tag{2}$$

where L_l is the path loss of the l-th path, and $\alpha_l e^{-j\phi_l}$ is its fading parameter, here α_l and ϕ_l are the amplitude and phase of the fading respectively. Similar to existing works [3], [6], [17], the physical channel coefficient $h_{i,j}^{(phy)}$ in our model is fixed during the channel coherent time. Then the multipath channel can be expressed with the distribution of angle-of-departure (AoD). According to the multipath model, a single transmission from the antenna propagates along multiple paths before reaching the receiver. Each signal that travels at a particular AoD along with different paths experiences a different amount of attenuation and phase shifts. Then the physical channel coefficient part expressed as (2) can be further extended as the summation of the CSI over all the departure directions, and only the CSI that in the direction of multipaths is non-trivial. The distribution of CSI over all possible AoDs is defined as the AoD distribution. Then,

$$h_{i,j}^{(phy)} = \sum_{d=1}^{D} \mathbf{a}_{i,j}(\theta_d) \tag{3}$$

where the angular space is discretized into D unique, equally spaced angles $\{\theta_1, \theta_2, \ldots, \theta_D\}$, and $\mathbf{a}_{i,j}$ is the AoD distribution of (i,j)-th receive-transmit channel.

With RA, various antenna modes are associated with different radiation patterns. When the antenna gain under antenna mode u and angle-of-departure θ_l is denoted as $\mathbf{G}(u, \theta_d)$, then the CSI $h_{i,j}$ under antenna mode u can written as:

$$h_{i,j}(u) = \sum_{d=1}^{D} \mathbf{G}(u, \theta_d) \mathbf{a}_{i,j}(\theta_d) \tag{4}$$

Similarly, the channel from Alice to Bob ($\mathbf{H}_{AB}$) is measured at Bob's side and can be sent back to Alice through an out-of-band (OOB) channel or rely on implicit feedback, but $\mathbf{H}_{AB}$ is unknown to Eve. And Eve's can measure the channel from Alice to her ($\mathbf{H}_{AE}$), and it is unknown to neither Alice nor Bob [3], [6], [17].

IV. Review of Orthogonal Blinding

Orthogonal blinding is designed to achieve secure communication by injecting noise into channels orthogonal to the main channel and corrupt the eavesdropper's signal reception. However, it has been proven vulnerable against multi-antenna eavesdropper capable of discerning the message from the noise. In this section, we provide a brief review of orthogonal blinding scheme and cause of its vulnerabilities.

A. Transmitter-Side Precoding

The core technique behind orthogonal blinding is known as transmitter-side precoding. To achieve secure transmission, Alice stirs both message and artificial noise (AN) via precoding. So Bob receives the pure message, and Eve receives the mixture of the noise and message. Zero-forcing and orthogonal blinding are two physical layer security schemes to achieved by transmitter-side precoding.

In zero-forcing, Alice aims to transmit within the null-space of Eve's channel, which requires the full knowledge of Eve's channel. Such condition is not practical for a passive eavesdropper. In orthogonal blinding, Alice needs only to know Bob's channel and transmits the AN in the null-space of Bob's channel to prevent eavesdroppers from extracting the data. Due to the orthogonality, Bob is not affected by the AN. But any receiver, whose channel is different from Bob's, receives a mixture of the message and AN. If the AN is strong enough in the mixture, the receiver cannot recover the message.

The channels orthogonal to Bob's can be computed with the Gram-Schmidt algorithm as mentioned in [3], [6], [17]. First, Alice computes the projection matrix:

$$\mathbf{H}_p = \mathbf{H}_{AB}^H (\mathbf{H}_{AB} \mathbf{H}_{AB}^H)^{-1} \mathbf{H}_{AB} \tag{5}$$

and randomly generates a complex uniform matrix $\mathbf{H}'_{AN}$ with dimension $(n_a - n_b) \times n_a$. Alice then computes the difference between $\mathbf{H}'_{AN}$ and the projection of $\mathbf{H}'_{AN}$:

$$\mathbf{H}''_{AN} = \mathbf{H}'_{AN} - \mathbf{H}'_{AN} \cdot \mathbf{H}_p \tag{6}$$

by normalizing this difference, we can obtain $\mathbf{H}_{AN}$:

$$\mathbf{H}_{AN} = \frac{\mathbf{H}''_{AN}}{\|\mathbf{H}''_{AN}\|} \tag{7}$$

where each row in $\mathbf{H}_{AN}$ is orthogonal to any other row in itself and to every row in $\mathbf{H}_{AB}$.

Next, Alice precodes the message ($\mathbf{D}_B$) and artificial noise (**AN**) with the pseudo-inverse of the matrix composed by $\mathbf{H}_{AB}$ and $\mathbf{H}_{AN}$, and obtain the transmitted signal $\mathbf{D}$ as:

$$\mathbf{D} = \mathbf{F}_A \begin{pmatrix} \mathbf{D}_B \\ \mathbf{AN} \end{pmatrix} \tag{8}$$

where $\mathbf{F}_A$ is the transmit filter represented as:

$$\mathbf{F}_A = \begin{pmatrix} \mathbf{H}_{AB} \\ \mathbf{H}_{\text{AN}} \end{pmatrix}^H \left(\begin{pmatrix} \mathbf{H}_{AB} \\ \mathbf{H}_{\text{AN}} \end{pmatrix} \begin{pmatrix} \mathbf{H}_{AB} \\ \mathbf{H}_{\text{AN}} \end{pmatrix}^H \right)^{-1} \tag{9}$$

Correspondingly, the received signal for Bob and Eve is:

$$\begin{pmatrix} \mathbf{R}_B \\ \mathbf{R}_E \end{pmatrix} = \begin{pmatrix} \mathbf{H}_{AB} \\ \mathbf{H}_{AE} \end{pmatrix} \cdot \mathbf{D} + \mathbf{N} \tag{10}$$

where

$$\mathbf{R}_E = \mathbf{H}_{AE} \cdot \mathbf{F}_A \cdot \begin{pmatrix} \mathbf{D}_B \\ \mathbf{AN} \end{pmatrix} + \mathbf{N} \tag{11}$$

B. Known-Plaintext Attack

Anand et al. [3] showed that single antenna eavesdroppers cannot recover the message with her reception, however, Schulz et al. [17] and Zheng et al. [6] showed that by exploiting the known parts or low entropy parts of the transmitted signal, the known-plaintext or ciphertext-only attack is possible in practice. Specifically, Schulz et al. introduced a practical known-plaintext attack for the orthogonal blinding scheme in [17]. Unlike the typical assumption in the literature which assumes that the transmitted signal is fully unknown to the eavesdropper, Schulz argued that Eve can utilize the well-known protocols or addresses fields to guess part of the transmitted signal, so that some plaintext-ciphertext pairs are known to the eavesdropper, which is similar to the known-plaintext attack in cryptography. Then the eavesdropper can use the known plaintexts to train an adaptive filter for AN suppression. Ideally, the receive filter $\mathbf{F}_E$ is:

$$\mathbf{F}_E = \mathbf{F}_A^{-1} \cdot \mathbf{H}_{AE}^{-1} \tag{12}$$

In practice, Eve estimates $\mathbf{F}_E$ as $\hat{\mathbf{F}}_E$ with some known plaintexts $\mathbf{D}_B$ through iterative process. More specifically, Eve minimizes the mean square error between the estimated data and the known plaintexts:

$$\min_{\hat{\mathbf{F}}_E} \; E|\mathbf{D}_B - \hat{\mathbf{F}}_E \cdot \mathbf{R}_E|^2 \tag{13}$$

There are several iterative training algorithms for this problem [17], but in general, for a fixed transmit filter $\mathbf{F}_A$, multiple symbols are required to obtain a good adaptive filter at Eve's side due to the iterative training procedure. In [17], even with good training technique and parameter setting, $20-30$ training symbols are required when the ratio of transmitted AN to data is fairly low.

