SECURE WAVEFORMS FOR SISO CHANNELS

Ming Li, Sandipan Kundu, Dimitris A. Pados†, Stella N. Batalama

Department of Electrical Engineering
The State University of New York at Buffalo
Buffalo, NY 14260 USA
E-mail: {mingli,skundu,pados,batalama}@buffalo.edu

ABSTRACT

We develop a novel waveform design approach to minimize the likelihood that a message transmitted wirelessly between trusted single-antenna nodes is intercepted by an eavesdropper. In particular, first, with knowledge of the eavesdropper's channel state information (CSI) we find the optimal waveform and transmit energy that minimize the signal-to-interference-plus-noise ratio (SINR) at the output of the eavesdropper's maximum-SINR linear filter, while at the same time provide the intended receiver with a required pre-specified SINR at the output of its own max-SINR filter. Next, if prior knowledge of the eavesdropper's CSI is unavailable, we design a waveform that maximizes the amount of energy available for generating disturbance to eavesdroppers, termed artificial noise (AN), while the SINR of the intended receiver is maintained at the pre-specified level. Simulation studies demonstrate our analytical developments and illustrate the benefits of the designed waveforms on securing single-input single-output (SISO) transmissions.

Index Terms— Artificial noise, eavesdropping, physical-layer security, power allocation, signal-to-interference-plus noise ratio, SISO wiretap channel, waveform design.

1. INTRODUCTION

By its broadcast nature, the wireless medium renders wireless networks ubiquitously accessible and inherently non-secure. Commonly used wireless security methods rely on cryptographic (encryption) and steganographic (covert communication) means employed at upper layers of the wireless network. It is still highly desirable, however, to enhance core security of wireless communications by reducing the likelihood that propagating signals are intercepted by eavesdroppers in the first place. As a result, there has been growing interest in the development of physical layer security mechanisms for the wireless link.

While many works focus on information-theoretic aspects and calculation/analysis of the achievable secrecy capacity [1]-[19], there is a growing sense of urgency from the signal processing perspective to provide actual algorithmic security solutions that weaken the eavesdroppers' intercepted signal and materialize -at least partly- the information theoretic secrecy capacity promises. Transmit (and receive) beamforming designs [20]-[25] which utilize the spatial degrees of freedom were seen to enhance the physical layer secrecy of wireless communications by avoiding eavesdroppers' interception efforts as much as possible.

In this present work, we consider the problem of secure transmissions over a multipath single-input single-output (SISO) channel where both transmitter and intended receiver have only one antenna. In parallel to beamforming approaches [20]-[25] which require multiple transmit (and receive) antennas to weaken eavesdroppers' receptions, we turn our attention to waveform design -another meaningful idea in physical-layer secrecy- which can exploit the temporal characteristics of a SISO multipath fading channel between trusted single-antenna nodes. We propose easy to compute waveform and energy designs with or without knowledge of the eavesdropper's channel state information (CSI) that weaken eavesdropper's reception while guaranteeing authorized reception at prescribed signal-to-interference-plus-noise (SINR) levels. Simulation results validate the effectiveness of the waveform and energy design to provide physical-layer security in SISO wiretap channels. It is interesting to point out that the design formulation described above is similar to cognitive radio (CR) application problems. Protecting primary users from being interfered by secondary users [26]-[31] parallels the problem of preventing eavesdroppers from overhearing.

2. SYSTEM MODEL

We consider a wireless transmission to an intended receiver in the presence of an eavesdropper. For convenience, we follow the common -whimsical- language in the field and name the transmitter, intended receiver, and eavesdropper, Alice, Bob, and Eve, respectively.

