Waveform Design for Secure SISO Transmissions and Multicasting

Ming Li, *Member, IEEE,* Sandipan Kundu, Dimitris A. Pados, *Member, IEEE,* and Stella N. Batalama, *Senior Member, IEEE*

Abstract—Wireless physical-layer security is an emerging field of research aiming at preventing eavesdropping in an open wireless medium. In this paper, we propose a novel waveform design approach to minimize the likelihood that a message transmitted between trusted single-antenna nodes is intercepted by an eavesdropper. In particular, with knowledge first of the eavesdropper's channel state information (CSI), we find the optimum 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. The extensions of the secure waveform design problem to multiple intended receivers are also investigated and semidefinite relaxation (SDR) -an approximation technique based on convex optimization- is utilized to solve the arising NP-hard design problems. Extensive simulation studies confirm our analytical performance predictions and illustrate the benefits of the designed waveforms on securing single-input single-output (SISO) transmissions and multicasting.

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

I. INTRODUCTION

THE BROADCAST nature of the wireless medium makes wireless networks ubiquitously accessible and inherently non-secure. An eavesdropper within range of a wireless transmission may intercept the transmitted signal while staying undetected. Commonly used 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 the 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 recently in the development of physical layer security mechanisms for the wireless link.

M. Li, S. Kundu, D. A. Pados, and S. N. Batalama are with the Department of Electrical Engineering, State University of New York at Buffalo, Buffalo, NY, 14260, USA (e-mail: {mingli,skundu,pados,batalama}@buffalo.edu).

A classical physical-layer secrecy setting was introduced in Wyner's seminal work [1] in the form of two single-input single-output (SISO) channels, transmitter-to-intended-receiver and transmitter-to-eavesdropper. The Wyner Gaussian wiretap channel was a first example of an information-theoretic security framework that demonstrated the possibility of secure communications at the physical layer. If the eavesdropper's channel is a degraded version of the channel of the intended receiver, perfectly secure communication between the transmitter and the intended receiver is possible with non-zero rate. Later on, the studies on secrecy capacity were extended to the cases of secure communications over SISO fading channels [2]-[7], Gaussian broadcast channels [8],[9], and Gaussian multiple access channels [10],[11]. Motivated by emerging wireless communication applications with multiple antennas, there has been recently a flurry of interesting studies of information-theoretic secrecy capacity for multiple-input multiple-output MIMO channels [12]-[16], single-input multiple-output (SIMO) channels [17], and multiple-input single-output (MISO) channels [18]-[20]. Practical applications of low-density parity-check (LDPC) codes to the wiretap channel problem were considered in [21]-[23].

While many works focus on information-theoretic aspects and calculation/analysis of the achievable secrecy capacity, there is growing interest 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. Secret transmit (and receive) beamforming designs [24]-[29] which utilize the spatial degrees of freedom can enhance the physical layer secrecy of wireless communications by crippling eavesdroppers' interception efforts as much as possible, while simultaneously guaranteeing a certain Quality-of-Service (QoS)/signal-to-interference-plus-noise-ratio (SINR) at the intended receiver. In particular, [24]-[25] focused on exploiting knowledge of the eavesdropper's MISO/MIMO instantaneous channel state information (CSI) to provide secure communications. Since eavesdropper's CSI is unlikely to be available in many scenarios, the use of artificially injected noise (AN) was considered [26]-[28]. AN-aided methods aim to generate a disturbance signal that degrades the eavesdropper's channel but does not affect the channel of the intended receiver, thus enabling secure communication. AN-aided methods can certainly be adopted for the case where the eavesdropper's instantaneous CSI is known as well. In [29], the transmit beamformer and AN spatial distribution were jointly optimized according to the CSI of the intended receiver

and the eavesdroppers, using a semidefinite relaxation (SDR) algorithmic approach.

In this present work, we consider the core problem of secure transmissions over a multipath SISO channel where both transmitter and intended receiver have only one antenna. Other than beamforming, which uses the spatial degrees of freedom 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 multipath fading channel. To the best of our knowledge, waveform design for secure transmissions over multipath SISO channels has not been investigated in the literature before. Like other signal-processing-based approaches [24]-[29], we will use again SINR as the optimization metric to pursue physical-layer security. In particular, with knowledge of eavesdropper's CSI, our objective is to find the optimum waveform and transmit energy that minimize the SINR at the output of the eavesdropper's maximum-SINR linear filter, while at the same time provide the intended receiver with a pre-specified SINR at the output of its own maximum SINR filter[1]. It is also interesting to point out that the design formulation described above is similar to cognitive radio (CR) application problems where protecting primary users from being interfered by secondary users [30]-[35] parallels the problem of preventing eavesdroppers from overhearing.

In the second part of this work, we study the case where no information regarding the eavesdropper's CSI is available and AN-aided methods are adopted in the waveform design problem. The studies are then extended to the scenario that the transmitter is to broadcast secure data to multiple intended receivers. We recognize that, regretfully, the waveform design problem for secure multicasting is non-convex NP-hard, in general. Yet, using SDR techniques we are able to develop a realizable suboptimal solution with excellent secure multicast system performance as demonstrated by simulation studies included in this paper.

The rest of the paper is organized as follows. The secure SISO transmission problem is formulated in Section II. Secure waveform designs are developed in Section III for one intended receiver. We then extend the studies to the case of multiple intended receivers in Section IV. In Section V, simulation results illustrate our developments and, finally, a few conclusions are drawn in Section VI.

The following notation is used throughout the paper. Boldface lower-case letters indicate column vectors and boldface upper-case letters indicate matrices; $\mathbb{C}$ is the set of all complex numbers; $()^T$ and $()^H$ denote the transpose and transpose-conjugate operation, respectively; $\mathbf{I}_L$ is the $L \times L$ identity matrix; $\mathfrak{Re}\{\cdot\}$ denotes the real part of a complex number; $\mathrm{sgn}\{\cdot\}$ denotes zero-threshold quantization; and $\mathbb{E}\{\cdot\}$ represents statistical expectation. $\mathbf{X} \succ \mathbf{0}$ and $\mathbf{X} \succeq \mathbf{0}$ state that $\mathbf{X}$ is positive definite and positive semidefinite, respectively; $\mathrm{Tr}\{\mathbf{X}\}$ is the trace of $\mathbf{X}$. Finally, $|\cdot|$ and $\|\cdot\|$ are the magnitude and norm of a scalar and vector, respectively.

[1]To the extend that the bit-error-rate (BER) of the eavesdropper's receiver is monotonically decreasing in SINR, minimization of SINR corresponds to maximization of the BER of the eavesdropper toward the 1/2 value.
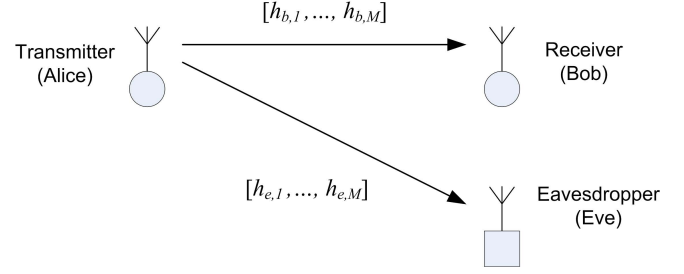

Fig. 1. SISO transmission system of a transmitter (Alice), an intended receiver (Bob), and an eavesdropper (Eve). All received signals exhibit multipath Rayleigh fading.

II. SYSTEM MODEL

We consider a wireless transmission to an intended receiver in the presence of an eavesdropper who is able to overhear the transmitted signal. For convenience, we follow the common -whimsical- language in the field and name the transmitter, intended receiver, and eavesdropper, Alice, Bob, and Eve, respectively. A simple diagram is shown in Fig. 1 to illustrate this basic communication scenario.