V. ROBIN: CHANNEL-RANDOMIZED ORTHOGONAL BLINDING

The vulnerability of preliminary orthogonal blinding results from the unchanged main channel, which allows the eavesdropper to estimate it via known symbols and filter the AN out. Actually, this flaw can be amended with the channel randomization approach, which is to actively randomize the wireless channel by introducing special antennas [18], [21], antenna motions [19] or artificial disturbance [20] to the wireless channel. Intuitively, as long as the wireless channel is randomized fast enough, we can block Eve from gathering enough symbols for filter training, so that the message cannot be extracted from Eve's received signal. Besides, except for filter training, Eve may also explore the correlation between her channels and the main channel to estimate Bob's channel directly for message recovering. Results in [21], [24] showed that there is a strong correlation between two channels when the attacker is delicately positioned, and this correlation can be reduced with channel randomization [21]. We show the benefits of reducing channel correlation to system security with the proposed metric in Sec. VI, which further supports our channel randomization approach. In this section, we present the challenges in our scheme design and the corresponding solutions.

A. Channel Prediction

When the physical wireless channel remains unchanged, we randomize the wireless channel through rapid antenna mode switching, however, when the main channel changes, a new transmit filter is needed by Alice to guarantee the orthogonality between the message and noise subspaces. Traditionally, the main channel information $\mathbf{H}_{AB}$ is measured at Bob's side and sent back to Alice through an OOB channel or relying on implicit feedback. However, when the channel is randomized frequently, it is to costly for the transceivers to measure channels and get feedback every time, which makes the channel measurement a major challenge for orthogonal blinding based schemes. To solve this problem, we introduce a compressive sensing based channel prediction algorithm for Alice to cancel the channel changing effect to Bob.

1) AoD Estimation: As the physical channel coefficient part is assumed as unchanged within the channel coherent time, it implies a stable AoD distribution correspondingly. To predict the CSI under different antenna modes, the distribution of AoD is estimated first to capture the physical wireless channel, and the effect of the antenna is added as in (4) for CSI prediction.

2) Conventional AoD Estimation: Traditionally, the distribution of AoD is estimated via MUSIC algorithm [25]. To simplify, we describe it with a uniform linear array (ULA), where identical antenna elements are arranged along a line with

uniform spacing. Assume that there are M antenna elements on the ULA, and there are L multipath signals $S_1, S_2, ..., S_L$ arriving. The matrix representation of the received signal at the array can be represented as:

$$\mathbf{J} = \mathbf{AS} + \mathbf{N} \tag{14}$$

where $\mathbf{J}$ is the $M \times 1$ received signal, $\mathbf{S}$ is the $L \times 1$ signal source and $\mathbf{A}$ is the $M \times L$ steering vector matrix.

The basic idea of MUSIC algorithm is to implement eigenvalue decomposition of the received signal covariance matrix:

$$\mathbf{\Phi}_J = E[\mathbf{J}\mathbf{J}^H] \tag{15}$$

$$= \mathbf{A}\mathbf{\Phi}_S\mathbf{A}^H + \mathbf{\Phi}_N \tag{16}$$

$$= \mathbf{Q}_S \sum \mathbf{Q}_S{}^H + \mathbf{Q}_N \sum \mathbf{Q}_N{}^H \tag{17}$$

where $\mathbf{\Phi}_S$ and $\mathbf{\Phi}_N$ are the correlation matrix for the signal and noise respectively. Decomposing (16) results in M eigen values out of which the larger L eigenvalues correspond to the multipath signals, where $\mathbf{Q}_S$ and $\mathbf{Q}_N$ are the basis of signal and noise subspaces respectively. Then by exploiting the orthogonality between the signal and noise subspaces, the direction of the arrived angles can be represented as:

$$\theta_{MUSIC} = \text{argmin } \boldsymbol{\beta}^H(\theta)\mathbf{Q}_N\mathbf{Q}_N{}^H\boldsymbol{\beta}(\theta) \tag{18}$$

which is equivalent to obtain peaks in the spectral estimation:

$$P_{MUSIC} = \frac{1}{\boldsymbol{\beta}^H(\theta)\mathbf{Q}_N\mathbf{Q}_N{}^H\boldsymbol{\beta}(\theta)} \tag{19}$$

We need to point out that as the MUSIC algorithm was mainly proposed for radio direction finding, the distribution obtained from it is only about the magnitude of CSI, which is not the AoD distribution we need. Hence the traditional MUSIC algorithm is not applicable to our problem.

3) Compressive AoD Estimation with RA: Intuitively, the easiest way to estimate the AoD distribution for a given channel is to transmit with D different antenna modes, so that we can solve (4) directly. However, it is not practical to estimate through this linear algebra approach due to large D (e.g. in our case $D = 360$). Fortunately, by exploiting the sparsity of AoD distribution, the problem is solvable even with a small number of training modes.

Previous works [26], [27] have shown that for a typical multipath environment, there are only 3-5 distinct directions are dominant components. In other words, when we look into the AoD distribution, only a small number of them contribute significantly to the CSI. With this sparsity property, we can recover the AoD distribution from only a small number of measurements. Specifically, we use compressive sensing technique [28] to estimate AoD distribution.

Compressive sensing is a sampling algorithm that capable of recovering sparse signals with much fewer samples than traditional sampling approaches. One of the basic problems is to recover a signal $\mathbf{x}$ from a $M \times 1$ observation $\mathbf{y}$, with a given $M \times N$ sensing basis $\mathbf{\Phi}$, where $M < N$ and the signal $\mathbf{x}$ has a sparse representation with a $N \times N$ representation basis $\mathbf{\Psi}$ and $N \times 1$ weighting coefficients $\mathbf{s}$: $\mathbf{x} = \mathbf{\Psi s}$. Mathematically speaking, the problem is to get $\mathbf{x}$/$\mathbf{s}$ from $\mathbf{y} = \mathbf{\Phi x} = \mathbf{\Phi\Psi s}$. The problem is solvable when the largest correlation between any two elements of $\mathbf{\Phi}$ and $\mathbf{\Psi}$ is small, which is refereed as incoherence [28].