Alice will be attempting to transmit confidential messages to Bob securely with the aid of an appropriately crafted waveform. The transmitted signal is

$$u(t) = \sum_{n=0}^{\infty} \sqrt{E} b(n) s(t - nT) e^{j2\pi f_c t} \qquad (1)$$

where f_c is the carrier frequency, $b(n) \in \{\pm 1\}$, $n = 1, 2, \ldots$, is the nth transmitted information bit, $E > 0$ represents trans-

†Corresponding author.

mitted energy per bit with bit period T, and $s(t)$ is the unit-energy ($\int_0^T |s(t)|^2 dt = 1$) complex continuous waveform of the form

$$s(t) = \sum_{l=0}^{L-1} \mathbf{s}(l)\psi(t - lT_c) \tag{2}$$

where $\mathbf{s}(l) \in \mathbb{C}$, $l = 0, 1, \ldots, L-1$, are to be designed/optimized and $\psi(t)$ is the continuous pulse shaper function with duration $T_c = T/L$ assumed to be given and fixed (for example, ideal square pulse, raised cosine, or otherwise).

The transmitted signal is modeled to propagate to Bob and Eve over SISO multipath Rayleigh fading channels and experience additive white Gaussian noise (AWGN) and interference -potentially- from other concurrent transmissions. After carrier demodulation and $\psi(\cdot)$-pulse matched filtering over a presumed multipath extended data bit period of $L_M = L + M - 1$ pulses where M is the number of resolvable multipaths[1], the data vector $\mathbf{y}_{b/e}(n) \in \mathbb{C}^{L_M}$ received by Bob (subscript b) or Eve (subscript e) takes the following general form

$$\mathbf{y}_{b/e}(n) = \sqrt{E}b(n)\mathbf{H}_{b/e}\mathbf{s} + \mathbf{i}_{b/e} + \mathbf{z}_{b/e} + \mathbf{n}_{b/e}, \quad n = 1, 2, \ldots, \tag{3}$$

where $\mathbf{H}_{b/e} \in \mathbb{C}^{L_M \times L}$ is the multipath channel matrix between Alice and Bob/Eve

$$\mathbf{H}_{b/e} \triangleq \begin{bmatrix} h_{b/e,1} & 0 & \ldots & 0 & 0 \\ h_{b/e,2} & h_{b/e,1} & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ h_{b/e,M} & h_{b/e,M-1} & & 0 & 0 \\ 0 & h_{b/e,M} & & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & h_{b/e,M} & h_{b/e,M-1} \\ 0 & 0 & \ldots & 0 & h_{b/e,M} \end{bmatrix} \tag{4}$$

with entries $h_{b/e,m} \in \mathbb{C}$, $m = 1, \ldots, M$, considered as complex Gaussian random variables to model fading phenomena, $\mathbf{i}_{b/e} \in \mathbb{C}^{L_M}$ denotes multipath induced inter-symbol-interference (ISI), $\mathbf{z}_{b/e} \in \mathbb{C}^{L_M}$ represents comprehensively interference to Bob/Eve from other potential concurrent transmitters, and $\mathbf{n}_{b/e}$ is a zero-mean additive white Gaussian noise (AWGN) vector with autocorrelation matrix $\sigma_{b/e}^2 \mathbf{I}_{L_M}$. Since the effect of ISI is, arguably, negligible for applications of interest where the number of resolvable multipaths M is much less than the number of pulses L, for mathematical and notational convenience we will not consider the ISI terms in our theoretical developments that follow[2]. Thus, Bob/Eve's received signal in (3) is simplified/approximated by

$$\mathbf{y}_{b/e}(n) = \sqrt{E}b(n)\mathbf{H}_{b/e}\mathbf{s} + \mathbf{z}_{b/e} + \mathbf{n}_{b/e}, \quad n = 1, 2, \ldots . \tag{5}$$

Information bit detection at Bob is carried out optimally in second-order statistics terms via linear maximum SINR filtering (or, equivalently, minimum mean square error filtering) as follows

$$\widehat{b}_b(n) = \text{sgn}\left\{\mathfrak{Re}\{\mathbf{w}_{maxSINR,b}^H \mathbf{y}_b(n)\}\right\}, \quad n = 1, 2, \ldots, \tag{6}$$

where $\mathbf{w}_{maxSINR,b} = c\mathbf{R}_b^{-1}\mathbf{H}_b\mathbf{s} \in \mathbb{C}^{L_M}$, $c > 0$, is the maximum SINR filter and $\mathbf{R}_b \triangleq \mathbb{E}\{(\mathbf{z}_b + \mathbf{n}_b)(\mathbf{z}_b + \mathbf{n}_b)^H\} = \mathbb{E}\{\mathbf{z}_b\mathbf{z}_b^H\} + \sigma_b^2\mathbf{I}_{L_M} \succ 0$ is the autocorrelation matrix of the combined total additive channel disturbance. The output SINR of $\mathbf{w}_{maxSINR,b}$ can be calculated to be