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 transmitted 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

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

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 inter-ference -potentially- from other concurrent users. The com-bined received signal to Bob (subscript b) or Eve (subscript e) over individual multipath fading channels of impulse response $h_{b/e}(t)$ is

$$y_{b/e}(t) = h_{b/e}(t) * u(t) + z_{b/e}(t) + n_{b/e}(t) \qquad (3)$$

where $z_{b/e}(t)$ is other user(s) interference and $n_{b/e}(t)$ is white Gaussian noise. 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, the data vector $\mathbf{y}_b(n) \in \mathbb{C}^{L_M}$ received by Bob takes the following general form

$$\mathbf{y}_b(n) = \sqrt{E}b(n)\mathbf{H}_b\mathbf{s} + \mathbf{i}_b + \mathbf{z}_b + \mathbf{n}_b, \quad n = 1, 2, \ldots, \qquad (4)$$

where $\mathbf{H}_b \in \mathbb{C}^{L_M \times L}$ is the multipath channel matrix between Alice and Bob

$$\mathbf{H}_b \triangleq \begin{bmatrix} h_{b,1} & 0 & \ldots & 0 & 0 \\ h_{b,2} & h_{b,1} & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ h_{b,M} & h_{b,M-1} & & 0 & 0 \\ 0 & h_{b,M} & & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & h_{b,M} & h_{b,M-1} \\ 0 & 0 & \ldots & 0 & h_{b,M} \end{bmatrix} \quad (5)$$

with entries $h_{b,m} \in \mathbb{C}$, $m = 1, \ldots, M$, considered as complex Gaussian random variables to model fading phenomena, $\mathbf{i}_b \in \mathbb{C}^{L_M}$ denotes multipath induced inter-symbol-interference (ISI), $\mathbf{z}_b \in \mathbb{C}^{L_M}$ represents comprehensively interference to Bob from other potential concurrent transmitters, and $\mathbf{n}_b$ is a zero-mean additive white Gaussian noise (AWGN) vector with autocorrelation matrix $\sigma_b^2 \mathbf{I}_{L_M}$. The information bits $b(n)$ are handled as binary equiprobable random variables that are independent within the data stream (i.e., in $n = 1, 2, \ldots$). 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's received signal in (4) is simplified/approximated by

$$\mathbf{y}_b(n) = \sqrt{E} b(n) \mathbf{H}_b \mathbf{s} + \mathbf{z}_b + \mathbf{n}_b, \quad n = 1, 2, \ldots. \quad (6)$$

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

$$\widehat{b}_b(n) = \text{sgn}\left\{\Re\mathfrak{e}\{\mathbf{w}_{maxSINR,b}^H \mathbf{y}_b(n)\}\right\}, \quad n = 1, 2, \ldots, \quad (7)$$

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. Practically, $\mathbf{R}_b$ can be estimated by averaging signal-absent observations over $N \geq L_M$ samples $\mathbf{y}_b(n)$ in the absence of the signal of interest, $\widehat{\mathbf{R}}_b := \frac{1}{N}\sum_{n=1}^{N}[\mathbf{z}_b(n) + \mathbf{n}_b][\mathbf{z}_b(n) + \mathbf{n}_b]^H$. If interference $\mathbf{z}_b$ from other concurrent users is not present, $\mathbf{R}_b = \sigma_b^2 \mathbf{I}_{L_M}$ and the maximum SINR filter becomes a simple matched-filter $\mathbf{w}_{maxSINR,b} \equiv \mathbf{w}_{MF,b} = \mathbf{H}_b \mathbf{s}$. The output SINR of $\mathbf{w}_{maxSINR,b}$ can be calculated to be

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

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

Due to the broadcast nature of the wireless medium, Eve can also hear the signal transmitted by Alice. Without loss of generality and for simplicity in notation, we account the multipath channels Alice-to-Bob and Alice-to-Eve to have the

same number of resolvable paths (M, that is). Then, the signal vector received by Eve can be expressed as

$$\mathbf{y}_e(n) = \sqrt{E} b(n) \mathbf{H}_e \mathbf{s} + \mathbf{z}_e + \mathbf{n}_e, \quad n = 1, 2, \ldots, \quad (9)$$

where $\mathbf{H}_e \in \mathbb{C}^{L_M \times L}$ is the Alice-to-Eve channel matrix with multipath channel coefficients $h_{e,m} \in \mathbb{C}$, $m = 1, \ldots, M$, $\mathbf{z}_e$ is other-signals interference to Eve, and $\mathbf{n}_e$ is AWGN.

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. Knowledge by Eve of the waveform $\mathbf{s}$ and the Alice-to-Eve channel coefficients $[h_{e,1}, \ldots, h_{e,M}]$ allows Eve to carry out maximum SINR filtering eavesdropping[3]. With this information, Eve attempts to extract/retrieve message bits via her own linear maximum SINR filter $\mathbf{w}_{maxSINR,e}$,

$$\widehat{b}_e(n) = \text{sgn}\left\{\Re\mathfrak{e}\{\mathbf{w}_{maxSINR,e}^H \mathbf{y}_e(n)\}\right\}, \quad n = 1, 2, \ldots, \quad (10)$$

where $\mathbf{w}_{maxSINR,e} = c \mathbf{R}_e^{-1} \mathbf{H}_e \mathbf{s} \in \mathbb{C}^{L_M}$, $c > 0$, and $\mathbf{R}_e \triangleq \mathbb{E}\{\mathbf{z}_e\mathbf{z}_e^H\} + \sigma_e^2 \mathbf{I}_{L_M} \succ 0$ is the autocorrelation matrix of the total additive disturbance to Eve (which can also be sample-average estimated). The output SINR of the filter $\mathbf{w}_{maxSINR,e}$ is given by

$$\begin{aligned} \text{SINR}_e &\triangleq \frac{\mathbb{E}\{|\mathbf{w}_{maxSINR,e}^H(\sqrt{E}b\mathbf{H}_e\mathbf{s})|^2\}}{\mathbb{E}\left\{|\mathbf{w}_{maxSINR,e}^H(\mathbf{z}_e + \mathbf{n}_e))|^2\right\}} \\ &= E\mathbf{s}^H \mathbf{H}_e^H \mathbf{R}_e^{-1} \mathbf{H}_e \mathbf{s} = E\mathbf{s}^H \mathbf{Q}_e \mathbf{s} \quad (11) \end{aligned}$$

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 minimum required SINR level that corresponds to an acceptable BER, while Eve can only have far, far inferior SINR reception performance with, consequently, BER near 1/2. In the next section, we attempt to lay the foundation for such a development utilizing Alice's transmit waveform vector $\mathbf{s}$ as a security design parameter[4].

III. SECURE WAVEFORM DESIGN

A. Known Eavesdropper Channel

We first consider the scenario under which Alice/Bob know Eve's channel $\mathbf{H}_e$ and disturbance autocorrelation matrix $\mathbf{R}_e$. This may be possible, for example, if the location of Eve is known or projected/anticipated.

---

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

[3]Knowledge by Eve of Bob's channel $[h_{b,1}, \ldots, h_{b,M}]$ would be of no value to passive eavesdropping, which is the only security breach considered in this present work.

[4]Our pre-detection SINR-based development approach is independent of symbol alphabet sets and employed detectors. For simplicity and clarity in presentation, we consider herein binary symbols $b(n) \in \{\pm 1\}$ (eq. (1)) and corresponding (optimal for Gaussian disturbance) zero-threshold detection (eqs. (7), (10)).

