Security-Aware Waveform and Artificial Noise Design for Time-Reversal-Based Transmission

Qian Xu [ID], Pinyi Ren [ID], Qinghe Du [ID], and Li Sun [ID]

Abstract—Among the plenty of studies on physical layer security, multi-antenna signal processing and nodes cooperation are two widely adopted techniques. However, in practical systems there are many single-antenna devices that do not support cooperative transmission either. To guarantee the information security in this scenario, we propose a novel transmission strategy that exploits the temporal characteristics of a multipath fading channel. Specifically, we apply this strategy to a time-reversal-based communication system. We consider a joint design of signal waveform and artificial noise. Based on this approach, specific transmission schemes are designed for the cases with and without eavesdropper's channel state information (CSI), respectively. The numerical results show the superiority of our proposed schemes in terms of security enhancement even when the eavesdropper's CSI is unavailable.

Index Terms—Multipath propagation, physical layer security, time reversal, waveform design, artificial noise, optimization.

Notations: $\mathbf{A}(m,n)$ denotes the element in the mth row and nth column of matrix $\mathbf{A}$. $\mathbb{H}^{+}$ denotes the set of all Hermitian positive semidefinite matrices. $\mathbf{x} \sim \mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Omega})$ denotes the circular symmetric complex Gaussian vector with mean $\boldsymbol{\mu}$ and covariance $\boldsymbol{\Omega}$. $\lambda_{\max}(\mathbf{A}, \mathbf{B})$ denotes the largest generalized eigenvalue of the matrix pair $(\mathbf{A}, \mathbf{B})$.

I. INTRODUCTION

The traditional approach to address confidentiality is using cryptographic algorithms at higher layers while the physical layer has been generally neglected. Recently, the concept of physical layer security (PLS) has attracted much interest for adding one more layer of protection against eavesdropping [1], [2]. One important approach to PLS is to degrade the quality of the received signal at the eavesdropper by using multi-antenna signal processing or cooperative transmission. However, many devices do not have multi-antennas or support complicated protocols for cooperative transmission. In these cases, security assurance is difficult and needs more research effort. On the other hand, most previous works on PLS have assumed flat-fading channels and ignored the multipath propagation effect, which actually provides extra degrees of freedom (DoFs) for the security-enhancing signal design [3].

To tackle the above problems, in this correspondence we propose a novel secure transmission strategy which exploits the temporal characteristics of a multipath fading channel. Specifically, we focus on the single-antenna time-reversal-based (TR-based) communication system.[1] Time reversal is a promising technique for single-carrier wideband communications, especially when the bandwidth is much broader than the current 4G system [4]. By using the multipath channel as a natural filter, TR can focus the signal energy at the intended receiver with a very simple receiver structure. Although the spectral efficiency of TR is not that high, it exhibits lower complexity, reduced sensitivity to frequency offset and a lower peak-to-average power ratio, compared with orthogonal frequency division multiplexing (OFDM).[2]

Different from the rich body of studies on PLS, in this correspondence we consider utilizing the multipath propagation. More specifically, we propose TR-based anti-eavesdropping schemes which adopt a joint design of signal waveform and artificial noise (AN). Compared with [3] where the inter-symbol-interference (ISI) is neglected, our work is based on a more practical communication system. We study the cases with and without eavesdropper's channel state information (CSI), respectively. For each case, the signal waveform and AN are optimized to minimize the eavesdropper's signal-to-interference-plus-noise ratio (SINR), while the intended receiver achieves its signal-quality requirement.

II. SYSTEM MODEL AND TRANSMISSION SCHEMES

We consider a TR-based communication system consisting of a source node S, a destination node B (intended receiver), and an eavesdropper E. All the nodes are equipped with a single antenna. Like [4], [5], we use the sampled channel impulse responses (CIRs) $\mathbf{h}_{\mathrm{B}} = \left[h_{\mathrm{B}}[0] \cdots h_{\mathrm{B}}[L_{\mathrm{B}} - 1] \right]^{T}$ and $\mathbf{h}_{\mathrm{E}} = \left[h_{\mathrm{E}}[0] \cdots h_{\mathrm{E}}[L_{\mathrm{E}} - 1] \right]^{T}$ to model the frequency-selective channels from the source to the destination and the eavesdropper, respectively. Considering whether the information of $\mathbf{h}_{\mathrm{E}}$ is available and the computational complexity, we propose several security-aware transmission schemes, namely, the optimal AN scheme and the optimized null-space-based AN (ONS-AN) scheme for the case with $\mathbf{h}_{\mathrm{E}}$, and the random null-space-based AN (RNS-AN) scheme for the case without $\mathbf{h}_{\mathrm{E}}$. In all the schemes, the transmission is carried out block by block and the channels during one block are unchanged.

Q. Xu, Q. Du, and L. Sun are with the School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: xq1216@stu.xjtu.edu.cn; duqinghe@mail.xjtu.edu.cn; lisun@mail.xjtu.edu.cn).

P. Ren is with the School of Electronic and Information Engineering, Xi'an Jiaotong University and also with Guangdong Xi'an Jiaotong University Academy, Foshan, Guangdong 528300, China (e-mail: pyren@mail.xjtu.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2018.2813318

---

[1]The TR-based technique, which has attracted great research attention [4]–[8], is one of the promising solutions to realize our proposed idea. In fact, our idea can be used in any communication systems under the multipath wireless environment.

[2]As discussed in [9], [10], OFDM is not the only potential technique for communication systems with broad bandwidth and high carrier frequency. The reduced complexity at the transceiver in TR-based systems, plus the signal focusing effect which reduces signal leakage to unintended receivers [6], [8], makes TR an appealing technique for our study. When considering information-theoretic secrecy with optimal wiretap codes, it is more likely to avoid secrecy outage [11] in TR systems due to the signal focusing effect. When considering the traditional cryptographic encryption, the signal focusing effect of TR can make the eavesdropper suffer a higher bit error rate (BER) compared with the intended receiver. Consequently, the eavesdropper will receive a noisier ciphertext and find it more difficult to perform cryptanalysis [2]. The comprehensive comparison between TR and OFDM are beyond the scope of this paper and may be left for future study.