For our problem, since the AoD distribution $\mathbf{a}(\cdot)$ is sparse itself, our presentation basis degrades to an identity matrix, but we can still use the compressive sensing formulation to solve our problem. When training modes are randomly selected, the incoherence condition is roughly satisfied and the AoD distribution of (i, j)-th receive-transmit channel can be recovered from the following compressive sensing formulation:

$$\begin{aligned} \mathbf{a}_{i,j} &= \text{argmin } ||\mathbf{a}_{i,j}(\theta)||_1 \\ \text{s.t. } h_{i,j}(u) &= \sum_{d=1}^{D} G(u, \theta_d)\mathbf{a}_{i,j}(\theta_d), \quad 1 \le u \le U \end{aligned} \tag{20}$$

where $\| \cdot \|_1$ represents the L1 norm and $U \ll D$ are the total number of antenna modes needed for AoD distribution recovery. Note that, Xie et al. presented an estimation algorithm of AoA distribution based on compressive sensing in [29]. However, since they use antenna array, the CSI they use for estimation is the composite CSI instead of the one between each receive-transmit antenna pair. Besides, similar to MUSIC, their AoA distribution only computes the magnitude of the CSI.

4) Channel Prediction: Once the AoD distribution of $h_{i,j}^{(phy)}$ is estimated with the above compressive sensing formulation, the CSI $h_{i,j}$ under any given antenna mode can be predicted with (4). When the AoD distribution of every CSI element in the main channel is estimated, the whole matrix $\mathbf{H}_{AB}$ can be predicted correspondingly. Note that, the physical wireless channel is stable only within the channel coherent time, once the physical channel changes, a new round of AoD distribution estimation is required. In practice, since carrier frequency offset or accurate external clocks such as GPS clocks can eliminate the impact of frequency and phase offset, the channel coherent time can be long. Then the channel prediction is applicable, and it reduces the overhead for channel sounding comparing with the orthogonal blinding scheme.

B. Secure Transmission Scheme

In short, our RA based secure transmission scheme comprises two phases that we summarize hereunder, and for clarification, we denote the set of whole antenna modes, training modes, transmitting modes as $\mathcal{S}$, $\mathcal{S}_1$, $\mathcal{S}_2$ respectively.

1. **Training phase**: (a) Alice selects a certain number of antenna modes as training modes ($\mathcal{S}_1$). For each training mode $u \in \mathcal{S}_1$, several pilots are sent for each receive-transmit antenna pair (i, j) with time-division multiplexing;

(b) Bob measures the corresponding CSI $h_{i,j}(u)$ and shares it with Alice through OOB or implicit feedback;

(c) Alice estimates the corresponding AoD distribution following (20) and gets $\mathbf{a}_{i,j}$.

2. **Secure transmission phase**: (a) Alice randomly selects a set of antenna modes from the complement of $\mathcal{S}_1$ as transmitting modes ($\mathcal{S}_2 \subseteq \mathcal{S} \backslash \mathcal{S}_1$);

(b) For each transmitting mode $v \in \mathcal{S}_2$, Alice predicts the corresponding channel matrix to Bob as $\hat{\mathbf{H}}_{AB}(v)$ following (4), then the transmit filter $\mathbf{F}_A$ is computed based on the predicted $\hat{\mathbf{H}}_{AB}(v)$ following (9);

(c) Alice transmits the message $\mathbf{D}_B$ and AN as in (8). For each packet, Alice uses a different mode randomly chosen from above, and Bob demodulates/decodes the received signal to get the messages from the packets directly.

Note that, the training phase needs to be executed once for every channel coherent time period (which is inversely proportional to the maximum Doppler spread of the physical channel). During the secure transmission phase, Alice does not need to include any pilots/preamble in the packets due to the transmit filter that cancels the channel effect to Bob.

VI. Security Analysis

In this section, we formally analyze the security properties of ROBin. To model ROBin, we define the CSI of a wireless channel, $\mathbf{H}(\cdot)$ as a function of discrete-time t and antenna mode u. Under this definition, the CSI in ROBin behaves as a function $\mathbf{H}\left(t, u(t)\right)$, where u changes for each time step. We further assume that a sequence of $\mathbf{H}\left(t, u(t)\right)$s, forms a Markov chain [30], such that $\mathbf{H}\left(T, u(T)\right)$ is independent of past CSIs, $\{\mathbf{H}\left(t, u(t)\right) \mid t < T-1\}$, given $\mathbf{H}\left(T{-}1, u(T{-}1)\right)$. To quantify the security of ROBin, we derive the conditional mutual information between Eve's receiving signal at time T, $\mathbf{R}_E(T)$, and the pre-blinding message, $\mathbf{D}_B(T)$, assuming Eve knows all previous CSIs between Alice and Bob, $\{\mathbf{H}_{AB}\left(t, u(t)\right) \mid t = 0, ..., T{-}1\}$, and all CSIs between Alice and herself, $\{\mathbf{H}_{AE}\left(t, u(t)\right) \mid t = 0, ..., T\}$ (Sec. VI-A). Finally, we verify the correctness of the proposed metric and explain the insights gained from the analytical results (Sec. VI-B).

A. Secrecy Leakage as Conditional Mutual Information

To quantify eavesdropper's capacity under known-plaintext attacks in a way congruence with cryptanalysis, we consider the secrecy leakage as the conditional mutual information between the Eve's receiving signal and the pre-blinding message, given Eve has full knowledge of all previous CSIs via known symbols. That is, we assume that, as $t = T$, all the previously transmitted symbols, $\mathbf{D}(t),\ t = 0, ..., T{-}1$, are known to Eve, which allows Eve to compute $\mathbf{H}_{AB}(t, u(t)),\ t = 0, ..., T{-}1$.

Let $\mathcal{H}(T)$ defines a set of previous CSIs up to time T:

$$\mathcal{H}(T) = \{\mathbf{H}\left(t, u(t)\right) \mid t = 0, ..., T\}. \tag{21}$$

Assuming $\mathcal{H}_{AE}(T)$ and $\mathcal{H}_{AB}(T-1)$ are known to Eve. The secrecy leakage is defined as a conditional mutual information:

$$I\left(\mathbf{D}_B(T); \mathbf{R}_E(T) \mid \mathcal{H}_{AB}(T-1), \mathcal{H}_{AE}(T)\right) \tag{22}$$

For simplicity, we first consider a single antenna system, in which $\mathbf{H}\left(t, u(t)\right)$ reduces to a scalar function $\mathbf{h}((t, u(t))$. and the pre-coding filter becomes the inverse of the main channel, e.g., $F_A(T) = h_{AB}^{-1}((T, u(T))$. Note that all derivations below also apply to MIMO system, which we will discuss later. The received signal at Eve's side is:

$$\begin{aligned}\mathbf{R}_E(T) &= h_{AE}\left(T, u(T)\right) h_{AB}^{-1}((T, u(T))\, \mathbf{D}_B(T) + \mathbf{N} \\ &= h_{AB}^{-1}\left(T, u(T)\right) \mathbf{D}_B(T) + \mathbf{N},\end{aligned}$$

after Eve equalizes $h_{AE}\left(T, u(T)\right)$. Omitting $\mathbf{N}$, Eq. (22) expands to

$$I\left(\mathbf{D}_B(T); h_{AB}^{-1}((T, u(T))\, \mathbf{D}_B(T) \mid \mathcal{H}_{AB}(T-1), \mathcal{H}_{AE}(T)\right)$$

To simplify the equation above, consider the conditional probability of $h_{AB}\left(T, u(T)\right)$ given $\mathcal{H}_{AB}(T-1)$. Due to the Markov property,

$$\begin{aligned}&\Pr\left[h_{AB}\left(T, u(T)\right) \mid \mathcal{H}_{AB}(T-1)\right] = \\ &\quad \Pr\left[h_{AB}\left(T, u(T)\right) \mid h_{AB}\left(T-1, u(T-1)\right)\right].\end{aligned}$$