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 $\gamma > 0$. I.e., we would like to identify the optimal pair

$$(E, \mathbf{s})^{opt} = \arg \min_{E > 0, \, \mathbf{s} \in \mathbb{C}^L} E \mathbf{s}^H \mathbf{Q}_e \mathbf{s} \qquad (12)$$

$$\text{s. t.} \quad E \mathbf{s}^H \mathbf{Q}_b \mathbf{s} \geq \gamma, \qquad (13)$$

$$\mathbf{s}^H \mathbf{s} = 1, \qquad (14)$$

$$E \leq E_{max}, \qquad (15)$$

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

The constrained optimization problem (12)-(15) is non-convex. It is easy to verify that (13) always holds with equality at an optimal point. Therefore, for any given $\mathbf{s}$, the optimal transmitting energy can be calculated at

$$E = \frac{\gamma}{\mathbf{s}^H \mathbf{Q}_b \mathbf{s}}. \qquad (16)$$

By applying (16) to (12)-(15), the objective function can be reformulated as having only $\mathbf{s}$ to be optimized,

$$\mathbf{s}^{opt} = \arg \min_{\mathbf{s} \in \mathbb{C}^L} \frac{\mathbf{s}^H \mathbf{Q}_e \mathbf{s}}{\mathbf{s}^H \mathbf{Q}_b \mathbf{s}} \qquad (17)$$

$$\text{s. t.} \quad \mathbf{s}^H \mathbf{Q}_b \mathbf{s} \geq \frac{\gamma}{E_{max}}, \qquad (18)$$

$$\mathbf{s}^H \mathbf{s} = 1. \qquad (19)$$

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 (18). It is clear that constraint (18) 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 (18) for a moment, then the waveform to minimize the SINR ratio is the familiar generalized eigenvector solution [36] given by the following proposition.

Proposition 1: Let $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_L$ be the 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 (17) is the generalized eigenvector

$$\mathbf{s} = \mathbf{p}_L \qquad (20)$$

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

The eigen-design waveform in (20) is obtained with computational complexity $\mathcal{O}((L+M-1)^3)$. It 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 (18), which is a common case. If, however, (18) is not satisfied, we have to return to problem (12)-(15) and examine its Karush-Kuhn-Tucker (KKT) conditions[5]. The findings are summarized in the following proposition whose proof is provided in the Appendix.

Proposition 2: Consider the solvable (maximum eigenvalue of $\mathbf{Q}_b$ no less than γ/E_{max}) optimization problem (17)-(19) and assume that solution (20) does not satisfy constraint (18).

[5]The strong Lagrangian duality of (12)-(15) was proven in [37].

Then, the following KKT conditions are necessary for an $\mathbf{s}$ to be optimal

$$(\mathbf{Q}_e + \mu \mathbf{I})\mathbf{s} = \beta \mathbf{Q}_b \mathbf{s}, \; \beta > 0, \; \mu > 0, \qquad (21)$$

$$\mathbf{s}^H \mathbf{Q}_b \mathbf{s} = \frac{\gamma}{E_{max}}, \qquad (22)$$

$$\mathbf{s}^H \mathbf{s} = 1. \qquad (23)$$

∎

While, unfortunately, we cannot have closed-form expressions for $\mathbf{s}$ from the above KKT conditions, we can pursue an efficient numerical solution by bisection. We reformulate (21) as

$$((1 - \tilde{\mu})\mathbf{Q}_e + \tilde{\mu}\mathbf{I})\mathbf{s} = \beta(1 - \tilde{\mu})\mathbf{Q}_b \mathbf{s}, \; \beta > 0, \qquad (24)$$

where $\tilde{\mu} \triangleq \frac{\mu}{1+\mu}$, $\tilde{\mu} \in [0, 1)$. Condition (24) indicates that the optimal $\mathbf{s}$ is a generalized eigenvector of the matrices $((1 - \tilde{\mu})\mathbf{Q}_e + \tilde{\mu}\mathbf{I}, (1 - \tilde{\mu})\mathbf{Q}_b)$. For any given value of $\tilde{\mu} \in [0, 1)$, let $\mathbf{q}_L(\tilde{\mu})$ denote the generalized eigenvector of $((1 - \tilde{\mu})\mathbf{Q}_e + \tilde{\mu}\mathbf{I}, (1 - \tilde{\mu})\mathbf{Q}_b)$ that has minimum eigenvalue $\beta(\tilde{\mu})$. We can easily verify that $\mathbf{q}_L^H(\tilde{\mu})\mathbf{Q}_b \mathbf{q}_L(\tilde{\mu})$ is strictly monotonically increasing in $\tilde{\mu} \in [0, 1)$. Based on the monotonicity and bounds on $\tilde{\mu}$, we solve the KKT necessary conditions (22)-(24) with bisection on $\tilde{\mu}$ to a value $\tilde{\mu}^{opt}$ such that $|\mathbf{q}_L^H(\tilde{\mu}^{opt})\mathbf{Q}_b \mathbf{q}_L(\tilde{\mu}^{opt}) - \frac{\gamma}{E_{max}}| < \epsilon$ where $\epsilon > 0$ is a small positive value serving as stopping threshold. The resulting $\tilde{\mu}^{opt}$, $\beta(\tilde{\mu}^{opt})$, and $\mathbf{s}^{opt} = \mathbf{q}_L(\tilde{\mu}^{opt})$ values uniquely satisfy the necessary conditions (22)-(24) and give the globally optimal solution. While the optimization problem can also be solved by semidefinite relaxation (SDR) [43], our proposed generalized eigen-decomposition based algorithm is direct in nature, easy to implement (straight in the complex domain), and faster.

B. 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 $\mathbf{R}_e$. In this case, 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 since Eve's SINR is proportional to the transmitting energy. Alice, then, needs to use a waveform $\mathbf{s}$ that minimizes the transmitting energy while Bob maintains a given required QoS level

$$(E, \mathbf{s})^{opt} = \arg \min_{E > 0, \, \mathbf{s} \in \mathbb{C}^L} E \qquad (25)$$

$$\text{s. t.} \quad E \mathbf{s}^H \mathbf{Q}_b \mathbf{s} \geq \gamma, \qquad (26)$$

$$\mathbf{s}^H \mathbf{s} = 1, \qquad (27)$$

$$E \leq E_{max}. \qquad (28)$$

Mathematically, the optimization problem (25)-(28) is a special case of (12)-(15) under $\mathbf{Q}_e = \alpha \mathbf{I}, \alpha > 0$. The optimal design to minimize the transmit energy is summarized by the following proposition with straightforward derivation [38, Theorem 4.2.2].

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

$$\mathbf{s} = \mathbf{q}_1 \qquad (29)$$

and the minimum transmitting energy is

$$E_{min} = \gamma/\lambda_1. \tag{30}$$

∎

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 $E_{AN} = \text{Tr}\{\mathbf{R}_w\}$. Bob's received signal vector is then expressed as (compare to (6))

$$\mathbf{y}_b(n) = \sqrt{E}b(n)\mathbf{H}_b\mathbf{s} + \mathbf{H}_b\mathbf{w}(n) + \mathbf{z}_b + \mathbf{n}_b, \quad n = 1, 2, \ldots. \tag{31}$$

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 with AN is maximized to

$$\text{SINR}_b^{AN} = E\mathbf{s}^H\mathbf{H}_b^H(\mathbf{R}_b + \mathbf{H}_b\mathbf{R}_w\mathbf{H}_b^H)^{-1}\mathbf{H}_b\mathbf{s} \tag{32}$$

where the superscript AN is added to differentiate from Bob's SINR_b in (8) when no AN is injected by Alice. The autocorrelation matrix $\mathbf{R}_w$ of AN must now be designed by Alice such that Bob's SINR degradation due to AN is zero, that is $\text{SINR}_b - \text{SINR}_b^{AN} = 0$.