$$\begin{aligned} \text{SINR}_b &\triangleq \frac{\mathbb{E}\{|\mathbf{w}_{maxSINR,b}^H(\sqrt{E}b\mathbf{H}_b\mathbf{s})|^2\}}{\mathbb{E}\left\{|\mathbf{w}_{maxSINR,b}^H(\mathbf{z}_b + \mathbf{n}_b)|^2\right\}} \\ &= E\mathbf{s}^H\mathbf{H}_b^H\mathbf{R}_b^{-1}\mathbf{H}_b\mathbf{s} = E\mathbf{s}^H\mathbf{Q}_b\mathbf{s} \end{aligned} \tag{7}$$

where we define $\mathbf{Q}_b \triangleq \mathbf{H}_b^H\mathbf{R}_b^{-1}\mathbf{H}_b$, $\mathbf{Q}_b \succ 0$.

We consider as a "worst-case" to Alice and Bob the scenario under which Eve has perfect knowledge of the multipath channel coefficients $[h_{e,1}, \ldots, h_{e,M}]$ between Alice and Eve, as well as of the waveform $\mathbf{s}$ used by Alice. With this information, Eve attempts to extract/retrieve message bits via her own linear maximum SINR filter $\mathbf{w}_{maxSINR,e} = c\mathbf{R}_e^{-1}\mathbf{H}_e\mathbf{s} \in \mathbb{C}^{L_M}$, $c > 0$, $\mathbf{R}_e \triangleq \mathbb{E}\{\mathbf{z}_e\mathbf{z}_e^H\} + \sigma_e^2\mathbf{I}_{L_M} \succ 0$. The output SINR of the filter $\mathbf{w}_{maxSINR,e}$ is given by

$$\begin{aligned} \text{SINR}_e &\triangleq \frac{\mathbb{E}\{|\mathbf{w}_{maxSINR,e}^H(\sqrt{E}b\mathbf{H}_e\mathbf{s})|^2\}}{\mathbb{E}\left\{|\mathbf{w}_{maxSINR}^H(\mathbf{z}_e + \mathbf{n}_e))|^2\right\}} \\ &= E\mathbf{s}^H\mathbf{H}_e^H\mathbf{R}_e^{-1}\mathbf{H}_e\mathbf{s} = E\mathbf{s}^H\mathbf{Q}_e\mathbf{s} \end{aligned} \tag{8}$$

where we define $\mathbf{Q}_e \triangleq \mathbf{H}_e^H\mathbf{R}_e^{-1}\mathbf{H}_e$, $\mathbf{Q}_e \succ 0$.

From an information theoretic perspective, as long as $\text{SINR}_b > \text{SINR}_e$ there exists in theory a sequence of coding schemes in increasing block-length such that, by adjusting the transmitting energy appropriately, *only* Bob can perfectly decode and obtain the message from Alice while Eve fails. In a practical realistic secure wireless transmission application, we wish that Bob can receive Alice's signal at a desired SINR level that corresponds to an acceptable bit-error-rate (BER), while Eve can only have far, far inferior SINR and BER reception performance. In the next section, we attempt to lay the foundation for such a development utilizing Alice's transmit waveform vector $\mathbf{s}$ and transmit energy $E > 0$ as security design parameters.

3. SECURE WAVEFORM DESIGN

3.1. Known Eavesdropper Channel

We first consider the scenario under which Alice/Bob know Eve's channel $\mathbf{H}_e$ and disturbance autocorrelation matrix $\mathbf{R}_e$. Our objective, in this case, is to find the transmission bit energy E and the complex-valued normalized waveform $\mathbf{s}$ used by Alice that minimize SINR_e under the constraint that Bob achieves its pre-determined SINR requirement γ. I.e., we would like to identify the optimal pair

$$(E, \mathbf{s})^{opt} = \arg \min_{E>0,\, \mathbf{s}\in\mathbb{C}^L} E\mathbf{s}^H\mathbf{Q}_e\mathbf{s} \tag{9}$$

$$\text{s. t.} \quad E\mathbf{s}^H\mathbf{Q}_b\mathbf{s} \geq \gamma\,, \tag{10}$$

$$\mathbf{s}^H\mathbf{s} = 1\,, \tag{11}$$

$$E \leq E_{max}\,, \tag{12}$$

[1] Without loss of generality and for simplicity in notation, we assume the multipath channels Alice-to-Bob and Alice-to-Eve to have the same number of resolvable paths.