As for the conditional probability of $h_{AB}\left(T, u(T)\right)$ given $\mathcal{H}_{AE}(T)$. Although $h_{AB}\left(t, u(t)\right)$ and $h_{AE}\left(t, u(t)\right)$ are mostly independent, they are correlated at the same time step, since the antenna pattern is the same for $h_{AB}(u)$ and $h_{AE}(u)$, resulting

$$\begin{aligned}&\Pr\left[h_{AB}\left(T, u(T)\right) \mid \mathcal{H}_{AE}(T)\right] = \\ &\quad \Pr\left[h_{AB}\left(T, u(T)\right) \mid h_{AE}\left(T, u(T)\right)\right].\end{aligned}$$

Based on these conditions, we have the following Theorem:

Theorem VI.1. *Assuming the wireless channel has the Markov property, the secrecy leakage of ROBin can be simplified as*[1]*:*

$$\begin{aligned}&I\left(\mathbf{D}_B(T); \mathbf{R}_E(T) \mid \mathcal{H}_{AB}(T-1), \mathcal{H}_{AE}(T)\right) = \\ &I\left(\mathbf{D}_B(T); \mathbf{R}_E(T) \mid h_{AB}\left(T-1, u(T-1)\right), \right. \\ &\qquad\qquad h_{AE}\left(T-1, u(T-1)\right), \\ &\qquad\qquad \left. h_{AE}\left(T, u(T)\right)\right) = \\ &I\left(\mathbf{D}_B(T); \mathbf{R}_E(T) \mid \delta\mathcal{H}_{ABE}(T)\right),\end{aligned} \tag{23}$$

where

$$\begin{aligned}\delta\mathcal{H}_{ABE}(T) = \{\ & h_{AB}\left(T-1, u(T-1)\right), \\ & h_{AE}\left(T-1, u(T-1)\right), \\ & h_{AE}\left(T, u(T)\right)\ \}\end{aligned}$$

This simplification allows us to calculate the numerical secrecy leakage when all the possible values of discretize CSI are in a small range. Next we use numerical results to show the relationship between channel correlation and privacy leakage.

B. Correctness and Insights

1) Single-Antenna Eavesdropper: Alice can apply a reduced ROBin scheme without orthogonal blinding in a single-input and single-output (SISO) system, with Bob and Eve having one regular antenna and Alice having one reconfigurable antenna. To calculate the secrecy leakage, we first generate the CSI with the truncated Gaussian distribution in the range of $(-2, 2)$, then we normalize its real (imaginary) part into four values, i.e. $\mathrm{Re}[\delta\mathcal{H}_{ABE}(T)] \in \{\pm 1.5, \pm 0.5\}$. And for

[1]The proof of this Theorem can be found in our technical report at https://tinyurl.com/y2t4njcx

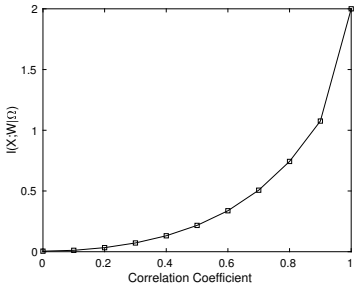

Fig. 2: Secrecy leakage over the channel correlation coefficient between $\mathbf{H}_{AB}$ and $\mathbf{H}_{AB}$.

the message we consider 4QAM, namely that $\mathbf{D}_B(T) = x \in \{\pm 1 + j, \pm 1 - j\}$, then the entropy of the message is $\mathrm{H}(\mathbf{D}_B(T)) = 2$. and $\mathrm{Re}[\mathbf{R}_E(T)] \in \{\pm 1.5, \pm 0.5\}$, $|\mathbf{R}_E(T)| = 16$, $|(\mathbf{D}_B(T), \mathbf{R}_E(T), \delta\mathcal{H}_{ABE}(T))| = 256 \times 2^{10}$ correspondingly. Hence we set the number of the samples to 30 million, which is about 100 times of $|(\mathbf{D}_B(T), \mathbf{R}_E(T), \delta\mathcal{H}_{ABE}(T))|$. The calculated Eq. 23 versus correlation coefficient between $\mathbf{H}_{AB}$ and $\mathbf{H}_{AB}$ is shown in Fig. 2.

We can observe that the leakage increases with the increase of the correlation coefficient between $\mathbf{H}_{AB}$ and $\mathbf{H}_{AB}$, in other words, the information the eavesdropper gained decreases with the decrease of the correlation between $\mathbf{H}_{AB}$ and $\mathbf{H}_{AB}$. This result quantitatively verifies the motivation of our channel randomization strategy: the system becomes more secure after reducing the correlation between the two channels to the receiver and the eavesdropper. And results in [21] shown that a reconfigurable antenna is capable of decreasing the correlation of two channels. Hence introducing a reconfigurable antenna to the system brings us two benefits: actively randomizing wireless channel and reducing correlations among channels.

2) Multi-Antenna Eavesdropper: Alice can apply the full ROBin scheme with orthogonal blinding in a multi-input and single-output (MISO) or multi-input and multi-output (MIMO) system. Assume Eve has multiple antennas. For a given antenna mode, if the number of known symbols is less than the number of Alice's antennas, n_a, Eve cannot find a unique decoding filter. This is because that the least square problem for the LS channel estimation is underdetermined. When the number of known symbols is greater than n_a, the least square problem becomes overdetermined and allows Eve to identify the correct decoding filter. Note that the number of known symbols do not accumulate when Alice reuses the same antenna model at different channel coherent periods. Therefore, as long as Alice switches the antenna mode faster than the duration of n_a symbols, the secrecy leakage of our scheme is low regardless of the number of antennas Eve has.

VII. Performance Evaluation

In this section, we evaluate the performance of our scheme under the practical known-plaintext attack with both simulation and real-world experiments. We start with the overview of simulation setup, and investigate the effects of various parameters. With simulation, we can cover a wide parameter range and establish the operating environment for the known-plaintext attack with a MIMO eavesdropper. Then with an implementation using USRP platform and a rotating RA, we validate the simulation results via experiments.

A. Customized Reconfigurable Antenna

For the channel randomization purpose, we prefer RAs with distinct radiation patterns across different antenna modes. There are different types of RAs in the literature [31], however, most of them are designed for communication purpose so that they only steer to several directions. Hence the resulted radiation patterns are similar for different antenna modes, which make them unsuitable for channel randomization. To better evaluate our ROBin scheme, we build our own RA by rotating two log periodic antennas manufactured by Ettus Research [32]. We first measure all the design parameters for the given log periodic antenna, including arm width, arm spacing and etc., then its radiation pattern is simulated using the antenna toolbox provided by MATLAB, which is illustrated in Fig. 3i. In the simulation, we rotate the antenna every one degree, so that we have 360 antennas modes in total. And in practice, the rotator is constructed with a motor and a microcontroller, in order to rotate the antenna agilely to an arbitrary angle in the azimuth plane. The rotator is illustrated in Fig. 3j, putting with two antennas configured with two RF chains. Note that, we can have various antenna configurations at Alice's side, e.g. Alice can enrich antenna patterns by varying the gain level of each antenna, which can be achieved with power allocation among RF chains. Also, Alice can have more antennas than use and randomly selects one among them for transmission, or randomize the power ratio among antennas to introduce additional randomness to wireless channels as in [19].