By Woodbury's matrix inversion lemma [39],

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

and (32) can be rewritten as

$$\text{SINR}_b^{AN} = E\mathbf{s}^H\mathbf{H}_b^H\mathbf{R}_b^{-1}\mathbf{H}_b\mathbf{s} -$$
$$E\mathbf{s}^H\mathbf{H}_b^H\mathbf{R}_b^{-1}\mathbf{H}_b\mathbf{R}_w(\mathbf{I} + \mathbf{H}_b^H\mathbf{R}_b^{-1}\mathbf{H}_b\mathbf{R}_w)^{-1}\mathbf{H}_b^H\mathbf{R}_b^{-1}\mathbf{H}_b\mathbf{s} \tag{33}$$

where the first term is Bob's SINR without AN (see (8)) and the second term quantifies Bob's SINR degradation due to AN. To make the second term (degradation) in (33) equal to zero, it suffices to design AN with autocorrelation matrix $\mathbf{R}_w$ such that

$$\mathbf{s}^H\mathbf{H}_b^H\mathbf{R}_b^{-1}\mathbf{H}_b\mathbf{R}_w = \mathbf{s}^H\mathbf{Q}_b\mathbf{R}_w = \mathbf{0}^T \tag{34}$$

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

It is easy to see that, to achieve equality in (34) with waveform design $\mathbf{s} = \mathbf{q}_1$, we should have $\mathbf{R}_w = \mathbf{W}\mathbf{\Sigma}\mathbf{W}^H$ with $\mathbf{W} \triangleq [\mathbf{q}_2, \ldots, \mathbf{q}_L]$, $L \geq 2$, and $\mathbf{\Sigma} \in \mathbb{R}^{(L-1)\times(L-1)}$ a diagonal matrix with $\text{Tr}\{\mathbf{\Sigma}\} = E_{AN}$. 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

$$\mathbf{R}_w = \frac{E_{max} - E_{min}}{L - 1}\mathbf{W}\mathbf{W}^H. \tag{35}$$
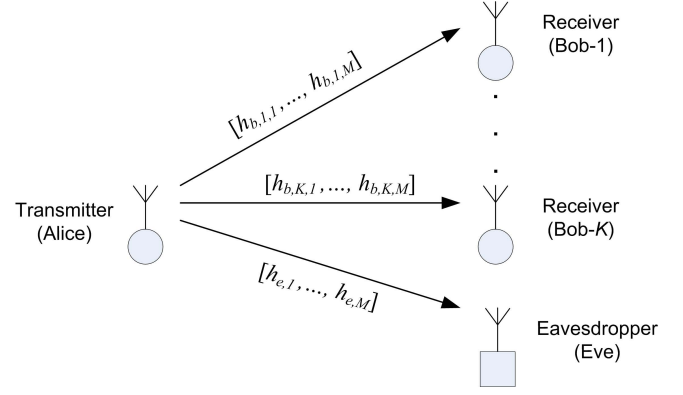

Fig. 2. Secure multicast system model of a transmitter, K intended receivers, and an eavesdropper (all received signals exhibit multipath Rayleigh fading).

The task of weakening Eve's SINR (subject to meeting Bob's QoS requirements) is now complete at a best effort basis by the AN approach when neither instantaneous nor statistical CSI of Eve is available.

IV. SECURE MULTICASTING

Multicasting is an efficient method of supporting group communication by allowing simultaneous transmission of the same information to multiple destinations. In the scenario of (secure) multicasting shown in Fig. 2, Alice intends to transmit securely the same data stream to multiple receivers (K Bobs) in the presence of an eavesdropper (Eve). With K Bobs to be served, the received signal of each Bob is denoted by

$$\mathbf{y}_{b,k}(n) = \sqrt{E}b(n)\mathbf{H}_{b,k}\mathbf{s} + \mathbf{z}_{b,k} + \mathbf{n}_{b,k},$$
$$k = 1, \ldots, K, \ n = 1, 2, \ldots,$$

where $\mathbf{H}_{b,k} \in \mathbb{C}^{L_M \times L}$ is the channel matrix from Alice to Bob-k with multipath channel coefficients $h_{b,k,m} \in \mathbb{C}$, $m = 1, \ldots, M$, and $\mathbf{z}_{b,k}$ is compound interference to Bob-k. Similar to the developments in the previous section, the output SINR of Bob-k's maximum SINR filter is

$$\text{SINR}_{b,k} = E\mathbf{s}^H\mathbf{Q}_{b,k}\mathbf{s}$$

where $\mathbf{Q}_{b,k} \triangleq \mathbf{H}_{b,k}^H\mathbf{R}_{b,k}^{-1}\mathbf{H}_{b,k}$, $\mathbf{R}_{b,k} \triangleq \mathbb{E}\{(\mathbf{z}_{b,k} + \mathbf{n}_{b,k})(\mathbf{z}_{b,k} + \mathbf{n}_{b,k})^H\}$. Eve's received signal model is the same as in (9) and the output SINR of Eve's maximum SINR filter is as in (11).

If we consider sum-SINR, which is defined as the sum of the individual SINRs of the K intended receivers, as a multicast performance metric,

$$\text{SINR}_{sum} \triangleq \sum_{k=1}^{K}\text{SINR}_{b,k} = E\mathbf{s}^H\left(\sum_{k=1}^{K}\mathbf{Q}_{b,k}\right)\mathbf{s} = E\mathbf{s}^H\widetilde{\mathbf{Q}}_b\mathbf{s},$$

$\widetilde{\mathbf{Q}}_b \triangleq \sum_{k=1}^{K}\mathbf{Q}_{b,k}$, then the presented secure waveform design problem is similar to (12)-(15) and can be solved by the algorithm developed in the previous section. Arguably, however, sum-SINR may not be an appropriate performance measure of choice, since no form of fairness/performance assurance among receivers can be guaranteed. Therefore, we turn our attention to the more difficult version of the problem that involves individual constraints by which each intended

receiver has its own SINR requirement γ_k, $k = 1, \ldots, K$. We investigate secure waveform design for the known and unknown eavesdropper channel case.

A. Known Eavesdropper Channel

Our objective is to find the transmission bit energy E and the complex-valued normalized waveform vector $\mathbf{s}$ that minimize $\text{SINR}_e = E\mathbf{s}^H\mathbf{Q}_e\mathbf{s}$ under the constraints $\text{SINR}_k = E\mathbf{s}^H\mathbf{Q}_{b,k}\mathbf{s} \geq \gamma_k$, $k = 1, \ldots, K$,

$$(E, \mathbf{s})^{opt} = \arg\min_{E>0, \mathbf{s}\in\mathbb{C}^L} E\mathbf{s}^H\mathbf{Q}_e\mathbf{s} \tag{36}$$

$$\text{s. t.} \quad E\mathbf{s}^H\mathbf{Q}_{b,k}\mathbf{s} \geq \gamma_k, \ k = 1, \ldots, K, \tag{37}$$

$$\mathbf{s}^H\mathbf{s} = 1, \tag{38}$$

$$E \leq E_{max}. \tag{39}$$

The optimization task of minimizing the quadratic objective function (36) subject to the $K > 1$ constraints in (37) and (38), (39) is, unfortunately, a non-convex NP-hard (in L) optimization problem. In the following, we delve into the details of the problem and derive a realizable suboptimum solution.

To effectively approach the problem, we first let $\mathbf{x} \triangleq \sqrt{E}\mathbf{s}$ denote the amplitude-including transmitted waveform vector. Then, the optimization problem in (36)-(39) can be rewritten as

$$\mathbf{x}' = \arg\min_{\mathbf{x}\in\mathbb{C}^L} \mathbf{x}^H\mathbf{Q}_e\mathbf{x} \tag{40}$$

$$\text{s. t.} \quad \mathbf{x}^H\mathbf{Q}_{b,k}\mathbf{x} \geq \gamma_k, \ k = 1, \ldots, K, \tag{41}$$

$$\mathbf{x}^H\mathbf{x} \leq E_{max}. \tag{42}$$

This optimization problem is in general a non-convex quadratically constrained quadratic program (non-convex QCQP) and the complexity of a solver of (40)-(42) is exponential in the dimension L (NP-hard problem). To circumvent this difficulty, we first observe that if we use the trace property of matrices, we are able to represent the objective function in (40) as

$$\mathbf{x}^H\mathbf{Q}_e\mathbf{x} = \text{Tr}\{\mathbf{Q}_e\mathbf{X}\}, \ \mathbf{X} \triangleq \mathbf{x}\mathbf{x}^H. \tag{43}$$

Thus, with $\mathbf{X} = \mathbf{x}\mathbf{x}^H$, the optimization problem in (40)-(42) takes the new equivalent matrix form

$$\mathbf{X}' = \arg\min_{\mathbf{X}\in\mathbb{C}^{L\times L}} \text{Tr}\{\mathbf{Q}_e\mathbf{X}\} \tag{44}$$

$$\text{s. t.} \quad \text{Tr}\{\mathbf{Q}_{b,k}\mathbf{X}\} \geq \gamma_k, \ k = 1, \ldots, K, \tag{45}$$

$$\text{Tr}\{\mathbf{X}\} \leq E_{max}, \tag{46}$$

$$\mathbf{X} \succeq 0, \tag{47}$$

$$\text{rank}(\mathbf{X}) = 1. \tag{48}$$

The re-formulated design problem is, of course, still NP-hard in general. To deal -or better say avoid- this issue, we relax/drop the rank constraint in (48) and solve the simplified version by semidefinite relaxation (SDR) [40]. The relaxed problem is a convex polynomial-complexity problem whose optimal solution can be efficiently obtained by available interior-point algorithms, for example the off-the-shelf solvers [41], [42]. The worst-case computational complexity is $\mathcal{O}((L + M - 1)^{4.5}\log(\epsilon))$ for a given minimization solution accuracy $\epsilon > 0$.