A. Optimal AN Scheme

During each block, a symbol sequence consisting of M data symbols $\{s[m]\}_{m=0}^{M-1}$ is first up-sampled with a rate back-off factor D, where $\mathbb{E}\{|s[m]|^2\} = 1$ for $\forall m \in \mathcal{M}$ with $\mathcal{M} \triangleq \{0, \ldots, M-1\}$. Then, the up-sampled sequence passes through a waveform filter $\{g[n]\}_{n=0}^{L-1}$ of length L. As shown in [5], the output sequence $\{x[n]\}_{n=0}^{L_M-1}$ is

$$x[n] = \sum_{m=0}^{M-1} s[m]g[n - mD], \tag{1}$$

where $L_M = (M-1)D + L$ is the length of the output sequence.

To confront eavesdropping, an AN sequence $\{z[n]\}_{n=0}^{L_M-1}$ is introduced and the transmitted sequence of each block becomes $\{x[n] + z[n]\}_{n=0}^{L_M-1}$. For simplicity, we add zero-padding to the end of each block so that we can treat each block independently. In TR systems, before symbol detection, the destination down-samples the received signal and obtains [5]

$$y_{\mathrm{B}}[m] = \sum_{l=0}^{L_M-1} (x + z)[l] h_{\mathrm{B}}[mD + L - 1 - l] + w_{\mathrm{B}}[m], \tag{2}$$

where $w_{\mathrm{B}}[m]$ is the down-sampled Gaussian noise with zero mean and unit variance.

By using a vector $\mathbf{y}_{\mathrm{B}} = \big[y_{\mathrm{B}}[0] \cdots y_{\mathrm{B}}[M-1]\big]^T$ to denote the down-sampled sequence $\{y_{\mathrm{B}}[m]\}_{m=0}^{M-1}$, (2) can be rewritten in a matrix form as

$$\mathbf{y}_{\mathrm{B}} = \mathbf{Q}_{\mathrm{B}} \tilde{\mathbf{H}}_{\mathrm{B}} (\mathbf{x} + \mathbf{z}) + \mathbf{w}_{\mathrm{B}}, \tag{3}$$

where $\mathbf{x} = \big[x[0] \cdots x[L_M - 1]\big]^T$, $\mathbf{z} = \big[z[0] \cdots z[L_M - 1]\big]^T$, and $\mathbf{w}_{\mathrm{B}} = \big[w_{\mathrm{B}}[0] \cdots w_{\mathrm{B}}[M-1]\big]^T$. Channel matrix $\tilde{\mathbf{H}}_{\mathrm{B}}$ is an $(L_B + L_M - 1) \times L_M$ Toeplitz matrix with $[\mathbf{h}_{\mathrm{B}}^T \mathbf{0}_{1 \times (L_M-1)}]^T$ being its first column. The sampling matrix $\mathbf{Q}_{\mathrm{B}}$ is a $M \times (L_B + L_M - 1)$ sparse matrix with only one element in each row being one and others being zero, $\mathbf{Q}_{\mathrm{B}}(m+1, mD+L) = 1$ for $\forall m \in \mathcal{M}$. It is assumed that $\mathbf{z} \sim \mathcal{CN}(\mathbf{0}, \boldsymbol{\Phi}_z)$ where $\boldsymbol{\Phi}_z = \mathbb{E}\{\mathbf{z}\mathbf{z}^H\}$ is to be optimized to degrade eavesdropper's channel quality.

We now focus on the detection of one symbol $s[m]$ at the destination. In TR-based systems, the detection of $s[m]$ is based on the single sample $y_{\mathrm{B}}[m]$ in (2). To show the effect of ISI clearly, we rewrite $y_{\mathrm{B}}[m]$ as

$$y_{\mathrm{B}}[m] = \underbrace{s[m](h_{\mathrm{B}} * g)[L-1]}_{\text{desired symbol}} + \underbrace{(h_{\mathrm{B}} * z)[mD + L - 1]}_{\text{AN}}$$
$$+ \underbrace{\sum_{k=-(\Delta_2-1), k\neq 0}^{\Delta_2-1} s[m+k](h_{\mathrm{B}} * g)[L-1-kD]}_{\text{ISI}} + \underbrace{w_{\mathrm{B}}[m]}_{\text{noise}}, \tag{4}$$

where $\Delta_1 = \lfloor (L_B - 1)/D \rfloor + 1$ and $\Delta_2 = \lfloor (L-1)/D \rfloor + 1$. The ISI term in (4) represents the worst-case ISI for $s[m]$, $m \in \mathcal{M}$ because when the symbol is located at either the beginning or the end of the transmitted sequence, there are not so many neighboring symbols causing ISI to such an extent.

According to (4) which adopts the worst-case ISI, the worst-case SINR of symbol $s[m]$ takes the form of

$$\gamma_{\mathrm{B},m} = \frac{\mathbf{h}_{\mathrm{B},\Delta_1}^H \mathbf{g}\mathbf{g}^H \mathbf{h}_{\mathrm{B},\Delta_1}}{1 + \sum_{l=1, l\neq \Delta_1}^{\Delta_1+\Delta_2-1} \mathbf{h}_{\mathrm{B},l}^H \mathbf{g}\mathbf{g}^H \mathbf{h}_{\mathrm{B},l} + \mathbf{q}_{\mathrm{B},m}^H \boldsymbol{\Phi}_z \mathbf{q}_{\mathrm{B},m}}, \tag{5}$$