[2] However, naturally, ISI will be considered and accounted for in our simulation studies.

where E_{max} denotes the maximum available/allowable bit energy for the transmitter.

The constrained optimization problem (9)-(12) is non-convex. It is easy to verify that (10) always holds with equality at an optimal point. Therefore, for any given $\mathbf{s}$, the optimal transmit energy can be calculated at

$$E = \gamma/(\mathbf{s}^H \mathbf{Q}_b \mathbf{s}). \tag{13}$$

By applying (13) to (9)-(12), the objective function can be reformulated as having only $\mathbf{s}$ to be optimized,

$$\mathbf{s}^{opt} = \arg \min_{\mathbf{s}\in\mathbb{C}^L} \frac{\mathbf{s}^H \mathbf{Q}_e \mathbf{s}}{\mathbf{s}^H \mathbf{Q}_b \mathbf{s}} \tag{14}$$

$$\text{s. t. } \mathbf{s}^H \mathbf{Q}_b \mathbf{s} \geq \frac{\gamma}{E_{max}}\,, \tag{15}$$

$$\mathbf{s}^H \mathbf{s} = 1\,. \tag{16}$$

Now, our problem is to find a normalized waveform vector $\mathbf{s}$ to minimize the SINR ratio (generalized Rayleigh quotient) $\frac{\text{SINR}_e}{\text{SINR}_b} = \frac{\mathbf{s}^H \mathbf{Q}_e \mathbf{s}}{\mathbf{s}^H \mathbf{Q}_b \mathbf{s}}$ between Eve and Bob under constraint (15). It is clear that constraint (15) may be satisfied and the optimization problem is feasible/solvable, only if the maximum eigenvalue of $\mathbf{Q}_b$ is no less than γ/E_{max}. If we ignore constraint (15) for a moment, then the waveform to minimize the SINR ratio is the familiar generalized eigenvector solution given by the following proposition.

Proposition 1: Let $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_L$ be the (normalized) generalized eigenvectors of matrices $(\mathbf{Q}_e, \mathbf{Q}_b)$ with corresponding eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_L$, i.e. $\mathbf{Q}_e \mathbf{p}_i = \lambda_i \mathbf{Q}_b \mathbf{p}_i$, $i = 1, \ldots, L$. The normalized waveform to minimize the generalized Rayleigh quotient in (14) is the generalized eigenvector

$$\mathbf{s} = \mathbf{p}_L \tag{17}$$

with corresponding smallest eigenvalue (and attained minimum quotient/ratio) λ_L. ■

The eigen-design waveform in (17) is *the optimal solution with Alice transmit energy* $E = \gamma/\mathbf{p}_L^H \mathbf{Q}_b \mathbf{p}_L$, if $\mathbf{s} = \mathbf{p}_L$ happens to satisfy (15) which is a common case. If, however, (15) is not satisfied, we have to return to problem (9)-(12) and examine its Karush-Kuhn-Tucker (KKT) conditions[3]. The findings are summarized in the following proposition whose proof is omitted due to space limitation.

Proposition 2: Consider the solvable (maximum eigenvalue of $\mathbf{Q}_b$ no less than γ/E_{max}) optimization problem (14)-(16) and assume that solution (17) does not satisfy constraint (15). Then, the following KKT conditions are necessary for an $\mathbf{s}$ to be optimal

$$(\mathbf{Q}_e + \mu \mathbf{I})\mathbf{s} = \beta \mathbf{Q}_b \mathbf{s},\ \beta > 0,\ \mu > 0, \tag{18}$$

$$\mathbf{s}^H \mathbf{Q}_b \mathbf{s} = \tfrac{\gamma}{E_{max}}\,, \tag{19}$$

$$\mathbf{s}^H \mathbf{s} = 1\,. \tag{20}$$

■

[3]The strong Lagrangian duality of (9)-(12) was proven in [32].