When $\mathbf{X}'$ returned by the solver happens to be of rank-1[6] with (eigenvalue, eigenvector) pair $(\lambda_1, \mathbf{a}_1)$, then $\mathbf{x}^{opt} = \sqrt{\lambda_1}\mathbf{a}_1$ and, consequently, $E^{opt} = \lambda_1$ and $\mathbf{s}^{opt} = \mathbf{a}_1$ for the original problem (36)-(39). If the rank of $\mathbf{X}'$ is not one, there is no direct path to extract $(E, \mathbf{s})^{opt}$ from $\mathbf{X}'$ and a Gaussian randomization procedure [40] can be employed to turn the SDR solution to an approximate solution to (36)-(39). In particular, we can draw now a sequence of samples $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N$ from $\mathcal{N}(\mathbf{0}, \mathbf{X}')$, i.e. Gaussian random variables with $\mathbf{0}$ mean and covariance matrix $\mathbf{X}'$. We first apply rescaling

$$\mathbf{x}_i' = \left(\max_{k=1,\ldots,K} \frac{\gamma_k}{\mathbf{x}_i^H\mathbf{Q}_{b,k}\mathbf{x}_i}\right)\mathbf{x}_i, \ i = 1, \ldots, N, \tag{49}$$

and then test all $\mathbf{x}_i'$ for "feasibility" on the constraints (41) and (42). Among the feasible vectors (if any), we choose the one, say $\mathbf{x}'^{(0)}$, with minimum $\mathbf{x}'^H\mathbf{Q}_e\mathbf{x}'$ objective function value. Consequently, E^{opt} and $\mathbf{s}^{opt}$ for problem (36)-(39) are set to $\widehat{E}^{opt} = |\mathbf{x}'^{(0)}|^2$ and $\widehat{\mathbf{s}}^{opt} = \mathbf{x}'^{(0)}/|\mathbf{x}'^{(0)}|$, respectively.

B. Unknown Eavesdropper Channel

For the unknown eavesdropper channel case, we pursue again the artificial-noise (AN)-aided method. To maximize the available energy to generate AN, we first aim at minimizing the transmitting energy while, still, each Bob's SINR is no less than a threshold γ_k,

$$(E, \mathbf{s})^{opt} = \arg\min_{E>0, \mathbf{s}\in\mathbb{C}^L} E \tag{50}$$

$$\text{s. t.} \quad E\mathbf{s}^H\mathbf{Q}_{b,k}\mathbf{s} \geq \gamma_k, \ k = 1, \ldots, K, \tag{51}$$

$$\mathbf{s}^H\mathbf{s} = 1, \tag{52}$$

$$E \leq E_{max}. \tag{53}$$

This NP-hard problem can also be approximately solved by SDR (with randomization) after reformulating (50)-(53) in matrix form to

$$\mathbf{X}' = \arg\min_{\mathbf{X}\in\mathbb{C}^{L\times L}} \text{Tr}\{\mathbf{X}\}$$

$$\text{s. t.} \quad \text{Tr}\{\mathbf{Q}_{b,k}\mathbf{X}\} \geq \gamma_k, \ k = 1, \ldots, K,$$

$$\text{Tr}\{\mathbf{X}\} \leq E_{max},$$

$$\mathbf{X} \succeq 0,$$

where $\mathbf{X} \triangleq \mathbf{x}\mathbf{x}^H$, $\mathbf{x} \triangleq \sqrt{E}\mathbf{s}$. After obtaining the optimal waveform $\mathbf{s}$ and the minimum energy E_{min} via the sole eigenvector of $\mathbf{X}'$ or an approximate solution via (49) as before, we turn our attention to the design of AN with the residual energy $E_{max} - E_{min}$.

We recall the results from (31)-(33) that, when Alice transmits AN $\mathbf{w}(n)$ along with the information bearing signal, the output SINR of Bob-k's maximum SINR filter is

$$\text{SINR}_{b,k}^{AN} = E\mathbf{s}^H\mathbf{H}_{b,k}^H\mathbf{R}_{b,k}^{-1}\mathbf{H}_{b,k}\mathbf{s} - E\mathbf{s}^H\mathbf{H}_{b,k}^H\mathbf{R}_{b,k}^{-1}\mathbf{H}_{b,k}\mathbf{R}_w$$

$$(\mathbf{I} + \mathbf{H}_{b,k}^H\mathbf{R}_{b,k}^{-1}\mathbf{H}_{b,k}\mathbf{R}_w)^{-1}\mathbf{H}_{b,k}^H\mathbf{R}_{b,k}^{-1}\mathbf{H}_{b,k}\mathbf{s},$$

$$k = 1, \ldots, K.$$

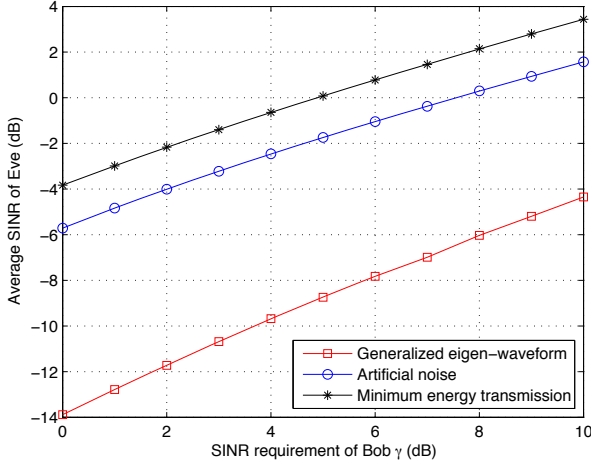[6]By Lemma 3.1 in [43], the SDR solution can always be made to have rank-one when $K \leq 2$.

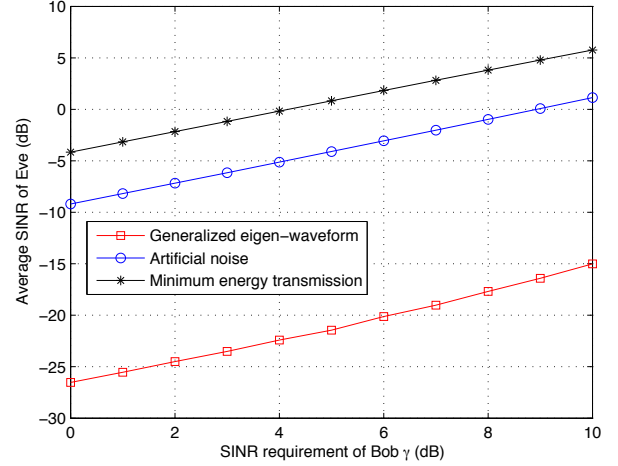Fig. 3. Average SINR of Eve versus SINR requirement of Bob γ ($E_{max} = 100$, $L = 8$).

Fig. 4. Average SINR of Eve versus SINR requirement of Bob γ ($E_{max} = 100$, $L = 16$).