where $\mathbf{g} = \big[g[0] \cdots g[L-1]\big]^T$ is the waveform filter, $\mathbf{q}_{\mathrm{B},m}^H = \hat{\mathbf{e}}_{mD+L}^T \tilde{\mathbf{H}}_{\mathrm{B}}$ with $\hat{\mathbf{e}}_l$ being the lth column of $\mathbf{I}_{L_B+L_M-1}$, and $\mathbf{h}_{\mathrm{B},l}^H$ is the lth row of the decimated matrix $\mathbf{H}_{\mathrm{B}}^d$ given by

$$\mathbf{H}_{\mathrm{B}}^d = \sum_{k=-(\Delta_1-1)}^{\Delta_2-1} \tilde{\mathbf{e}}_{\Delta_1+k} \mathbf{e}_{L-kD}^T \mathbf{H}_{\mathrm{B}}, \tag{6}$$

where $\tilde{\mathbf{e}}_l$ and $\mathbf{e}_l$ are the lth column of $\mathbf{I}_{\Delta_1+\Delta_2-1}$ and $\mathbf{I}_{L_B+L-1}$, respectively. $\mathbf{H}_{\mathrm{B}}$ is a $(L_B + L - 1) \times L$ Toeplitz matrix with the first column being $[\mathbf{h}_{\mathrm{B}}^T \mathbf{0}_{1\times(L-1)}]^T$.

As for the detection of $s[m]$ at the eavesdropper, following the approach in [3], we assume that the eavesdropper can utilize all the received signal samples related to $s[m]$. Denote the number of the related samples as T_{E}, the value of which is equal to the length of $h_{\mathrm{E}}[n] * g[n]$, i.e., $T_{\mathrm{E}} = L_{\mathrm{E}} + L - 1$. Moreover, we assume that the ISI can be completely eliminated while the injected AN cannot, which in fact provides a lower bound of the security performance. After removing the ISI, the received samples related to $s[m]$ can be written as

$$\mathbf{y}_{\mathrm{E},m} = \mathbf{H}_{\mathrm{E}} \mathbf{g} s[m] + \mathbf{Q}_{\mathrm{E},m} \tilde{\mathbf{H}}_{\mathrm{E}} \mathbf{z} + \mathbf{w}_{\mathrm{E}}, \tag{7}$$

where $\mathbf{H}_{\mathrm{E}}$ and $\tilde{\mathbf{H}}_{\mathrm{E}}$ are $T_{\mathrm{E}} \times L$ and $(L_{\mathrm{E}} + L_M - 1) \times L_M$ Toeplitz matrices with the first columns being $[\mathbf{h}_{\mathrm{E}}^T \mathbf{0}_{1\times(L-1)}]^T$ and $[\mathbf{h}_{\mathrm{E}}^T \mathbf{0}_{1\times(L_M-1)}]^T$, respectively. The first term in (7) is the desired symbol without ISI as in [3]. The second term is the AN existing in the received samples related to $s[m]$, where the extraction matrix $\mathbf{Q}_{\mathrm{E},m} = [\mathbf{0}_{T_{\mathrm{E}} \times mD} \mathbf{I}_{T_{\mathrm{E}}} \mathbf{0}_{T_{\mathrm{E}} \times (M-m-1)D}]$. $\mathbf{w}_{\mathrm{E}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ is the AWGN vector.

For the signal model (7), the mutual information at the eavesdropper is $I_{\mathrm{E},m} = \log_2(1 + \gamma_{\mathrm{E},m})$, where the SINR $\gamma_{\mathrm{E},m}$ is given by

$$\gamma_{\mathrm{E},m} = (\mathbf{H}_{\mathrm{E}} \mathbf{g})^H \left(\mathbf{F}_{\mathrm{E},m} \boldsymbol{\Phi}_z \mathbf{F}_{\mathrm{E},m}^H + \mathbf{I} \right)^{-1} \mathbf{H}_{\mathrm{E}} \mathbf{g} \tag{8}$$

with $\mathbf{F}_{\mathrm{E},m} = \mathbf{Q}_{\mathrm{E},m} \tilde{\mathbf{H}}_{\mathrm{E}}$. In this correspondence, we focus on $\gamma_{\mathrm{E},m}$, since any degradation of $\gamma_{\mathrm{E},m}$ can be viewed as the degradation of eavesdropper's channel quality.

With perfect $\mathbf{h}_{\mathrm{E}}$, the optimal AN scheme tries to identify the optimal waveform $\mathbf{g}$ and AN covariance $\boldsymbol{\Phi}_z$ that minimize eavesdropper's SINR[3] under an SINR requirement at the destination. The optimization problem is formulated as

$$\min_{\mathbf{g}, \boldsymbol{\Phi}_z \succeq \mathbf{0}} \quad \max_{m \in \mathcal{M}} \quad \gamma_{\mathrm{E},m} \tag{9a}$$

$$\text{s.t.:} \quad \gamma_{\mathrm{B},m} \geq \gamma_0, \quad \forall m \in \mathcal{M} \tag{9b}$$

$$M\,\mathrm{Tr}\left(\mathbf{g}\mathbf{g}^H\right) + \mathrm{Tr}\left(\boldsymbol{\Phi}_z\right) \leq E_0. \tag{9c}$$

Constraint (9b) is a worst-case SINR requirement by recalling that the SINR defined in (5) is a worst-case SINR. Constraint (9c) accounts for the total energy constraint.