While, unfortunately, we cannot have closed-form expressions for $\mathbf{s}$ from the above KKT conditions, we can pursue a numerical solution easily. Condition (18) indicates that the optimal $\mathbf{s}$ is a generalized eigenvector of the matrices $(\mathbf{Q}_e + \mu \mathbf{I}, \mathbf{Q}_b)$. For any given value of $\mu \geq 0$, let $\mathbf{q}_L(\mu)$ denote the generalized eigenvector of $(\mathbf{Q}_e + \mu \mathbf{I}, \mathbf{Q}_b)$ that has minimum eigenvalue $\beta(\mu)$. We know that $\mathbf{q}_L^H(\mu = 0)\mathbf{Q}_b \mathbf{q}_L(\mu = 0) < \gamma/E_{max}$. We can easily verify that $\mathbf{q}_L^H(\mu)\mathbf{Q}_b \mathbf{q}_L(\mu)$ is strictly monotonically increasing in $\mu \in [0, \infty)$. Based on this property, we propose to solve the KKT necessary conditions (18)-(20) by numerically increasing the searching parameter $\mu > 0$ from zero to a value μ^{opt} such that $|\mathbf{q}_L^H(\mu^{opt})\mathbf{Q}_b \mathbf{q}_L(\mu^{opt}) - \frac{\gamma}{E_{max}}| < \epsilon$ where $\epsilon > 0$ is a small positive value serving as stopping threshold. The resulting μ^{opt}, $\beta(\mu^{opt})$, and $\mathbf{s}^{opt} = \mathbf{q}_L(\mu^{opt})$, values uniquely satisfy the necessary conditions (18)-(20), and give the globally optimal solution. While the optimization problem can also be solved by semidefinite relaxation (SDR) [33], our proposed generalized eigen-decomposition based algorithm is direct in nature, easy to implement (straight in the complex domain), and faster.

3.2. Unknown Eavesdropper Channel

In many applications it is impractical to assume that Alice/Bob may have (continuously updated) information about Eve's channel and disturbance autocorrelation matrix $\mathbf{R}_e$. Therefore, the waveform design solution of the previous section cannot be adopted due to lack of access to Eve's SINR.

By common intuition, low-power Alice-to-Bob transmission ("whispering") improves security by making signal interception by Eve more difficult. Alice, then, needs to use a waveform $\mathbf{s}$ that minimizes the transmitting energy while Bob maintains a given required QoS level

$$(E, \mathbf{s})^{opt} = \arg \min_{E>0,\, \mathbf{s}\in\mathbb{C}^L} E \tag{21}$$

$$\text{s. t. } E\mathbf{s}^H \mathbf{Q}_b \mathbf{s} \geq \gamma\,, \tag{22}$$

$$\mathbf{s}^H \mathbf{s} = 1\,, \tag{23}$$

$$E \leq E_{max}\,. \tag{24}$$

The optimal design to minimize the transmit energy is given by the following proposition.

Proposition 3: Let $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_L$ be the eigenvectors of $\mathbf{Q}_b$ with corresponding eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_L$. The waveform $\mathbf{s}$ to minimize transmitting energy is

$$\mathbf{s} = \mathbf{q}_1$$

and the minimum transmitting energy is

$$E_{min} = \gamma/\lambda_1. \qquad ■$$

If $E_{min} < E_{max}$, Alice-to-Bob transmission can be established with waveform $\mathbf{s} = \mathbf{q}_1$ and transmitting energy $E_{min} = \gamma/\lambda_1$.