To ensure that AN will not degrade the SINR of any Bob, AN should be designed with autocorrelation matrix $\mathbf{R}_w$ such that

$$\mathbf{s}^H \mathbf{H}_{b,k}^H \mathbf{R}_{b,k}^{-1} \mathbf{H}_{b,k} \mathbf{R}_w = \mathbf{0}^T, \ \forall k = 1, \ldots, K. \quad (55)$$

Set $\mathbf{v}_k \triangleq \mathbf{H}_{b,k}^H \mathbf{R}_{b,k}^{-1} \mathbf{H}_{b,k} \mathbf{s}, k = 1, \ldots, K$, and $\mathbf{V} \triangleq [\mathbf{v}_1, \ldots, \mathbf{v}_K]$. To achieve the equalities in (55), we need $L \geq K + 1$ and require that $\mathbf{R}_w \perp \mathbf{V}$. Let $\mathbf{u}_i$, $i = 1, \ldots, L$, be left singular vectors of $\mathbf{V}$ with singular values $\lambda_1 \geq \lambda_2 \geq, \ldots, \lambda_L$. Isotropical AN should be designed with autocorrelation matrix

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

where $\mathbf{W} \triangleq [\mathbf{u}_{K+1}, \ldots, \mathbf{u}_L]$.

V. SIMULATION EXPERIMENTS

In this section, we present simulation results that show the average SINR and bit-error-rate (BER) of Eve for various target performance levels of Bob, lengths of waveform L, and total energy constraints. In all simulations, the channel is assumed to be multipath fading with $M = 3$ resolvable paths with additive interference from concurrent users and white Gaussian noise. The multipath coefficients are taken to be independent complex Gaussian random variables of mean zero and variance $1/M$. In each channel realization, a number of concurrent users is randomly selected between 5 and 10; for each concurrent user, the energy per-bit is uniformly drawn from $[1, 4]$ and a normalized waveform of length L is arbitrarily generated from the zero-mean Gaussian distribution and placed on the same carrier f_c as Alice's signal. Finally, the white Gaussian noise autocorrelation matrix at both Bob and Eve is set at $\mathbf{I}_{L+2}$ (identity matrix of size $L + 2$)[7].

First, Alice attempts to establish a secure transmission to Bob using a waveform of length $L = 8$ in the presence of eavesdropper Eve. 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 III.A (known CSI); *ii*) artificial noise (AN) injection of Section III.B (no CSI); and *iii*) as a reference line, minimum required energy transmission (no CSI, no AN). The average pre-detection SINR of Eve over 10^6 channel realizations is plotted in Fig. 3 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. 3 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[8]. For unknown CSI, the AN-aided method degrades Eve's SINR by about 2dB over the no-AN approach and maintains a significant Bob-to-Eve SINR margin of 6dB to 8dB. In Fig. 4, we repeat the same study with a longer $L = 16$ waveform (twice as many degrees of freedom). Comparing Fig. 4 to Fig. 3, we notice the much larger SINR gains on security even by AN alone.

In Fig. 5, we collect some useful statistics on the experiments of Figs. 3 and 4. We first, Fig. 5(a), calculate the probability (frequency of occurrence) that the generalized eigenwaveform optimization problem in (12)-(15) is solvable, i.e. Bob's SINR constraint γ can be satisfied by a waveform design for the given E_{max} value. By Fig. 5(a), the problem is almost always solvable with $L = 16$ and less likely solvable with $L = 8$ [9]. In Fig. 5(b), we focus our attention on the unknown Eve channel case and plot the average percentage of available energy to create artificial noise. Again, $L = 16$ easily supports effective creation of AN even for large SINR requirements for Bob.

To elaborate on the relationship between security performance and waveform length, in Fig. 6 we fix Bob's SINR requirement at 6dB and plot the average SINR of Eve versus waveform length L. While for known CSI and generalized

---

[7]Bob's and Eve's channel are then originally statistically equivalent in the study.

[8]The transmission can be called perfectly secure if Eve's SINR is zero or, equivalently, when her BER is 1/2. This ideal security performance bound may not be achieved with practical system settings, for example the short waveform length in our SISO transmission. Nonetheless, the proposed design provides highly effective near-optimal security, especially when the waveform length grows to $L = 16$ (Fig. 4).

[9]When Alice is to transmit with an optimal generalized eigenwaveform and no solution exists, Alice shall not transmit to prevent eavesdropping breach.
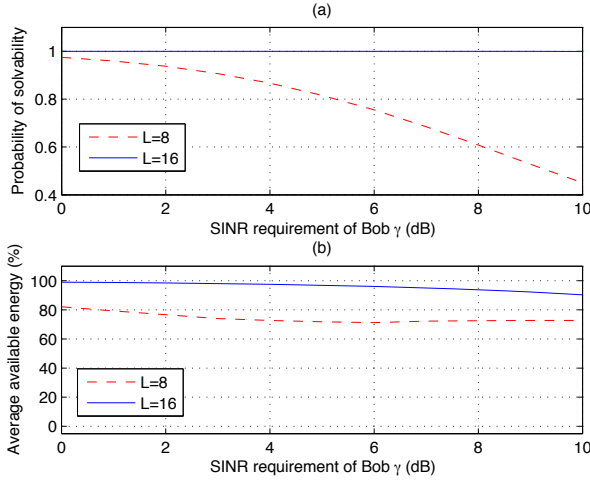
Fig. 5. (a) Probability of solvability of the generalized eigenwaveform optimization problem versus Bob's SINR constraint γ ($E_{max} = 100$); (b) average available energy (%) for artificial noise creation versus Bob's SINR constraint γ ($E_{max} = 100$).
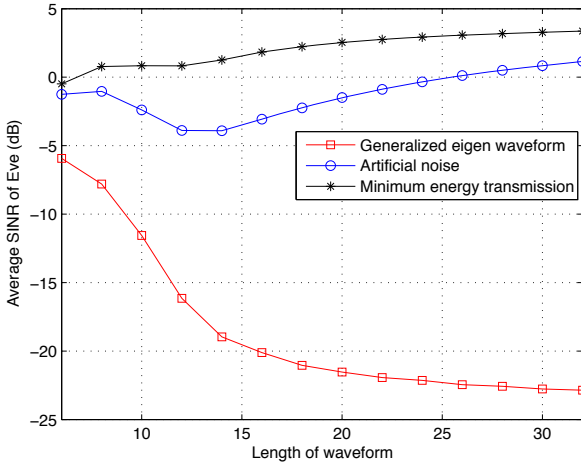

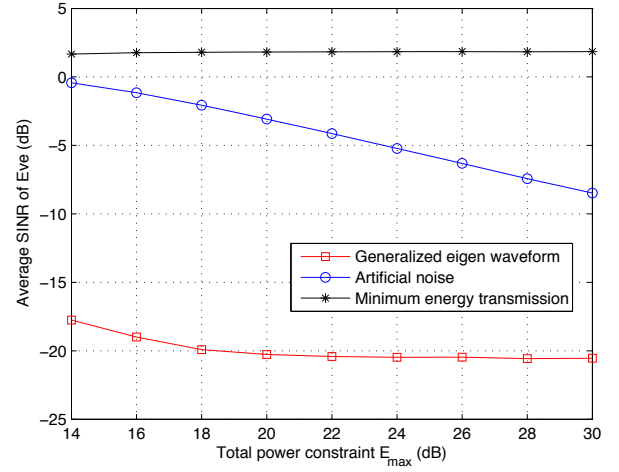Fig. 6. Average SINR of Eve versus length of waveform L ($E_{max} = 100$, $\gamma = 6$dB).

Fig. 7. Average SINR of Eve versus total transmit energy constraint E_{max} ($L = 16$, $\gamma = 6$dB).

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

eigenwaveform design the average SINR of Eve continuously decreases as L increases, this is not the case for unknown CSI and AN injection. Waveforms with longer length can reduce the transmit energy to satisfy Bob's SINR requirement and leave more residual energy to be used for generating AN. Ironically, while the energy of AN can be increased by employing a longer waveform, Eve's ability to suppress interference and noise is also enhanced[10] due to the higher space dimensions and her SINR may even increase. Therefore, waveform length for the unknown CSI case must be selected appropriately to balance the availability of AN energy to Alice and space dimensions to Eve. Average SINR of Eve versus energy constraint E_{max} is shown in Fig. 7. Obviously, for the unknown CSI case with AN, the average SINR of Eve is decreasing with higher energy constraint E_{max}, since more residual energy can be used for generating AN.

