Secure Array Synthesis

Rashid Mehmood, *Student Member, IEEE*, Jon W. Wallace, *Senior Member, IEEE*, and Michael A. Jensen, *Fellow, IEEE*

***Abstract*—A new array synthesis problem, whose objective is to maximize secure information shared with a legitimate recipient in the presence of a passive eavesdropper, is posed for line-of-sight (LOS) wireless transmission. By casting the problem into the form of a semidefinite program, it is found that the problem is convex and that optimal solutions can be efficiently found irrespective of the array topology. Representative results for a uniform linear array (ULA) and uniform circular array (UCA) are presented to demonstrate the utility of the method. Furthermore, it is shown that the radiated power of the optimal solution can be naturally decomposed into a *signal pattern* and *noise pattern*, providing an intuitive description of the optimal solutions and allowing comparison with standard array synthesis techniques.**

***Index Terms*—Adaptive arrays, antenna radiation pattern synthesis, security.**

I. Introduction

SECURITY is an important concern for today's wireless communications systems, where the public nature of the transmission enables potential interception of sensitive information by unauthorized parties. Typically, wireless security is accomplished by encrypting binary information before modulation and transmission over the channel. However, recent work has focused on developing techniques that exploit the physical layer, including the antennas and propagation channel, to provide increased security in wireless transmissions. Examples of such techniques may be found in [1]–[12].

One method for using the physical layer to achieve increased secrecy is to use conventional antenna array synthesis to design a transmit radiation pattern that provides high gain to a desired receiver and low gain in directions of potential eavesdroppers [13]. Such an approach reduces the likelihood that an attacker can decode the information-bearing signal, particularly if the channel coding is carefully matched to the realized channel gain. The information-carrying transmit radiation pattern designed in this way is referred to herein as the *signal pattern*. To further enhance security, artificial noise can be transmitted on *noise patterns* that are ideally designed to be orthogonal to the signal pattern, thereby realizing low artificial noise levels to the desired receiver and higher noise in the direction of eavesdroppers [14]–[17]. This enables enhanced control over the signal-to-noise ratio (SNR) (and therefore decoding probability) observed at unauthorized nodes.

Although array synthesis is a mature topic, and there are many powerful techniques available for synthesizing an individual pattern with desired properties, no work has demonstrated how to *jointly* synthesize signal and noise patterns to obtain *optimal* secrecy. This paper solves this outstanding problem of *secure array synthesis* by posing the secure transmission problem in a form analogous to that of conventional array synthesis, but in which we constrain information-theoretic secrecy metrics as a function of eavesdropper angle as opposed to constraining radiated power as a function of transmission angle. The resulting convex optimization problem can be solved using semidefinite programming (SDP) [18] to produce the covariance matrix for the signals transmitted by the array. This covariance is then decomposed to identify the signal and noise patterns. Numerical results and comparisons with a conventional but suboptimal method demonstrate the effectiveness of the new pattern synthesis technique.

II. Problem Statement

This initial treatment considers a narrowband, two-dimensional (2-D) scenario, with a discussion of the extension to wideband operation and three-dimensional (3-D) radiation appearing in Section V-C. Fig. 1 shows a free-space communications scenario involving three nodes. Alice and Bob are legitimate nodes who wish to communicate securely, while Eve is a passive eavesdropper who attempts to receive and decode Alice's and Bob's transmissions. It is assumed that all nodes know the angles of Alice ($\phi_{\rm A}$) and Bob ($\phi_{\rm B}$), whereas Eve's angle ($\phi_{\rm E}$) is unknown to Alice and Bob.

Consistent with traditional antenna array synthesis, a free-space or line-of-sight (LOS) channel is assumed with Bob and Eve in the far-field of Alice's array of $N_{\rm T}$ elements. It is sufficient to consider a single antenna at Bob and Eve, as using arrays (or changing element gain patterns) only changes the SNR observed at these nodes, a quantity already controlled by model parameters. The channels denoted $\mathbf{h}_{\rm AB}$, $\mathbf{h}_{\rm BA}$, and $\mathbf{h}_{\rm AE}$ are vectors that represent the complex baseband gains from Alice's array to Bob's antenna, from Bob's antenna to Alice's array, and from Alice's array to Eve's antenna, respectively. These channel vectors are scaled versions of the electromagnetic steering vectors, or

$$h_{{\rm A}\xi,i} = g_i(\phi_\xi)\exp[jk_0(a_{x,i}\cos\phi_\xi + a_{y,i}\sin\phi_\xi)] \quad (1)$$

Manuscript received September 18, 2014; revised April 23, 2015; accepted June 06, 2015; Date of publication June 22, 2015; date of current version September 01, 2015. This work was supported in part by the German Science Foundation (DFG) under the COIN Priority Program and in part by the U.S. Army Research Office under Grant W911NF-12-1-0469.