B. ONS-AN Scheme

A simplified design of the above AN injection scheme is the null-space-based AN scheme. By recalling (3), the null-space-based AN is designed as $\mathbf{z} = \mathbf{W}\mathbf{v}$ where the columns of $\mathbf{W}$ form an orthonormal

---

[3] Degrading eavesdropper's channel quality has two-fold benefits. From the viewpoint of information-theoretic secrecy with wiretap codes, it improves the secrecy rate. From the viewpoint of signal detection, it increases eavesdropper's BER, which will decrease the eavesdropper's ability to recover the message correctly. Furthermore, as discussed in [1], [2], the proposed physical-layer scheme can also be combined with cryptography to build a multi-layer security architecture and improve the resilience against eavesdropping.

basis of the null-space of $\mathbf{Q}_B \tilde{\mathbf{H}}_B$ and $\mathbf{v} \sim \mathcal{CN}(\mathbf{0}, \mathbf{V})$ where $\mathbf{V} = \mathbb{E}\{\mathbf{v}\mathbf{v}^H\}$ is an $N_z \times N_z$ positive semidefinite matrix to be optimized with $N_z = L_M - M$. Note that this AN scheme requires $L_M > M$, which can be satisfied by increasing M, i.e., the number of symbols in a transmission block. Thus, the auto-correlation matrix of $\mathbf{z}$ is

$$\mathbf{\Phi}_z^{\mathrm{NS}} = \mathbf{W}\mathbf{V}\mathbf{W}^H. \tag{10}$$

Since the AN is generated in the null-space of $\mathbf{Q}_B \tilde{\mathbf{H}}_B$, the AN term in (4) dose not exist and the worst-case SINR of each symbol takes the same form of

$$\gamma_B^{\mathrm{NS}} = \frac{\mathbf{h}_{B,\Delta_1}^H \mathbf{g}\mathbf{g}^H \mathbf{h}_{B,\Delta_1}}{1 + \sum_{l=1, l \neq \Delta_1}^{\Delta_1 + \Delta_2 - 1} \mathbf{h}_{B,l}^H \mathbf{g}\mathbf{g}^H \mathbf{h}_{B,l}}. \tag{11}$$

With perfect $\mathbf{h}_E$, the target of the ONS-AN scheme is

$$\min_{\mathbf{g}, \mathbf{V} \succeq \mathbf{0}} \quad \max_{m \in \mathcal{M}} \quad \gamma_{\mathrm{E},m}^{\mathrm{NS}} \tag{12a}$$

$$\text{s.t.:} \quad \gamma_B^{\mathrm{NS}} \geq \gamma_0, \tag{12b}$$

$$M\mathrm{Tr}\left(\mathbf{g}\mathbf{g}^H\right) + \mathrm{Tr}\left(\mathbf{W}\mathbf{V}\mathbf{W}^H\right) \leq E_0, \tag{12c}$$

where $\gamma_{\mathrm{E},m}^{\mathrm{NS}} = (\mathbf{H}_E \mathbf{g})^H \left(\mathbf{F}_{\mathrm{E},m} \mathbf{W}\mathbf{V}\mathbf{W}^H \mathbf{F}_{\mathrm{E},m}^H + \mathbf{I}\right)^{-1} \mathbf{H}_E \mathbf{g}$.

C. RNS-AN Scheme

When the eavesdropper's CSI is unavailable, the AN covariance $\mathbf{V}$ in (10) cannot be optimized due to the absence of $\mathbf{h}_E$. Therefore, the RNS-AN scheme distributes energy equally over the AN signal. More specifically, the covariance of the null-space-based AN takes the same form as (10) with $\mathbf{V} = \frac{E_z}{N_z}\mathbf{I}$, where E_z represents the energy for AN.

Generally, for minimizing eavesdropper's SINR, the transmission energy of the information-bearing signal needs to be minimized, which will also leave more energy for injecting AN. Following this, we try to optimize the waveform $\mathbf{g}$ to minimize the energy of the information-bearing signal while the destination can still reach its SINR requirement. This optimization problem can be formulated as

$$\min_{\mathbf{g}} \mathbf{g}^H \mathbf{g} \quad \text{s.t.:} \quad \gamma_B^{\mathrm{NS}} \geq \gamma_0, \; M\mathrm{Tr}\left(\mathbf{g}\mathbf{g}^H\right) \leq E_0, \tag{13}$$

where the expression of γ_B^{NS} has been given in (11).

III. OPTIMAL SOLUTIONS

A. Optimal AN Scheme

To solve problem (9), we introduce a slack variable t and transform problem (9) into an equivalent form as

$$\min_{t, \mathbf{g}, \mathbf{\Phi}_z \succeq \mathbf{0}} \quad t \tag{14a}$$

$$\text{s.t.:} \quad \gamma_{\mathrm{E},m} \leq t, \; \forall m \in \mathcal{M}, \tag{14b}$$

$$(9b) - (9c). \tag{14c}$$

Using Schur's Complement [12], we rewrite (14b) as

$$\mathbf{F}_{\mathrm{E},m} \mathbf{\Phi}_z \mathbf{F}_{\mathrm{E},m}^H - \frac{1}{t}\mathbf{H}_E \mathbf{g}\mathbf{g}^H \mathbf{H}_E^H + \mathbf{I} \succeq \mathbf{0}, \; \forall m \in \mathcal{M}. \tag{15}$$

The problem is still non-convex due to (9b). Thus, we use the semidefinite relaxation (SDR) [13] technique by introducing $\mathbf{G} \triangleq \mathbf{g}\mathbf{g}^H$ with the constraints $\mathrm{rank}(\mathbf{G}) = 1$ and $\mathbf{G} \succeq \mathbf{0}$. The SDR form of problem