To further quantify the practical effectiveness of the proposed transmission scheme with secure waveform design, we also evaluate the bit-error-rate (BER) of Bob and Eve for both uncoded and coded transmissions. An $(1024, 512)$ low-density parity-check (LDPC) code[11] with belief-propagation decoding is adopted for the simulation experiments. Both Bob and Eve perfectly know the coding scheme. The BER performance curves ($L = 8$) are shown in Fig. 8. While Bob can achieve (by all practical measures) errorless transmission with LDPC coding at SINR 2dB, Eve has error rate barely less than $1/2$.

Now we turn to examine the performance of secure multicasting to multiple Bobs as described in Section IV. Similar to the one-Bob studies, in Figs. 9 and 10 we show the average SINR and BER, respectively, of Eve with the SDR-based waveform designs. All $K = 5$ Bobs satisfy the same SINR requirement $\gamma_1 = \ldots = \gamma_5$, which is set to vary from 0dB to

---

[10]Of course, herein, we follow the conservative approach by which Eve is supposed to have exact knowledge of Alice's waveform.

[11]Punctured (weakened) LDPC codes were used in [21], [22] to support security. SINR-based security optimization, as described in this present paper, places intrinsically Bob in the "waterfall" region of the code while keeping Eve "on the top." Therefore, puncturing is unnecessary or even detrimental to Bob's relative performance with respect to Eve.
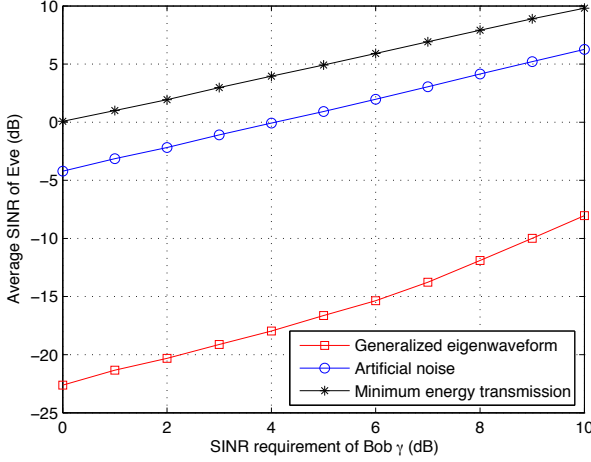
Fig. 9. Average SINR of Eve versus SINR requirement of Bobs γ ($E_{max} = 100$, $L = 16$, multicast to $K = 5$ Bobs).

Fig. 10. BER versus SINR requirement of Bobs γ ($E_{max} = 100$, $L = 16$, multicast to $K = 5$ Bobs).

10dB. It can be observed that the Bobs can achieve practically errorless reception with the $(1024, 512)$ LDPC code when their SINR is at 2dB. Eve's average BER is still too high (more than 10^{-1}).

VI. CONCLUSIONS

We presented waveform-based approaches to secure wireless transmissions between trusted (single-antenna) nodes in the presence of an eavesdropper. We formulated the problem as the search for the (transmit energy, waveform) pair that minimizes the eavesdropper's SINR subject to the condition that the intended receiver's SINR value is maintained at a given required SINR level (QoS determined). A low-complexity, highly-effective eigenwaveform and transmit energy design was proposed. We, then, extended the waveform design problem to multiple intended receivers (secure multicasting). Regretfully, the formulated multicasting optimization problem is non-convex and NP-hard in the waveform dimension. Nevertheless, we employed semi-definite relaxation to reach computationally manageable and performance-wise appealing suboptimal solutions. Extensive simulation experiments verified our analytical performance predictions and illustrated the benefits of waveform optimization for secure SISO transmission and multicasting.

As a natural next step in future work, waveform-based physical-layer security can be combined with the existing successful beamform-based security works in MIMO systems to carry out joint space-time security optimization. We can harness, then, the product of space (number of antennas) and time (waveform dimension) degrees of freedom (DoF) to secure the link.

APPENDIX - PROOF OF PROPOSITION 2

We start with the original problem (12)-(15). We combine the function to be optimized with the constraints and form the Lagrangian

$$\mathcal{L} = E\mathbf{s}^H\mathbf{Q}_e\mathbf{s} + \beta(\gamma - E\mathbf{s}^H\mathbf{Q}_b\mathbf{s}) + \mu(E - E_{max}) + \lambda(\mathbf{s}^H\mathbf{s} - 1) \tag{56}$$
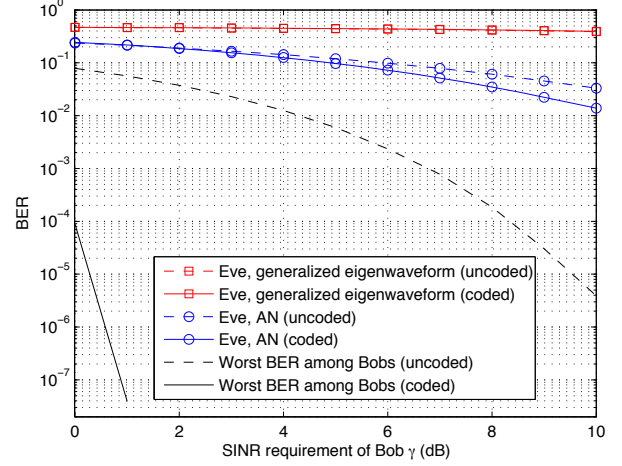
where $\beta \geq 0$, $\mu \geq 0$, and λ are KKT multipliers. The KKT necessary conditions of the optimization problem consist of

$$\frac{\partial\mathcal{L}}{\partial\mathbf{s}^H} = E\mathbf{Q}_e\mathbf{s} - \beta E\mathbf{Q}_b\mathbf{s} + \lambda\mathbf{s} = \mathbf{0}, \tag{57}$$

$$\frac{\partial\mathcal{L}}{\partial E} = \mathbf{s}^H\mathbf{Q}_e\mathbf{s} - \beta\mathbf{s}^H\mathbf{Q}_b\mathbf{s} + \mu = 0, \tag{58}$$

the complementary slackness conditions, and the primal constraints

$$\beta(\gamma - E\mathbf{s}^H\mathbf{Q}_b\mathbf{s}) = 0, \tag{59}$$

$$\mu(E - E_{max}) = 0, \tag{60}$$

$$E\mathbf{s}^H\mathbf{Q}_b\mathbf{s} \geq \gamma, \tag{61}$$

$$\mathbf{s}^H\mathbf{s} = 1, \tag{62}$$

$$E \leq E_{max}. \tag{63}$$

We first examine the above KKT conditions for the cases $\beta = 0$ and $\beta > 0$, separately. If $\beta = 0$, (58) becomes

$$\mathbf{s}^H\mathbf{Q}_e\mathbf{s} + \mu = 0 \tag{64}$$

which cannot be satisfied since $\mu \geq 0$ and $\mathbf{s}^H\mathbf{Q}_e\mathbf{s} > 0$. Therefore, we must have $\beta > 0$ and

$$E\mathbf{s}^H\mathbf{Q}_b\mathbf{s} = \gamma \Rightarrow E = \frac{\gamma}{\mathbf{s}^H\mathbf{Q}_b\mathbf{s}}. \tag{65}$$

We reach the equivalent problem (17)-(19).