R. Mehmood is with Wavetronix, LLC, Provo, UT 84606 USA (e-mail: r.mehmood@ieee.org).

J. W. Wallace is with Lafayette College, Easton, PA 18042 USA (e-mail: wall@ieee.org).

M. A. Jensen is with Brigham Young University, Provo, UT 84602 USA (e-mail: jensen@byu.edu).

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

Digital Object Identifier 10.1109/TAP.2015.2448110

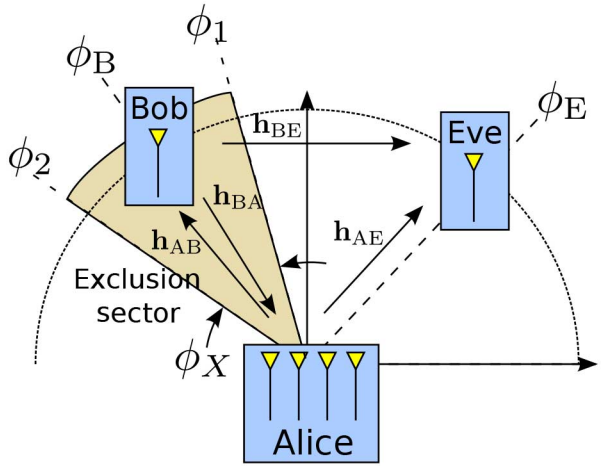

Fig. 1. Generic system model for secure array synthesis.

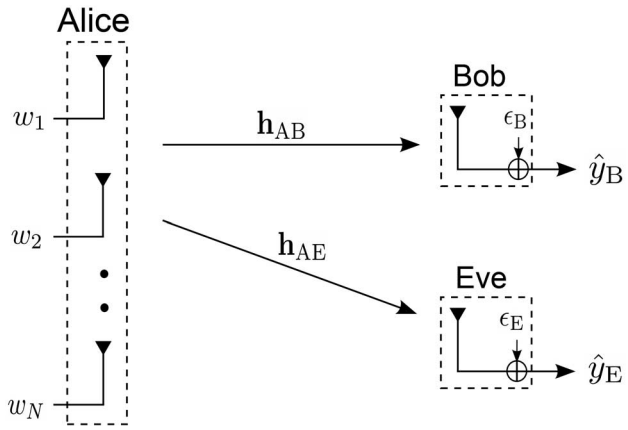

Fig. 2. Signal model for secrecy capacity.

where $\xi \in \{\mathrm{B}, \mathrm{E}\}$, $h_{\mathrm{BA},i} = h_{\mathrm{AB},i}$, k_0 is the free-space wavenumber and $g_i(\phi)$ and $(a_{x,i}, a_{y,i})$ are, respectively, the field radiation pattern and coordinate of the ith antenna in Alice's array. It is assumed that Eve knows all of the channel gains, whereas Alice and Bob know only $\mathbf{h}_{\mathrm{AB}}$ and $\mathbf{h}_{\mathrm{BA}}$.

In this LOS environment, if Bob and Eve are close in angle, it will be difficult to provide different signals to the two, based only on beamforming. Therefore, we define an *exclusion sector*, which is an angular extent ϕ_{X} ranging from ϕ_1 to ϕ_2 that is assumed to be free of eavesdroppers. In some cases, it may be possible to ensure that this sector is eavesdropper-free by using visual information or restricting physical access. When this is *not* possible, having an eavesdropper in the exclusion sector will compromise physical layer security, meaning that secrecy must rely on upper layer protocols alone.

An informal problem statement for secure array synthesis is as follows: find Alice's array signaling strategy to maximize the information exchanged between Alice and Bob while minimizing the information given to an eavesdropper outside of the exclusion sector. This is very similar to standard array synthesis where a typical objective is to maximize the gain in the direction of the intended receiver (the main beam direction) while minimizing sidelobe transmission outside of the main beam. While this informal problem statement is helpful, we now seek to more precisely formulate the problem statement by considering two specific security metrics.