(14) is

$$\min_{t, \mathbf{G}, \mathbf{\Phi}_z} \quad t \tag{16a}$$

$$\text{s.t.:} \quad \mathbf{F}_{\mathrm{E},m} \mathbf{\Phi}_z \mathbf{F}_{\mathrm{E},m}^H - \frac{1}{t}\mathbf{H}_E \mathbf{G}\mathbf{H}_E^H + \mathbf{I} \succeq \mathbf{0}, \; \forall m \in \mathcal{M}, \tag{16b}$$

$$\gamma_0 \sum_{l=1, l \neq \Delta_1}^{\Delta_1 + \Delta_2 - 1} \mathbf{h}_{B,l}^H \mathbf{G}\mathbf{h}_{B,l} - \mathbf{h}_{B,\Delta_1}^H \mathbf{G}\mathbf{h}_{B,\Delta_1}$$

$$+ \gamma_0 \mathbf{q}_{B,m}^H \mathbf{\Phi}_z \mathbf{q}_{B,m} + \gamma_0 \leq 0, \; \forall m \in \mathcal{M}, \tag{16c}$$

$$M\mathrm{Tr}\left(\mathbf{G}\right) + \mathrm{Tr}\left(\mathbf{\Phi}_z\right) \leq E_0, \tag{16d}$$

$$\mathbf{\Phi}_z \succeq \mathbf{0}, \; \mathbf{G} \succeq \mathbf{0}. \tag{16e}$$

As a basic property of SDR, only when the SDR is tight, i.e., $\mathrm{rank}(\mathbf{G}^*) = 1$ where $\mathbf{G}^*$ is the optimal solution to problem (16), the optimal values of problems (14) and (16) are equal. The following theorem shows the tightness of SDR.

Theorem 1: If problem (16) is feasible, there exists an optimal solution $(t^*, \hat{\mathbf{G}}, \hat{\mathbf{\Phi}}_z)$, for which $\mathrm{rank}(\hat{\mathbf{G}}) = 1$.

Proof: Let t^* and $(\mathbf{G}^*, \mathbf{\Phi}_z^*)$ denote the optimal objective value and the corresponding optimal solution of (16), respectively. Consider the following power minimization problem

$$\min_{\mathbf{G}, \mathbf{\Phi}_z} \quad M\mathrm{Tr}\left(\mathbf{G}\right) + \mathrm{Tr}\left(\mathbf{\Phi}_z\right) \tag{17a}$$

$$\text{s.t.:} \quad \mathbf{F}_{\mathrm{E},m} \mathbf{\Phi}_z \mathbf{F}_{\mathrm{E},m}^H - \frac{1}{t^*}\mathbf{H}_E \mathbf{G}\mathbf{H}_E^H + \mathbf{I} \succeq \mathbf{0}, \; \forall m \in \mathcal{M}, \tag{17b}$$

$$(16c), (16e). \tag{17c}$$

Problem (17) is convex and can be solved via some convex optimization solvers such as SDPT3 with the toolbox CVX [14]. Denote the optimal solution to problem (17) as $(\hat{\mathbf{G}}, \hat{\mathbf{\Phi}}_z)$. It can be easily verified that $(\mathbf{G}^*, \mathbf{\Phi}_z^*)$ is a feasible solution to (17). Furthermore, since $(\hat{\mathbf{G}}, \hat{\mathbf{\Phi}}_z)$ minimizes the objective function of (17), we have

$$M\mathrm{Tr}(\hat{\mathbf{G}}) + \mathrm{Tr}(\hat{\mathbf{\Phi}}_z) \leq M\mathrm{Tr}(\mathbf{G}^*) + \mathrm{Tr}(\mathbf{\Phi}_z^*) \leq E_0. \tag{18}$$

Combining (17b), (17c), and (18), one can see that $(\hat{\mathbf{G}}, \hat{\mathbf{\Phi}}_z)$ is also an optimal solution to problem (16), since it can achieve the optimal objective value t^* and satisfy all other constraints. Therefore, $(\mathbf{G}^*, \mathbf{\Phi}_z^*)$ and $(\hat{\mathbf{G}}, \hat{\mathbf{\Phi}}_z)$ are equivalent for problem (16) in terms of achieving the optimal objective value.

Next, we show that $\mathrm{rank}(\hat{\mathbf{G}}) = 1$. Since Karush-Kuhn-Tucker (KKT) conditions are necessary conditions for the optimum of convex problems, we now check the KKT conditions of problem (17). The Lagrangian function of problem (17) is

$$L(\mathcal{X}) = M\mathrm{Tr}\left(\mathbf{G}\right) + \mathrm{Tr}\left(\mathbf{\Phi}_z\right)$$

$$- \sum_{m=0}^{M-1} \mathrm{Tr}\left(\mathbf{\Theta}_m \left(\mathbf{F}_{\mathrm{E},m} \mathbf{\Phi}_z \mathbf{F}_{\mathrm{E},m}^H - \frac{1}{t^*}\mathbf{H}_E \mathbf{G}\mathbf{H}_E^H + \mathbf{I}\right)\right)$$

$$+ \sum_{m=0}^{M-1} \lambda_m \left(\sum_{l=1, l \neq \Delta_1}^{\Delta_1 + \Delta_2 - 1} \gamma_0 \mathbf{h}_{B,l}^H \mathbf{G}\mathbf{h}_{B,l} - \mathbf{h}_{B,\Delta_1}^H \mathbf{G}\mathbf{h}_{B,\Delta_1}\right.$$

$$\left. + \gamma_0 \mathbf{q}_{B,m}^H \mathbf{\Phi}_z \mathbf{q}_{B,m} + \gamma_0\right)$$

$$- \mathrm{Tr}(\mathbf{\Lambda}_1 \mathbf{\Phi}_z) - \mathrm{Tr}(\mathbf{\Lambda}_2 \mathbf{G}), \tag{19}$$

where $\mathbf{\Theta}_m \in \mathbb{H}^+$, $\lambda_m \geq 0$, $\mathbf{\Lambda}_1 \in \mathbb{H}^+$, and $\mathbf{\Lambda}_2 \in \mathbb{H}^+$ are the corresponding dual variables associated with constraints (17b)–(17c). $\mathcal{X}$

Algorithm 1: The algorithm to find $(\mathbf{g}^{\mathrm{opt}}, \boldsymbol{\Phi}_z^{\mathrm{opt}})$.