B. Simulation Setup

As described in the system model, Alice, Bob and Eve are multi-antenna users with OFDM transmitters. W.l.o.g, we focus our simulation on a setup where Alice has two given log periodic antennas, Bob and Eve have one and two omnidirectional antenna(s) respectively. For data transmission, the 30MHz wide AWGN channel is split into 48 equally spaced sub-channels, and the OFDM frames contain 192 symbols for each sub-channel. To evaluate the effect of Alice's AN, we vary the ratio of AN to the transmitted data signal, namely that Noise to Data Ratio (NDR). With fixed transmit power, the power for data signal is:

$$D = \frac{1}{\mathrm{NDR} + 1} \begin{pmatrix} D_B \\ \mathrm{NDR} \cdot \mathrm{AN} \end{pmatrix} \tag{24}$$

We simulation 100 different environment settings, where five scatters are put for each of them and the data signal are transmitted as 4-QAM symbols. The distance from Eve to Bob is set as 150cm, which is 12 times of the signal wavelength. Most importantly, for all the simulations, we consider the eavesdropper in a more practical sense, instead of the attacker as in theoretical analysis. In particular, the symbols known by attackers are from the well-known protocols in the WiFi

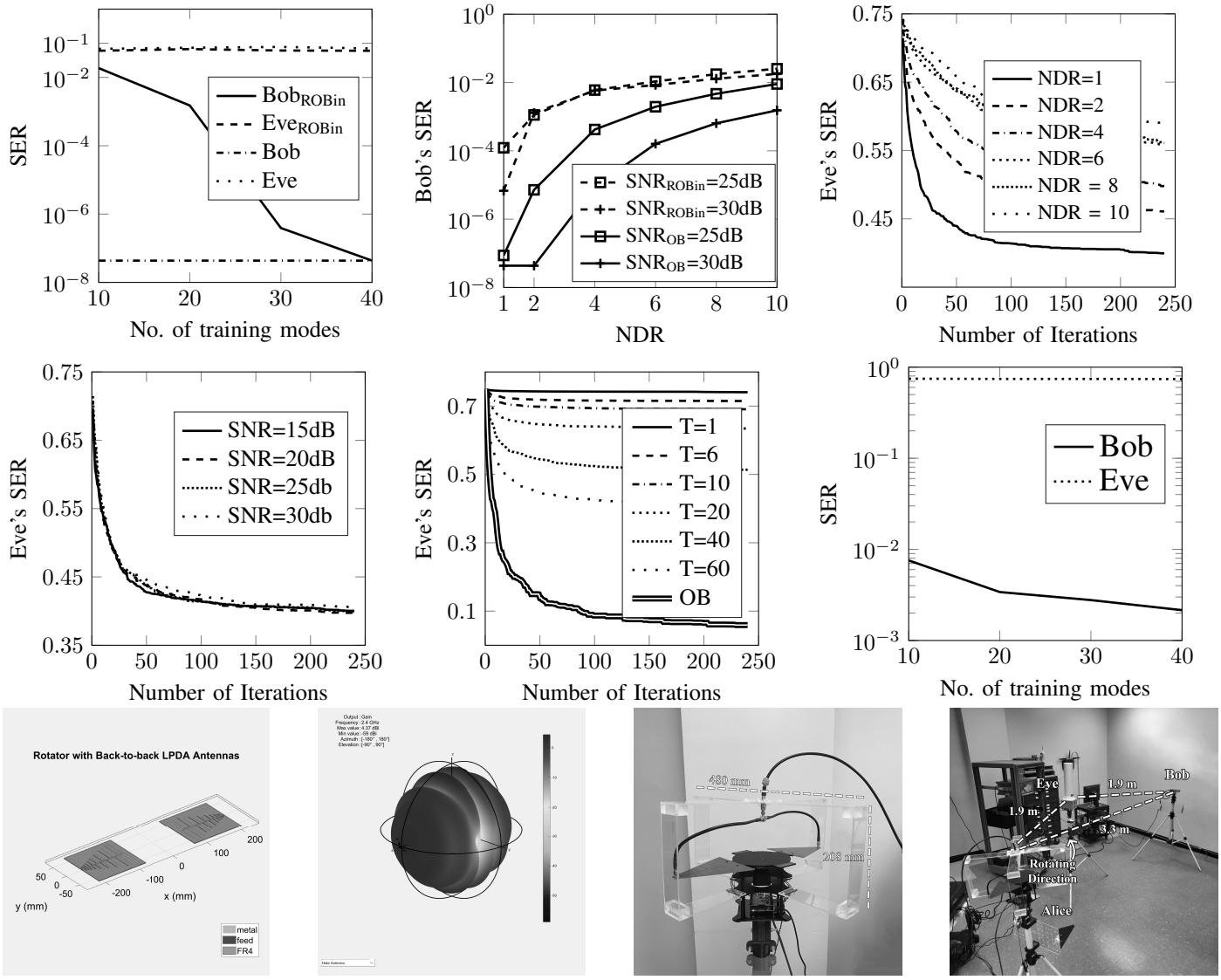

Fig. 3: From top to bottom, left to right: (a) SER of Bob and Eve over the number of training modes. SNR = 25dB; NDR = 1; Eve's SER is obtained after 240 iterations. (b) SER of Bob over Alice's NDR for different SNRs. The number of training modes is 20. (c) Eve's SER over the number of iterations; SNR = 25dB; various NDR. (d) Eve's SER over the number of iterations. NDR = 1; various SNR. (f) Eve's SER over the number of iterations; SNR = 25dB; NDR = 1; various antenna switching period. (g) SER of Bob and Eve over the number of training mode based on the real-world channel data. (h) Platform for RA rotating. (i) Radiation pattern of RA. (j) Real-world rotator. (k) Real-world experiment setup.

frame, though no pilots are needed in transmission phase of ROBin, the attacker is still able to guess parts of symbols from information like addresses. However, the attacker is not able to obtain all the historical data signal in practice. Besides, since AN is not intended for the receiver, it is random data in general, which makes it hard for the attacker to get enough plaintext and identify the correct decoding filter. Correspondingly, we define the switching period T of RA based on an OFDM frame, and 120 frames are sent during the channel coherent time, hence we have $T \in [1, 120]$. For each frame, the attacker is assumed to obtain two symbols. Then if $T = 10$, it means that the transmission mode changes every ten packets, hence for a given transmit filter (computed from the given transmission mode), the attacker has 20 known symbols for filter training.

C. Effect of the number of training modes

Since the estimation of the AoD distribution is based on compressive sensing in ROBin, theoretically, the more training modes we use, the more precise the estimation will be. Fig. 3a illustrates the SER of Bob and Eve over the number of training modes, obtained under ROBin and orthogonal blinding. Here to better show the impact of channel prediction to Bob's SER, we do not change the antenna mode during transmission which is to set $T = 120$, then the only difference of these two schemes is

that ROBin computes the transmit filter based on the predicted channel, while orthogonal blinding uses the measured channel matrix obtained from channel sounding. From Fig. 3a we can see that there is a gap between Bob's SER obtained from two schemes, which is caused by the imperfect channel prediction and the missing channel sounding. However, it decreases with the number of training modes as expected, and when 20 training modes are used, Bob's SER is small enough for communication. On the other hand, Eve's SER obtained after 240 iterations is quite stable under the different number of training modes, this is because the effect of the transmit filter and artificial noise are both filtered out by Eve's receive filter.