After applying (65) to the original KKT necessary conditions, we obtain the KKT necessary conditions for the equivalent problem (17)-(19) as follows

$$\mathbf{Q}_e\mathbf{s} - \beta\mathbf{Q}_b\mathbf{s} + \lambda(\mathbf{s}^H\mathbf{Q}_b\mathbf{s}/\gamma)\mathbf{s} = \mathbf{0}, \tag{66}$$

$$\mathbf{s}^H\mathbf{Q}_e\mathbf{s} - \beta\mathbf{s}^H\mathbf{Q}_b\mathbf{s} + \mu = 0, \tag{67}$$

$$\mu(\gamma/\mathbf{s}^H\mathbf{Q}_b\mathbf{s} - E_{max}) = 0, \tag{68}$$

$$\mathbf{s}^H\mathbf{s} = 1, \tag{69}$$

$$\mathbf{s}^H\mathbf{Q}_b\mathbf{s} \geq \frac{\gamma}{E_{max}}. \tag{70}$$

Left multiplying both sides of (66) by $\mathbf{s}^H$, we have

$$\mathbf{s}^H\mathbf{Q}_e\mathbf{s} - \beta\mathbf{s}^H\mathbf{Q}_b\mathbf{s} + \lambda(\mathbf{s}^H\mathbf{Q}_b\mathbf{s}/\gamma) = 0. \tag{71}$$

Combining (67), (69), and (71), we have $\lambda(\mathbf{s}^H\mathbf{Q}_b\mathbf{s}/\gamma) = \mu$ and then (66) can be rewritten as

$$(\mathbf{Q}_e + \mu\mathbf{I})\mathbf{s} = \beta\mathbf{Q}_b\mathbf{s}. \tag{72}$$

For $\mu = 0$, (72) becomes

$$\mathbf{Q}_e\mathbf{s} = \beta\mathbf{Q}_b\mathbf{s} \tag{73}$$

that implies that the optimal waveform $\mathbf{s}$ is a generalized eigenvector of the matrices $(\mathbf{Q}_e, \mathbf{Q}_b)$. If the solution satisfies constraint (70), then it is the optimal solution; if not, then we turn to examine case $\mu > 0$. When $\mu > 0$, to satisfy (68), we must have $\gamma/\mathbf{s}^H\mathbf{Q}_b\mathbf{s} - E_{max} = 0$, and consequently (68) and (70) together become $\mathbf{s}^H\mathbf{Q}_b\mathbf{s} = \frac{\gamma}{E_{max}}$. Then, the KKT necessary conditions are (72), together with $\beta > 0$, $\mu > 0$, and the constraints $\mathbf{s}^H\mathbf{R}_b\mathbf{s} = \frac{\gamma}{E_{max}}$, $\mathbf{s}^H\mathbf{s} = 1$. The proof of Proposition 2 is complete. ∎

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. Inf. 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. Inf. Theory*, vol. 54, pp. 4687-4698, Oct. 2008.

[7] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," *IEEE Trans. Inf. Theory*, vol. 57, pp. 1975-1982, Apr. 2010.

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

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

[10] 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.

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

[12] 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.

[13] 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.

[14] 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.

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

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

[17] 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.

[18] 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.

[19] 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.

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

[21] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Forens. Security*, vol. 6, pp. 532-540, Sept. 2011.

[22] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, pp. 2933-2945, Aug. 2008.

[23] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2515-2534, June 2008.

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

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

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

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

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

[29] 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 Process.*, vol. 59, pp. 1202-1216, Mar. 2011.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] T. De Bie, N. Cristianini, and R. Rosipal, "Eigenproblems in pattern recognition," in *Handbook of Geometric Computing: Applications in Pattern Recognition, Computer Vision, Neuralcomputing, and Robotics*, E. Bayro-Corrochano (editor). New York, NY: Springer, Aug. 2005, pp. 129-170.

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

[38] R. A. Horn and C. R. Johnson. *Matrix Analysis*, NY, USA: Cambridge University Press, 1985.

[39] C. D. Meyer. *Matrix Analysis and Applied Linear Algebra*, Philadelphia, PA: SIAM, 2000.

[40] Z.-Q. Luo, W.-K. Ma, A. M.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems: From its practical deployments and scope of applicability to key theoretical results," *IEEE Signal Process. Mag.*, Special Issue on Convex Optimiz. Signal Proc., vol. 27, pp. 20-34, May 2010.

[41] J. F. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optimization Methods and Software*, vol. 11-12, pp. 625-653, 1999.

[42] M. Grant and S. Boyd, *CVX: MATLAB Software for Disciplined Convex Programming*, June 2009, [Online]. Available: http://stanford.edu/ boyd/cvx

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

Ming Li (S'05, M'11) received the M.S. and Ph.D. degrees in electrical engineering from the State University of New York at Buffalo, Buffalo, in 2005 and 2010, respectively. He is currently a Post-Doctoral Research Associate with the Signals, Communications, and Networking Research Group, Department of Electrical Engineering, State University of New York at Buffalo.

His research interests include spread-spectrum communications and adaptive multiuser detection, cognitive radios and networks, covert communications and steganography, physical layer secrecy, compressed sensing.

Dr. Li is a member of the IEEE Communications and Signal Processing Societies.

Sandipan Kundu received his B.S. and M.S. degrees in electrical engineering from the State University of New York at Buffalo in 2006 and 2008, respectively. He is currently a Ph.D. candidate and member of the Signals, Communications, and Networking Research Group, Department of Electrical Engineering, State University of New York at Buffalo.

His research interests include space-time coding, low-complexity multi-antenna, multi-user detection, physical layer secrecy, cognitive radio, and optimization of wireless feedback protocols.

Mr. Kundu is a recipient of the University at Buffalo Graduate Presidential Fellowship Award and the Motorola Senior Scholar Award.

Dimitris A. Pados (M'95) was born in Athens, Greece, on October 22, 1966. He received the Diploma degree in computer science and engineering (five-year program) from the University of Patras, Greece, in 1989, and the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, in 1994.

From 1994 to 1997, he held an Assistant Professor position in the Department of Electrical and Computer Engineering and the Center for Telecommunications Studies, University of Louisiana, Lafayette. Since August 1997, he has been with the Department of Electrical Engineering, State University of New York at Buffalo, where he is presently a Professor. He served the Department as Associate Chair in 2009-2010. Dr. Pados was elected three times University Faculty Senator (terms 2004-06, 2008-10, 2010-12) and served on the Faculty Senate Executive Committee in 2009-10.

His research interests are in the general areas of communication theory and adaptive signal processing with applications to interference channels and signal waveform design, secure wireless communications, cognitive radios and networks.

Dr. Pados is a member of the IEEE Signal Processing, Communications, Information Theory, and Computational Intelligence Societies. He served as an Associate Editor for the IEEE Signal Processing Letters from 2001 to 2004 and the IEEE Transactions on Neural Networks from 2001 to 2005. He received a 2001 IEEE International Conference on Telecommunications best paper award, the 2003 IEEE Transactions on Neural Networks Outstanding Paper Award, and the 2010 IEEE International Communications Conference Best Paper Award in Signal Processing for Communications for articles that he coauthored with students and colleagues. Professor Pados is a recipient of the 2009 SUNY-system-wide Chancellor's Award for Excellence in Teaching and the 2011 University at Buffalo Exceptional Scholar - Sustained Achievement Award.

Stella N. Batalama (S'91, M'94, SM'13) received the Diploma degree in computer engineering and science (5-year program) from the University of Patras, Greece in 1989 and the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, in 1994.

In 1995 she joined the Department of Electrical Engineering, State University of New York at Buffalo, Buffalo, NY, where she is presently a Professor. From 2009 to 2011, she served as the Associate Dean for Research of the School of Engineering and Applied Sciences and since 2010, she is serving as the Chair of the Electrical Engineering Department. During the summers of 1997-2002 she was Visiting Faculty in the U.S. Air Force Research Laboratory (AFRL), Rome, NY. From Aug. 2003 to July 2004 she served as the Acting Director of the AFRL Center for Integrated Transmission and Exploitation (CITE), Rome NY.

Her research interests include small-sample-support adaptive filtering and receiver design, cooperative and cognitive communications and networks, covert communications and steganography, robust spread-spectrum communications and adaptive multiuser detection, compressive sampling. Dr. Batalama was an associate editor for the IEEE Communications Letters (2000-2005) and the IEEE Transactions on Communications (2002-2008).