Input: lower bound l, upper bound u, tolerance $\varepsilon > 0$.
1: **repeat**
2:     Solve the feasibility problem (16) with $t = (l + u)/2$.
3:     **if** the problem is infeasible, $l = t$;   **else** $u = t$.
4: **until** $u - l < \varepsilon$.
5: Obtain the optimal value t^*.
6: Solve problem (17) with t^* and obtain $(\hat{\mathbf{G}}, \hat{\boldsymbol{\Phi}}_z)$.
7: Obtain $\mathbf{g}^{\mathrm{opt}}$ by calculating the principal eigenvector of $\hat{\mathbf{G}}$.
8: **return** $(\mathbf{g}^{\mathrm{opt}}, \boldsymbol{\Phi}_z^{\mathrm{opt}})$ with $\boldsymbol{\Phi}_z^{\mathrm{opt}} = \hat{\boldsymbol{\Phi}}_z$.

---

denotes the collection of all primal and dual variables. KKT conditions related to the proof are listed as

$$MI + \frac{1}{t^*}\sum_{m=0}^{M-1}\mathbf{H}_{\mathrm{E}}^H \boldsymbol{\Theta}_m \mathbf{H}_{\mathrm{E}} + \sum_{m=0}^{M-1}\lambda_m\big(\mathbf{U}_{\mathrm{ISI}} - \mathbf{h}_{\mathrm{B},\Delta_1}\mathbf{h}_{\mathrm{B},\Delta_1}^H\big) - \boldsymbol{\Lambda}_2 = \mathbf{0},$$
$$(20)$$

$$\boldsymbol{\Lambda}_2 \mathbf{G} = \mathbf{0}, \tag{21}$$

where $\mathbf{U}_{\mathrm{ISI}} \triangleq \sum_{l=1,l\neq\Delta_1}^{\Delta_1+\Delta_2-1} \gamma_0 \mathbf{h}_{\mathrm{B},l}\mathbf{h}_{\mathrm{B},l}^H$.

Post-multiplying (20) with $\mathbf{G}$ and using (21), we have

$$\boldsymbol{\Psi}\mathbf{G} = \tilde{\lambda}\mathbf{h}_{\mathrm{B},\Delta_1}\mathbf{h}_{\mathrm{B},\Delta_1}^H\mathbf{G}, \tag{22}$$

where $\boldsymbol{\Psi} \triangleq MI + \frac{1}{t^*}\sum_{m=0}^{M-1}\mathbf{H}_{\mathrm{E}}^H \boldsymbol{\Theta}_m \mathbf{H}_{\mathrm{E}} + \tilde{\lambda}\mathbf{U}_{\mathrm{ISI}}$, and $\tilde{\lambda} \triangleq \sum_{m=0}^{M-1}\lambda_m$.

The equation in (22) implies that

$$\mathrm{rank}\,(\boldsymbol{\Psi}\mathbf{G}) = \mathrm{rank}\,\big(\tilde{\lambda}\mathbf{h}_{\mathrm{B},\Delta_1}\mathbf{h}_{\mathrm{B},\Delta_1}^H\mathbf{G}\big) \leq 1. \tag{23}$$

Since $\boldsymbol{\Psi} \succ \mathbf{0}$, we further have

$$\mathrm{rank}(\mathbf{G}) = \mathrm{rank}\,(\boldsymbol{\Psi}\mathbf{G}) \leq 1. \tag{24}$$

The optimal solution $\hat{\mathbf{G}}$ must satisfy condition (24). Moreover, $\hat{\mathbf{G}} = \mathbf{0}$ cannot be a solution. Thus, we have $\mathrm{rank}(\hat{\mathbf{G}}) = 1$. ∎

From Theorem 1 we know that we can obtain the optimal solution to problem (9) by solving (16). When t is fixed, problem (16) becomes a convex feasibility problem [12], which can be easily solved. When t increases from 0 to ∞, there must be a critical point t^* which is the smallest t that makes the feasibility problem (16) feasible. Obviously, t^* is the optimal objective value of (16). The method to find t^* and the corresponding optimal solution $(\mathbf{g}^{\mathrm{opt}}, \boldsymbol{\Phi}_z^{\mathrm{opt}})$ to problem (9) is summarized in Algorithm 1, where we adopt a *bisection* search approach, the number of iterations of which is $\log_2 \frac{u-l}{\varepsilon}$.

B. ONS-AN Scheme

In fact, problem (12) can be solved directly by Algorithm 1. Fortunately, for the null-space-based AN scheme, we can transform constraint (12b) into a second-order cone (SOC) constraint and thus avoid the SDR and one-dimensional search.

By using Schur's Complement and introducing a phase constraint, problem (12) can be rewritten as

$$\min_{t, \mathbf{g}, \mathbf{V} \succeq \mathbf{0}} \quad t \tag{25a}$$

$$\text{s.t.:} \quad \begin{bmatrix} t & \mathbf{g}^H\mathbf{H}_{\mathrm{E}}^H \\ \mathbf{H}_{\mathrm{E}}\mathbf{g} & \mathbf{F}_{\mathrm{E},m}\mathbf{W}\mathbf{V}\mathbf{W}^H\mathbf{F}_{\mathrm{E},m}^H + \mathbf{I} \end{bmatrix} \succeq \mathbf{0}, \forall m \in \mathcal{M}, \tag{25b}$$

$$\sqrt{\gamma_0 + \gamma_0\sum_{l=1,l\neq\Delta_1}^{\Delta_1+\Delta_2-1} |\mathbf{h}_{\mathrm{B},l}^H\mathbf{g}|^2} \leq \mathbf{h}_{\mathrm{B},\Delta_1}^H\mathbf{g}, \tag{25c}$$

$$\mathrm{Im}\{\mathbf{h}_{\mathrm{B},\Delta_1}^H\mathbf{g}\} = 0, \quad (12c). \tag{25d}$$

Note that the constraint $\mathrm{Im}\{\mathbf{h}_{\mathrm{B},\Delta_1}^H\mathbf{g}\} = 0$ incurs no loss of optimality since the values of the objective function and constraint functions in (12) are unchanged when $\mathbf{g}$ undergoes an arbitrary phase rotation. Problem (25) is a convex optimization problem and can be numerically solved via convex optimization toolboxes.