D. Effect of artificial noise and channel noise to Bob

Fig. 3b shows Bob's SER with orthogonal blinding and ROBin, at this time the antenna switching period is set as $T = 6$, hence 20 transmission modes are used under a given environmental setting. From Fig. 3b, we can see that Bob's SER decreases as SNR increases under both schemes. Especially, both SNR and NDR have significant impacts on Bob's SER for orthogonal blinding. In contrast, the increase of SNR does not bring much benefit to Bob's SER for ROBin, since Bob's SER is dominated by the precise of channel prediction. Due to the imperfect channel prediction, part of the artificial noise is leaked to Bob's channel, which increases Bob's SER. Fortunately, as long as the NDR is not too large, the communication quality is still guaranteed. For instance, when SNR = 25dB and NDR = 2, Bob can still achieve an average SER of 1.1×10^{-3}.

E. Effect of artificial noise and channel noise to Eve

Theoretically, the higher the NDR is, the higher is the SER on Eve's side. Here we set the antenna switching period as $T = 60$ to provide Eve some advantages. In Fig. 3c, we illustrate how Alice's NDR affects Eve's performance. As we expected, Eve's SER decreases with the increase of NDR. It is worth noticing that, when the power of artificial noise is not too strong, NDR ≤ 4 for instance, we can see that Eve's SER has an obvious reduction with the iterative process; whereas, as the artificial noise becomes stronger, even if the number of iterations increases, the decrease of Eve's SER is not significant. Besides, in Fig. 3d we illustrate how SNR affects Eve's SER. The effect of channel noise to Eve's SER is much weaker than that to Bob's SER, no significant variation for Eve's SER with the increase of SNR. Hence we can conclude that Eve's attack performance is mainly constrained by the power of artificial noise that Alice sent. And there is a tradeoff between the system secrecy (Eve's SER) and the communication quality (Bob's SER) when injecting artificial noise to the channel.

F. Effect of switching period to Eve

Intuitively, the faster the antenna switches, the higher is Eve's SER. In Fig. 3e, we show Eve's SER over the antenna switching period. As we expect, Eve's SER decreases as T increases. When $T = 60$, it is the best case for Eve under ROBin scheme in Fig. 3e, we can see that Eve's SER is still fairly high, which is 0.4047. To quantify ROBin's security improvement, we compute the difference between Eve's SER in ROBin and in orthogonal blinding and normalize it with Eve's SER in the worst case, e.g., the SER of random guessing. For instance, when Alice transmits QPSK (4QAM) symbols, we compute: (SEROB+ESEROBE)/0.75. The result shows we can elevate the eavesdropper's SER by 46% under 4-QAM modulation. When the antenna mode changes rapidly, especially for $T = 1$, we suppress Eve's attack success rate to the level of random guessing. Finally, we vary the number of known symbols in each frame from 2 to 20. And the result shows that Eve's SER does not fluctuate much due to the convergence of the algorithm.

G. Effect of real-world channels

We rotate the RA with the platform in Fig. 3g for the real-world CSI collection. In the experiment, each of our OFDM frames contains 320 symbols and lasts for 0.08s. We collect the CSI data for about 17 seconds and rotate 1 antenna degree every 1/30 seconds, which means the antenna switching period is less than the duration of a frame. To facilitate our simulation process, we set the antenna switching period to $T = 1$ while simulating. Based on the data collected, we studied the effects of all the parameters as the previous simulation results present. However, due to the page limitation, we only show the SER of Bob and Eve over the number of training modes. This result is more important than others because it shows the effectiveness of our channel prediction algorithm. From Fig. 3f we can see that it has a similar trend as in Fig. 3a, which validates the consistency of our simulation and implementation.

VIII. Conclusions

In this paper, we propose an orthogonal-blinding based secret transmission scheme, which is resistant to known-plaintext attack by leveraging reconfigurable antennas to rapidly randomize the channel state during transmission. To enable reliable decoding at the receiver end, we propose a compressive sensing based AoD estimation algorithm to predict Alice-Bob channel and cancel out channel effects at Bob by pre-coding, while still blinding Eve. We formally analyze the security of the scheme using conditional mutual information, which is applicable to both single and multi-antenna eavesdroppers. We show that the secrecy leakage decreases with less channel correlation created by artificial channel randomization, and the leakage is independent of Eve's number of antennas if channel state is switched fast enough. We conduct extensive simulations and real-world experiments to evaluate its performance. Results show that, the communication quality between Alice and Bob remains acceptable, whereas the randomized channel can successfully prevent Eve from launching the known-plaintext attack even if all the historical symbols are known. In the future, we will study other better practical alternatives to OB and analyze the security from the secure degree-of-freedom perspective.

REFERENCES

[1] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: non-invasive security for implantable medical devices," in *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4. ACM, 2011, pp. 2–13.

[2] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *INFOCOM, 2011 Proceedings IEEE*. IEEE, 2011, pp. 1125–1133.

[3] N. Anand, S.-J. Lee, and E. W. Knightly, "Strobe: Actively securing wireless communications using zero-forcing beamforming," in *INFOCOM, 2012 Proceedings IEEE*. Citeseer, 2012, pp. 720–728.

[4] M. Schulz, A. Loch, and M. Hollick, "Practical Known-Plaintext Attacks against Physical Layer Security in Wireless MIMO Systems." in *NDSS*.

[5] Y. Zheng, M. Schulz, W. Lou, Y. T. Hou, and M. Hollick, "Highly Efficient Known-Plaintext Attacks Against Orthogonal Blinding Based Physical Layer Security," vol. 4, no. 1, pp. 34–37.

[6] ——, "Profiling the strength of physical-layer security: A study in orthogonal blinding," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2016, pp. 21–30.

[7] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[8] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, 1978.

[9] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE transactions on information theory*, vol. 24, no. 4, pp. 451–456, 1978.

[10] P. Parada and R. Blahut, "Secrecy capacity of simo and slow fading channels," in *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on*. IEEE, 2005, pp. 2152–2155.

[11] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Information Sciences and Systems, 2007. CISS'07. 41st Annual Conference on*. IEEE, 2007, pp. 905–910.

[12] A. Khisti and G. Wornell, "Secure transmission with multiple antennas: The misome wiretap channel," *arXiv preprint arXiv:0708.4219*, 2007.

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

[14] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas i: The misome wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[15] W. Shen, P. Ning, X. He, and H. Dai, "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time," in *2013 IEEE Symposium on Security and Privacy*. IEEE, 2013, pp. 174–188.

[16] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *Security and Privacy (SP), 2013 IEEE Symposium on*. IEEE, 2013, pp. 160–173.

[17] M. Schulz, A. Loch, and M. Hollick, "Practical known-plaintext attacks against physical layer security in wireless mimo systems." in *NDSS*, 2014.

[18] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, 2005.