To further increase security by degrading Eve's SINR, we adopt an artificial-noise (AN)-aided approach. The maximum (by the waveform design $\mathbf{s} = \mathbf{q}_1$) remaining transmit energy

budget $E_{AN} = E_{max} - E_{min}$ will be utilized to insert artificially generated noise to interfere to signal reception by Eve only. Specifically, Alice shall transmit during the nth symbol period her data signal $\sqrt{E}b(n)\mathbf{s}$ along with artificially generated noise $\mathbf{w}(n)$ of mean $\mathbb{E}\{\mathbf{w}\} = \mathbf{0}$, autocorrelation matrix $\mathbf{R}_w \triangleq \mathbb{E}\{\mathbf{w}\mathbf{w}^H\}$, and energy $E_{AN} = \mathrm{Tr}\{\mathbf{R}_w\}$. Bob's received signal vector can be expressed as

$$\mathbf{y}_b(n) = \sqrt{E}b(n)\mathbf{H}_b\mathbf{s} + \mathbf{H}_b\mathbf{w}(n) + \mathbf{z}_b + \mathbf{n}_b, \quad n = 1, 2, \ldots .$$

With maximum SINR filtering by $\mathbf{w}_{maxSINR,b} = c(\mathbf{R}_b + \mathbf{H}_b\mathbf{R}_w\mathbf{H}_b^H)^{-1}\mathbf{H}_b\mathbf{s}$, $c > 0$, $\mathbf{R}_b \triangleq \mathbb{E}\{(\mathbf{z}_b + \mathbf{n}_b)(\mathbf{z}_b + \mathbf{n}_b)^H\}$, the output SINR is maximized to

$$\mathrm{SINR}_b = E\mathbf{s}^H\mathbf{H}_b^H(\mathbf{R}_b + \mathbf{H}_b\mathbf{R}_w\mathbf{H}_b^H)^{-1}\mathbf{H}_b\mathbf{s}. \qquad (25)$$

By Woodbury's matrix inversion lemma,

$$(\mathbf{R}_b + \mathbf{H}_b\mathbf{R}_w\mathbf{H}_b^H)^{-1} = \mathbf{R}_b^{-1} - \mathbf{R}_b^{-1}\mathbf{H}_b\mathbf{R}_w(\mathbf{I} + \mathbf{H}_b^H\mathbf{R}_b^{-1}\mathbf{H}_b\mathbf{R}_w)^{-1}\mathbf{H}_b^H\mathbf{R}_b^{-1}$$

and (25) can be rewritten as

$$\mathrm{SINR}_b = E\mathbf{s}^H\mathbf{H}_b^H\mathbf{R}_b^{-1}\mathbf{H}_b\mathbf{s} - E\mathbf{s}^H\mathbf{H}_b^H\mathbf{R}_b^{-1}\mathbf{H}_b\mathbf{R}_w(\mathbf{I} + \mathbf{H}_b^H\mathbf{R}_b^{-1}\mathbf{H}_b\mathbf{R}_w)^{-1}\mathbf{H}_b^H\mathbf{R}_b^{-1}\mathbf{H}_b\mathbf{s} \qquad (26)$$

where the first term is Bob's SINR without AN (see (7)) and the second term quantifies Bob's SINR degradation due to AN. To make the second term (degradation) in (26) zero, it suffices to design AN with autocorrelation matrix $\mathbf{R}_w$ such that

$$\mathbf{s}^H\mathbf{H}_b^H\mathbf{R}_b^{-1}\mathbf{H}_b\mathbf{R}_w = \mathbf{s}^H\mathbf{Q}_b\mathbf{R}_w = \mathbf{0}^T \qquad (27)$$

where $\mathbf{0}$ is the $L \times 1$ all zero vector.

It is easy to see that, to achieve equality in (27) with waveform design $\mathbf{s} = \mathbf{q}_1$, we should have $\mathbf{R}_w = \mathbf{W}\mathbf{\Sigma}\mathbf{W}^H$ where $\mathbf{W} \triangleq [\mathbf{q}_2, \ldots, \mathbf{q}_L]$, $L \geq 2$, $\mathbf{\Sigma} \in \mathbb{R}^{(L-1)\times(L-1)}$ is a diagonal matrix, and $E_{AN} = \mathrm{Tr}\{\mathbf{\Sigma}\}$. This means that AN $\mathbf{w}(n)$ must be chosen as a linear combination of the $L-1$ eigenvectors $\mathbf{q}_2, \ldots, \mathbf{q}_L$. With unknown eavesdropper's CSI, the best option available to Alice is to isotropically/uniformly spread the available transmit energy budget $E_{AN} = E_{max} - E_{min}$ along the $L-1$ eigen dimensions orthogonal to $\mathbf{s} = \mathbf{q}_1$ to interfere with the eavesdroppers' receiver. Therefore, AN is generated with the following autocorrelation matrix