C. RNS-AN Scheme

To solve problem (13), we introduce a unit-norm vector $\mathbf{x}$ and construct the waveform as $\mathbf{g} = \sqrt{E_s}\mathbf{x}$, where $E_s \in (0, E_0/M]$ is a variable to be optimized. Problem (13) can now be reformulated as

$$\min_{\mathbf{x}, E_s} \quad E_s \tag{26a}$$

$$\text{s.t.:} \quad \gamma_{E_s}(\mathbf{x}) \geq \gamma_0, \tag{26b}$$

$$\mathbf{x}^H\mathbf{x} = 1, \quad E_s \leq E_0/M, \tag{26c}$$

where the expression of $\gamma_{E_s}(\mathbf{x})$ is

$$\gamma_{E_s}(\mathbf{x}) = \frac{\mathbf{x}^H\mathbf{h}_{\mathrm{B},\Delta_1}\mathbf{h}_{\mathrm{B},\Delta_1}^H\mathbf{x}}{\mathbf{x}^H\left(\frac{1}{E_s}\mathbf{I} + \sum_{l=1,l\neq\Delta_1}^{\Delta_1+\Delta_2-1}\mathbf{h}_{\mathrm{B},l}\mathbf{h}_{\mathrm{B},l}^H\right)\mathbf{x}}. \tag{27}$$

For given E_s, the maximum value of (27) is $\gamma_{E_s}(\mathbf{x}_{E_s}^*) = \lambda_{\max}\big(\mathbf{h}_{\mathrm{B},\Delta_1}\mathbf{h}_{\mathrm{B},\Delta_1}^H, \frac{1}{E_s}\mathbf{I} + \sum_{l=1,l\neq\Delta_1}^{\Delta_1+\Delta_2-1}\mathbf{h}_{\mathrm{B},l}\mathbf{h}_{\mathrm{B},l}^H\big)$ where $\mathbf{x}_{E_s}^*$ is the eigenvector corresponding to $\gamma_{E_s}(\mathbf{x}_{E_s}^*)$. To minimize E_s, we first maximize $\gamma_{E_s}(\mathbf{x})$ by setting $\mathbf{x}$ as $\mathbf{x}_{E_s}^*$. Moreover, it can be easily verified that $\gamma_{E_s}(\mathbf{x}_{E_s}^*)$ is a monotonically increasing function of E_s. Therefore, solving problem (26) is equivalent to finding the unique solution E_s^* satisfying $\gamma_{E_s^*}(\mathbf{x}_{E_s^*}^*) = \gamma_0$. To find E_s^*, we use the *bisection* search algorithm with the search interval $(0, E_{\max}]$ where $E_{\max} = E_0/M$ and the tolerance ε. With the obtained E_s^* and the total energy constraint E_0, the energy left for AN is $E_z^* = E_0 - ME_s^*$. Thus, the covariance matrix of the injected AN is $\boldsymbol{\Phi}_z = \frac{E_z^*}{N_z}\mathbf{W}\mathbf{W}^H$ and the optimal waveform is $\mathbf{g} = \sqrt{E_s^*}\mathbf{x}_{E_s^*}^*$.

D. Complexity Analysis

Using the approach in [15], we can derive the computational complexities of the optimal AN scheme and the ONS-AN scheme, i.e., problems (16) and (25). For the RNS-AN scheme, the outer approach is a bisection method with complexity $\log_2 \frac{E_{\max}}{\varepsilon}$, and the inner approach is generalized eigenvalue decomposition with complexity order $\mathcal{O}\left(n^3\right)$, where n is the size of the matrix. The complexities of the three schemes are shown in Table I. From Table I, one can see that all the schemes are polynomial-time solvable and the RNS-AN scheme has the lowest complexity.

IV. SIMULATION RESULTS

This section presents some numerical results to evaluate the performance of the proposed schemes. Furthermore, when the perfect $\mathbf{h}_{\mathrm{E}}$ is available, we introduce a baseline scheme called No AN (N-AN) scheme which is the solution to problem (25) with $\mathbf{V} = \mathbf{0}$. In the simulations, each element of $\mathbf{h}_{\mathrm{B}}$ and $\mathbf{h}_{\mathrm{E}}$ follows the independent $\mathcal{CN}(0,1)$ distribution and we set $M = 3$, $D = 3$, $L_{\mathrm{B}} = 7$, $L_{\mathrm{E}} = 7$, and $\varepsilon = 10^{-3}$, unless explicitly stated. All the following results are obtained by averaging over 1000 channel realizations.

Fig. 1 depicts the maximum eavesdropper's SINR versus the total energy constraint with $\gamma_0 = 4$ dB. As shown in Fig. 1, the proposed three AN-aided schemes can make the eavesdropper's SINR less than that of the destination while the N-AN scheme cannot. This observation shows the importance of AN injection in obtaining a non-zero secrecy rate [1]. It can be also seen from Fig. 1 that the three AN-aided