[19] H. Hassanieh, J. Wang, D. Katabi, and T. Kohno, "Securing rfids by randomizing the modulation and channel," in *12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15)*, 2015, pp. 235–249.

[20] Y. Hou, M. Li, R. Chauhan, R. M. Gerdes, and K. Zeng, "Message integrity protection over wireless channel by countering signal cancellation: Theory and practice," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*. ACM, 2015, pp. 261–272.

[21] Y. Pan, Y. Hou, M. Li, R. M. Gerdes, K. Zeng, M. A. Towfiq, and B. A. Cetiner, "Message integrity protection over wireless channel: countering signal cancellation via channel randomization," *IEEE Transactions on Dependable and Secure Computing*, 2017.

[22] J. T. Bernhard, "Reconfigurable antennas," *Synthesis lectures on antennas*, vol. 2, no. 1, 2007.

[23] D. Rodrigo, B. A. Cetiner *et al.*, "Frequency, radiation pattern and polarization reconfigurable antenna using a parasitic pixel layer," *IEEE transactions on antennas and propagation*, vol. 62, no. 6, pp. 3422–3427, 2014.

[24] C. Pöpper, N. O. Tippenhauer, B. Danev, and S. Capkun, "Investigation of signal and message manipulations on the wireless channel," in *European Symposium on Research in Computer Security*. Springer, 2011, pp. 40–59.

[25] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE transactions on antennas and propagation*, vol. 34, no. 3, pp. 276–280, 1986.

[26] S. S. Ghassemzadeh, R. Jana, C. W. Rice, W. Turin, and V. Tarokh, "Measurement and modeling of an ultra-wide bandwidth indoor channel," *IEEE Transactions on Communications*, vol. 52, no. 10, pp. 1786–1796, 2004.

[27] N. Czink, X. Yin, H. Ozcelik, M. Herdin, E. Bonek, and B. H. Fleury, "Cluster characteristics in a mimo indoor propagation environment," *IEEE Transactions on Wireless Communications*, vol. 6, no. 4, pp. 1465–1475, 2007.

[28] E. J. Candès and M. B. Wakin, "An introduction to compressive sampling [a sensing/sampling paradigm that goes against the common knowledge in data acquisition]," *IEEE signal processing magazine*, vol. 25, no. 2, pp. 21–30, 2008.

[29] X. Xie, E. Chai, X. Zhang, K. Sundaresan, A. Khojastepour, and S. Rangarajan, "Hekaton: Efficient and practical large-scale mimo," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, 2015, pp. 304–316.

[30] C. C. Tan and N. C. Beaulieu, "On first-order markov modeling for the rayleigh fading channel," *IEEE Transactions on Communications*, vol. 48, no. 12, pp. 2032–2040, 2000.

[31] Z. Li, E. Ahmed, A. M. Eltawil, and B. A. Cetiner, "A Beam-Steering Reconfigurable Antenna for WLAN Applications," vol. 63, no. 1, pp. 24–32. [Online]. Available: http://ieeexplore.ieee.org/document/6948228/

[32] A. Inc., "Lp0965 antenna," https://www.ettus.com/product/details/LP0965.

PROOF OF THEOREM VI.1.

Proof. To prove Theorem VI.1., which states

$$\begin{aligned}&I\left(\mathbf{D}_B(T);\mathbf{R}_E(T)\mid \mathcal{H}_{AB}(T-1),\mathcal{H}_{AE}(T)\right)=\\&I\left(\mathbf{D}_B(T);\mathbf{R}_E(T)\mid \mathcal{H}_{ABE}\left(T-2\right),\delta\mathcal{H}_{ABE}(T)\right)=\\&I\left(\mathbf{D}_B(T);\mathbf{R}_E(T)\mid \delta\mathcal{H}_{ABE}(T)\right),\end{aligned}$$

where

$$\begin{aligned}\mathcal{H}_{ABE}(T-2)=\{\ &\mathcal{H}_{AB}\left(T-2\right),\ \mathcal{H}_{AE}\left(T-2\right)\}\\ \delta\mathcal{H}_{ABE}(T)=\{\ &h_{AB}\left(T-1,u(T-1)\right),\\ &h_{AE}\left(T-1,u(T-1)\right),\\ &h_{AE}\left(T,u(T)\right)\ \}\end{aligned}$$

itis equivalent to prove that given $\delta\mathcal{H}_{ABE}(T)$, $\mathcal{H}_{ABE}(T-2)$ and $(\mathbf{D}_B(T),\mathbf{R}_E(T))$ are conditionally independent. Since the messages $\mathbf{D}_B$ are independent from all the CSI information, and $\mathbf{R}_E(T)$ is a function of $\mathbf{D}_B(T)$ and $h_{AB}^{-1}\left(T,u(T)\right)$ plus some independent additive white Gaussian noise (AWGN), it is similar to prove that given $\delta\mathcal{H}_{ABE}(T)$, $\mathcal{H}_{ABE}(T-2)$ and $h_{AB}^{-1}(T,u(T))$ are conditionally independent, based on the Markov property.

Recall the Markov property of the channels:

$$\begin{aligned}&\Pr\left[h_{AB}\left(T,u(T)\right)\mid \mathcal{H}_{AB}(T-1)\right]=\\&\quad\Pr\left[h_{AB}\left(T,u(T)\right)\mid h_{AB}\left(T-1,u(T-1)\right)\right].\end{aligned}$$

and

$$\begin{aligned}&\Pr\left[h_{AB}\left(T,u(T)\right)\mid \mathcal{H}_{AE}(T)\right]=\\&\quad\Pr\left[h_{AB}\left(T,u(T)\right)\mid h_{AE}\left(T,u(T)\right)\right]\end{aligned}$$

To simplify, we denote $X_1=\mathcal{H}_{AB}(T-2)$, $X_2=h_{AB}(T-1,u(T-1))$, $X_3=h_{AB}(T,u(T))$, and similarly define Y for channel A-E. Then the Markov property can be rewritten as:

$$\begin{aligned}\Pr(X_3|X_1,X_2)&=\Pr(X_3|X_2)\\ \Pr(X_3|Y_1,Y_2,Y_3)&=\Pr(X_3|Y_3)\end{aligned}$$

which is illustrated below:

$$\begin{array}{ccccc}X_1&\longrightarrow&X_2&\longrightarrow&X_3\\ \updownarrow&&\updownarrow&&\updownarrow\\ Y_1&\longrightarrow&Y_2&\longrightarrow&Y_3\end{array}$$

And the CSI can be represented with X and Y in a simpler way as:

$$\begin{aligned}\mathcal{H}_{ABE}(T-2)&=\{\ X_1,\ Y_1\}\\ \delta\mathcal{H}_{ABE}(T)&=\{\ X_2,\ Y_2,\ Y_3\}\\ h_{AB}^{-1}\left(T,u(T)\right)&=X_3^{-1}\end{aligned}$$

Hence our problem is equivalent to prove that given (X_2,Y_2,Y_3), (X_1,Y_1) and X_3 (which is equivalent to X_3^{-1}) are conditionally independent. Then we begin with

$$\begin{aligned}&\Pr(X_1,Y_1,X_3|X_2,Y_2,Y_3)\\&=\Pr(X_3|X_2,Y_2,Y_3)\Pr(X_1,Y_1|X_2,Y_2,X_3,Y_3)\qquad(25a)\end{aligned}$$