$$\mathbf{R}_w = \frac{E_{max} - E_{min}}{L-1}\mathbf{W}\mathbf{W}^H.$$

4. SIMULATION EXPERIMENTS AND DISCUSSION

In this section, we present simulation results to validate the impact of the proposed waveform design to SISO secrecy. We let Alice attempt to establish a secure transmission to Bob using a waveform of length $L = 8$ in the presence of eavesdropper Eve. The channel is assumed to be multipath Rayleigh fading with $M = 3$ resolvable paths with additive interference from concurrent users and white Gaussian noise. The available transmit energy is assumed to be $E_{max} = 100$. Three schemes are examined under varying assumptions about Eve's CSI: *i*) Generalized eigenwaveform of Section 3.1 (known CSI); *ii*) artificial noise (AN) injection of Section 3.2 (no CSI); and *iii*) as a reference line, the obvious engineering approach of minimum-required-energy transmission. The average pre-detection SINR of Eve over 10^6 channel realizations is plotted in Fig. 1 as a function of Bob's pre-detection SINR requirement γ, which is set to range from 0dB to 10dB. It can be observed from Fig. 1 that, for the case of known CSI, the generalized eigenwaveform design keeps the SINR of Eve at lowest values and provides effectively secure transmission to Bob. For unknown CSI, the AN-aided method degrades Eve's SINR by about 2dB over the minimum-required-energy approach and maintains a significant Bob-to-Eve SINR margin of 6dB to 8dB.

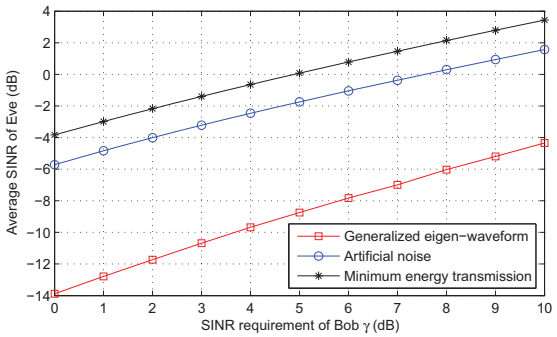

Fig. 1. Average SINR of Eve versus SINR requirement of Bob γ ($E_{max} = 100$, $L = 8$).

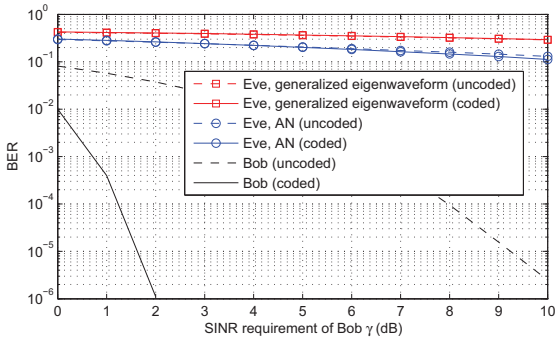

Fig. 2. BER versus SINR requirement of Bob γ ($E_{max} = 100$, $L = 8$).

To quantify the practical effectiveness of the proposed transmission scheme with secure waveform design, we "translate" Fig. 1 to bit-error-rate (BER) of Bob and Eve for both uncoded and coded transmissions. An $(1024, 512)$ low-density parity-check (LDPC) code with belief-propagation decoding is adopted for the simulation experiments. Bob and Eve know exactly the coding scheme. The BER performance curves are shown in Fig. 2. While Bob can achieve (by all practical measures) errorless transmission with LDPC coding at 2 dB SINR, Eve has error rate barely less than $1/2$ even when Alice has no knowledge of Eve's CSI (Eve, AN coded curve). The wireless link is, arguably, as secure as ever intended.

5. REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355-1387, Oct. 1975.

[2] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Intern. Symp. Inform. Th.*, Seattle, WA, July 2006, pp. 356-360.