TABLE I
COMPLEXITY ANALYSIS OF THE THREE TRANSMISSION SCHEMES

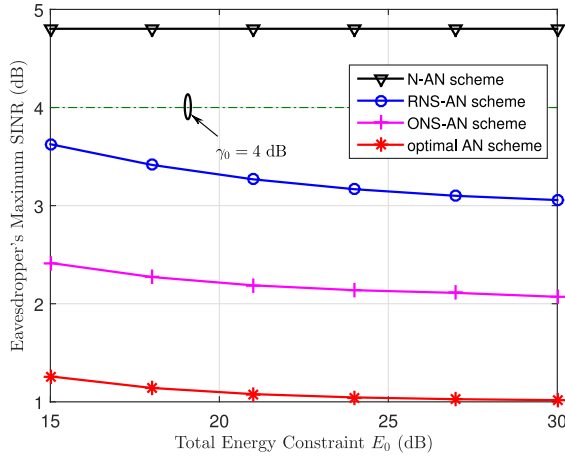| Scenario	Scheme	Complexity Order
With E's CSI	Optimal AN scheme	$\log_2 \frac{u-l}{\varepsilon} \cdot \sqrt{MT_E + L_M + L} \cdot n \cdot \left[\left(MT_E^3 + L_M^3 + L^3 \right) + n \left(MT_E^2 + L_M^2 + L^2 \right) + n^2 \right]$, where $n = \mathcal{O}\left(L_M^2 + L^2 \right)$
	ONS-AN scheme	$\sqrt{MT_E + L} \cdot n \cdot \left[\left(MT_E^3 + L^3 \right) + n \cdot \left(MT_E^2 + L^2 \right) + (\Delta_1 + \Delta_2)^2 + n^2 \right]$, where $n = \mathcal{O}\left((L_M - M)^2 + L \right)$
Without E's CSI	RNS-AN scheme	$\log_2 \frac{E_{\max}}{\varepsilon} \cdot L^3$

Fig. 1. Eavesdropper's maximum SINR as a function of total energy constraint with $L = 7$ and $\gamma_0 = 4$ dB.
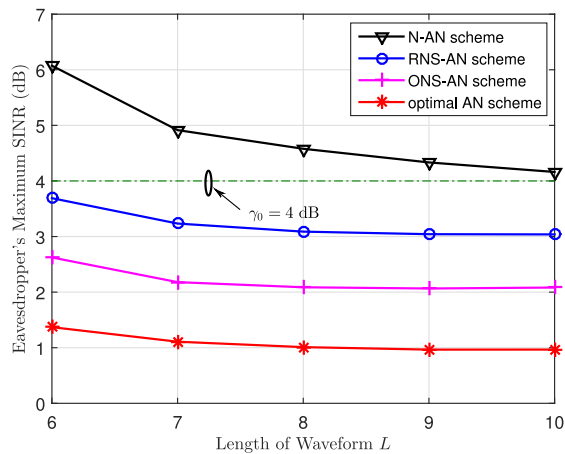

Fig. 2. Eavesdropper's maximum SINR as a function of waveform length with $\gamma_0 = 4$ dB and $E_0 = 25$ dB.

schemes yield decreasing eavesdropper's SINRs with the increase of E_0 while the performance of the N-AN scheme remains unchanged. This is expected because once the SINR requirement at the destination is satisfied, there is no need to further improve the transmission energy if no AN is injected.

Fig. 2 plots the maximum eavesdropper's SINR versus the waveform length. It is observed that the eavesdropper's SINR first decreases and then converges to a value floor, especially for the three AN-aided schemes. This is because longer waveform length offers higher space dimension for the design of signal and AN, which benefits the destination. However, too large L also incurs significant ISI and provides the eavesdropper with high degrees of freedom to suppress AN, which limits the further decreasing of eavesdropper's SINR. Therefore, as

illustrated in Fig. 2, for the AN-aided schemes, the waveform length should be set a little larger than $L_B = 7$ to achieve a good performance.

V. CONCLUSIONS

In this correspondence, we have studied the anti-eavesdropping issue for the TR-based transmission. According to whether the CSI of the eavesdropper is available, we have proposed three transmission schemes making use of security-aware waveform and AN. The optimal solutions to the proposed schemes have been obtained, respectively. The simulation results show that the introduction of properly designed AN can significantly degrade eavesdropper's channel. Moreover, the security performance can be further improved by appropriately increasing the waveform length.

REFERENCES

[1] A. Mukherjee, S. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tut.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[2] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B. J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Sec.*, vol. 6, no. 3, pp. 532–540, Sep. 2011.

[3] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, "Waveform design for secure SISO transmissions and multicasting," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1864–1874, Sep. 2013.

[4] Y. Chen, Y.-H. Yang, F. Han, and K. J. Ray Liu, "Time-reversal wideband communications," *IEEE Signal Process. Lett.*, vol. 20, no. 12, pp. 1219–1222, Dec. 2013.

[5] E. Yoon, S.-Y. Kim, and U. Yun, "A time-reversal-based transmission using predistortion for intersymbol interference alignment," *IEEE Trans. Commun.*, vol. 63, no. 2, pp. 455–465, Feb. 2015.

[6] L. Wang, R. Li, C. Cao, and G. L. Stüber, "SNR analysis of time reversal signaling on target and unintended receivers in distributed transmission," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 2176–2191, May 2016.

[7] N. Guo, B. M. Sadler, and R. C. Qiu, "Reduced-complexity UWB time-reversal techniques and experimental results," *IEEE Trans. Wireless Commun.*, vol. 6, no. 12, pp. 4221–4226, May 2007.

[8] Y. Chen, B. Wang, Y. Han, H. Q. Lai, Z. Safar, and K. J. R. Liu, "Why time reversal for future 5G wireless?" *IEEE Signal Process. Mag.*, vol. 33, no. 2, pp. 17–26, Mar. 2016.

[9] J. Andrews *et al.*, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[10] A. Ghosh *et al.*, "Millimeter-wave enhanced local area systems: A high-data-rate approach for future wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1152–1163, Jun. 2014.

[11] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[12] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge Univ. Press, 2004.

[13] Z.-Q. Luo, W.-K.Ma, A. M.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.

[14] M. Grant and S. Boyd, CVX: MATLAB Software for Disciplined Convex Programming, Apr. 2011. [Online]. Available: http://cvxr.com/cvx

[15] K.-Y. Wang, A. M.-C. So, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: Tractable approximations by conic optimization," *IEEE Trans. Signal Process.*, vol. 62, no. 21, pp. 5690–5705, Nov. 2014.