(25a) is obtained by expressing the joint probability with the conditional probability, then we focus on simplifying its last term, for which we look at:

$$\begin{aligned}&\Pr(X_3,Y_3|X_1,X_2,Y_1,Y_2)\\&=\Pr(X_3|X_1,X_2,Y_1,Y_2)\Pr(Y_3|X_1,X_2,Y_1,Y_2,X_3)\qquad(26a)\\&=\Pr(X_3|X_2)\Pr(Y_3|Y_2,X_3)\qquad(26b)\\&=\Pr(X_3|X_2,Y_2)\Pr(Y_3|X_2,Y_2,X_3)\qquad(26c)\\&=\Pr(X_3,Y_3|X_2,Y_2)\qquad(26d)\end{aligned}$$

Similarly, (26a) is obtained by expressing the joint probability with the conditional probability. With Markov property of the channels, it is further simplified to (26b). Then we can add more conditional independent variables to it and get (26c), which equals to (26d). (26d) implies that given (X_2,Y_2), (X_1,Y_1) and (X_3,Y_3) are conditionally independent. Then back to (25a), we have

$$\begin{aligned}&\Pr(X_1,Y_1,X_3|X_2,Y_2,Y_3)\\&=\Pr(X_3|X_2,Y_2,Y_3)\Pr(X_1,Y_1|X_2,Y_2,X_3,Y_3)\qquad(27a)\\&=\Pr(X_3|X_2,Y_2,Y_3)\Pr(X_1,Y_1|X_2,Y_2)\qquad(27b)\\&=\Pr(X_3|X_2,Y_2,Y_3)\Pr(X_1,Y_1|X_2,Y_2,Y_3)\qquad(27c)\end{aligned}$$

which means given (X_2,Y_2,Y_3), X_3 and (X_1,Y_1) are conditionally independent. Since X_3^{-1} is a function of X_3, then this conditional independence still holds when we replace X_3 with X_3^{-1}, which implies:

$$\Pr(X_3^{-1}|X_1,Y_1,X_2,Y_2,Y_3)=\Pr(X_3^{-1}|X_2,Y_2,Y_3)\qquad(28)$$

Then we reverse X, Y in (28) back to the CSI, which gives us:

$$\begin{aligned}&\Pr\left[h_{AB}^{-1}\left(T,u(T)\right)|\mathcal{H}_{ABE}(T-2),\delta\mathcal{H}_{ABE}(T)\right]=\\&\Pr\left[h_{AB}^{-1}\left(T,u(T)\right)|\mathcal{H}_{AB}(T-1),\mathcal{H}_{AE}(T)\right]=\\&\Pr\left[h_{AB}^{-1}\left(T,u(T)\right)|\delta\mathcal{H}_{ABE}(T)\right]\qquad(29)\end{aligned}$$

To compute $I\left(\mathbf{D}_B(T);\mathbf{R}_E(T)\mid \mathcal{H}_{AB}(T-1),\mathcal{H}_{AE}(T)\right)$, we ignore the AWGN and consider $\Pr\left(\mathbf{D}_B(T);\hat{\mathbf{R}}_E(T)\mid \mathcal{H}_{AB}(T-1),\mathcal{H}_{AE}(T)\right)$ first, where $\hat{\mathbf{R}}_E(T)=h_{AB}^{-1}((T,u(T))\,\mathbf{D}_B(T)$.

$$
\begin{aligned}
&\Pr\left(\mathbf{D}_B(T), \hat{\mathbf{R}}_E(T) \mid \mathcal{H}_{AB}(T-1), \mathcal{H}_{AE}(T)\right) \\
=&\Pr\left(\mathbf{D}_B(T), h_{AB}^{-1}\left(T, u(T)\right) = \frac{\hat{\mathbf{R}}_E(T)}{\mathbf{D}_B(T)} \mid \mathcal{H}_{AB}(T-1), \mathcal{H}_{AE}(T)\right) && \text{(30a)} \\
=&\Pr\left(\mathbf{D}_B(T) \mid \mathcal{H}_{AB}(T-1), \mathcal{H}_{AE}(T)\right) \\
&\times \Pr\left(h_{AB}^{-1}\left(T, u(T)\right) = \frac{\hat{\mathbf{R}}_E(T)}{\mathbf{D}_B(T)} \mid \mathcal{H}_{AB}(T-1), \mathcal{H}_{AE}(T)\right) && \text{(30b)} \\
=&\Pr\left(\mathbf{D}_B(T) \mid \mathcal{H}_{ABE}(T)\right) \\
&\times \Pr\left(h_{AB}^{-1}\left(T, u(T)\right) = \frac{\hat{\mathbf{R}}_E(T)}{\mathbf{D}_B(T)} \mid \delta\mathcal{H}_{ABE}(T)\right) && \text{(30c)} \\
=&\Pr\left(\mathbf{D}_B(T), \hat{\mathbf{R}}_E(T) \mid \delta\mathcal{H}_{ABE}(T)\right) && \text{(30d)}
\end{aligned}
$$

With the fact that messages are independent from all the CSI information, we can get (30b), and meanwhile get rid of $\mathcal{H}_{ABE}(T-2)$ from $\mathbf{D}_B$'s condition, which gives us the first term of (30c), and with (29) we get the second term of (30c). Then by converting conditional probability to joint probability, we get (30d). Since the AWGN is independent from every term of above equations, we can add it into $\hat{\mathbf{R}}_E$ and get $\mathbf{R}_E$ while above results still holds.

So far, we have proved that

$$
\begin{aligned}
&I\left(\mathbf{D}_B(T); \mathbf{R}_E(T) \mid \mathcal{H}_{AB}(T-1), \mathcal{H}_{AE}(T)\right) = \\
&I\left(\mathbf{D}_B(T); \mathbf{R}_E(T) \mid \delta\mathcal{H}_{ABE}(T)\right)
\end{aligned}
$$

for single antenna system. Next, we present the approach to extend it to MIMO. Note that, for the MIMO system, each element in the Markov chain becomes the channel matrix. Similarly,

$$
\begin{aligned}
&\Pr\left(\mathbf{D}_B(T), \hat{\mathbf{R}}_E(T) \mid \mathcal{H}_{AB}(T-1), \mathcal{H}_{AE}(T)\right) \\
=&\Pr\left(\mathbf{D}_B(T), \mathbf{H}_{AB}^{-1}\left(T, u(T)\right) \in \mathbf{\Gamma} \mid \mathcal{H}_{AB}(T-1), \mathcal{H}_{AE}(T)\right) && \text{(31a)}
\end{aligned}
$$

where

$$
\mathbf{\Gamma} = \{\mathbf{H}_{AB}^{-1}\left(T, u(T)\right) \in \mathbf{\Gamma}, \text{s.t. } \hat{\mathbf{R}}_E(T) = \mathbf{H}_{AB}^{-1}(T, u(T))\mathbf{D}_B(T)\}
$$

and represents a set of matrices where its element is a possible solution for $\mathbf{H}_{AB}^{-1}\left(T, u(T)\right)$. Then we can eliminate $\mathcal{H}_{ABE}(T-2)$ with similar procedures from Eq. (30b) to Eq. (30d).

□