[3] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2470-2492, June 2008.

[4] Z. Li, R. D. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. Allerton Conf. on Commun., Control, and Comp.*, Allerton Park, IL, Sept. 2006.

[5] Z. Li, R. D. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Proc. IEEE Intern. Symp. Inform. Th.*, Nice, France, June 2007, pp. 1296-1300.

[6] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, vol. 54, pp. 4687-4698, Oct. 2008.

[7] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, pp. 339-348, May 1978.

[8] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2453-2469, June 2008.

[9] E. Tekin and A. Yener, "Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy," in *Proc. Allerton Conf. on Commun., Control, and Comp.*, Allerton Park, IL, Sept. 2006.

[10] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 54, pp. 976-1002, Mar. 2008.

[11] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Intern. Symp. Inform. Th.*, June 2007, Nice, France, pp. 2471-2475.

[12] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Intern. Symp. Inform. Th.*, July 2008, Toronto, Canada, pp. 524-528.

[13] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," in *Proc. IEEE Intern. Symp. Inform. Th.*, June 2009, Seoul, Korea, pp. 2602-2606.

[14] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inform. Theory*, vol. 55, pp. 2547-2553, June 2009.

[15] S. Shafiee and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inform. Theory*, vol. 55, pp. 4033-4039, Sept. 2009.

[16] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Intern. Symp. Inform. Th.*, Adelaide, Australia, Sept. 2005, pp. 2152-2155.

[17] Z. Li, W. Trappe, and R. D. Yates, "Secret communication via multi-antenna transmission," in *Proc. Conf. Inform. Sc. and Sys.*, Mar. 2007, Baltimore, MD, pp. 905-910.

[18] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Intern. Symp. Inform. Th.*, Nice, France, June 2007, pp. 2466-2470.

[19] J. Li, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 1176-1187, Apr. 2011.

[20] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, pp. 3088-3104, July 2010.

[21] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, pp. 5515-5532, Nov. 2010.

[22] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180-2189, June 2008.

[23] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. of IEEE Intern. Conf. Acoustics, Speech, and Signal Proc.*, Taipei, Taiwan, Apr. 2009, pp. 2437-2440.

[24] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for secrecy in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Proc.*, vol. 59, pp. 351-361, Jan. 2011.

[25] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Proc.*, vol. 59, pp. 1202-1216, Mar. 2011.

[26] L. Zhang, Y.-C. Liang, Y. Pei, and R. Zhang, "Robust beamforming design: From cognitive radio MISO channels to secrecy MISO channels," in *Proc. IEEE GLOBECOM*, Miami, FL, Nov. 2009, pp. 1-5.

[27] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Trans. Commun.*, vol. 58, pp. 1877-1886, June 2010.

[28] K. Gao, S. N. Batalama, D. A. Pados, and J. D. Matyjas, "Cognitive CDMA channelization," in *Proc. Asilomar Conf. Signals, Syst., and Comp.*, Pacific Grove, CA, Nov. 2009, pp. 672-676.

[29] K. Gao, S. N. Batalama, D. A. Pados, and J. D. Matyjas, "Cognitive code-division channelization," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 1090-1097, Apr. 2011.

[30] M. Li, S. N. Batalama, D. A. Pados, T. Melodia, M. J. Medley, and J. D. Matyjas, "Cognitive code-division channelization with blind primary-system identification," in *Proc. IEEE MILCOM*, San Jose, CA., Oct. 2010, pp. 1460-1465.

[31] M. Li, S. N. Batalama, D. A. Pados, T. Melodia, M. J. Medley, and J. D. Matyjas, "Cognitive code-division links with blind primary-system identification," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 3743-3753, Nov. 2011.

[32] A. Beck and Y. C. Eldar, "Strong duality in nonconvex quadratic optimization with two quadratic constraints," *SIAM Journal on Optimization*, vol. 17, pp. 844-860.

[33] Y. Huang and D. P. Palomar, "Rank-constrained separable semidefinite programming with applications to optimal beamforming," *IEEE Trans. Signal Proc.*, vol. 58, pp. 664-678, Feb. 2010.