A. Secrecy Capacity

Secrecy capacity is defined as the maximum amount of information that can be transmitted between legitimate nodes without providing useful information to an eavesdropper. Fig. 2 depicts a detailed signal model that allows secrecy capacity to be defined for the LOS scenario in Fig. 1. In this model, for a single use of the channel, Alice transmits the complex baseband vector $\mathbf{w}$ that produces the signals $\hat{y}_{\mathrm{B}}$ and $\hat{y}_{\mathrm{E}}$ at Bob and Eve, respectively. Mathematically, we have

$$\hat{y}_\xi = \underbrace{\mathbf{h}_{\mathrm{A}\xi}^T \mathbf{w}}_{y_\xi} + \epsilon_\xi \quad (\xi \in \{\mathrm{B}, \mathrm{E}\}) \tag{2}$$

where $\{\cdot\}^T$ is a transpose and ϵ_ξ represents noise modeled as a zero-mean complex Gaussian random variable. We set $\mathrm{E}\{|\epsilon_{\mathrm{B}}|^2\} = \sigma_0^2$ and make the worst-case assumption that Eve's receiver is noiseless ($\epsilon_{\mathrm{E}} = 0$).

Secrecy capacity C_{S} for this model is the maximum mutual information that Alice and Bob can attain, conditioned on Eve's signal when Eve is at the worst-case position for security. This can be interpreted as the maximum secret information that Alice can transmit to Bob over all possible angles for Eve outside of the exclusion sector, or

$$C_{\mathrm{S}} = \max_{p(\mathbf{w})} \min_{\phi_{\mathrm{E}}} I(\mathbf{w}; \hat{y}_{\mathrm{B}} | \hat{y}_{\mathrm{E}}) \tag{3}$$

where

$$I(\mathbf{w}; \hat{y}_{\mathrm{B}} | \hat{y}_{\mathrm{E}}) = H(\hat{y}_{\mathrm{B}} | \hat{y}_{\mathrm{E}}) - H(\hat{y}_{\mathrm{B}} | \mathbf{w}, \hat{y}_{\mathrm{E}}) \tag{4}$$

$$= H(\hat{y}_{\mathrm{B}}, \hat{y}_{\mathrm{E}}) - H(\hat{y}_{\mathrm{E}}) - H(\epsilon_{\mathrm{B}}) \tag{5}$$

$I(\cdot;\cdot)$ is mutual information, $p(\mathbf{w})$ is the probability density function (pdf) of the vector $\mathbf{w}$, and $H(\cdot)$ is differential entropy. Note that in the minimization in (3), the minimizing ϕ_{E} can be a function of $p(\mathbf{w})$, which means that all possible Eve angles must be considered simultaneously in the minimization.

Assuming zero-mean complex Gaussian signaling, the pdf $p(\mathbf{w})$ is completely determined by its covariance matrix $\mathbf{R} = \mathrm{E}\{\mathbf{w}\mathbf{w}^H\}$, where $\{\cdot\}^H$ is a conjugate transpose. We constrain $\mathbf{R}$ to satisfy $\mathrm{Tr}(\mathbf{AR}) \le P_{\mathrm{T}}$, where $\mathrm{Tr}(\cdot)$ is trace, $\mathbf{A}$ is a coupling matrix [19], and P_{T} is the available transmit power. For uncoupled transmit antennas, $\mathbf{A} = \mathbf{I}$ where $\mathbf{I}$ is the identity matrix. The optimization problem in (3) becomes

$$C_{\mathrm{S}} = \max_{\mathbf{R}:\mathrm{Tr}(\mathbf{AR}) \le P_{\mathrm{T}}} \min_{\phi_{\mathrm{E}}} I(\mathbf{w}; \hat{y}_{\mathrm{B}} | \hat{y}_{\mathrm{E}}) \tag{6}$$

$$I(\mathbf{w}; \hat{y}_{\mathrm{B}} | \hat{y}_{\mathrm{E}}) = \log_2 \frac{|\mathbf{R}_{\mathrm{BE}}|}{\sigma_{\mathrm{E}}^2 \sigma_0^2} \tag{7}$$

where

$$\mathbf{R}_{\mathrm{BE}} = \mathrm{E}\{[\hat{y}_{\mathrm{B}},\ \hat{y}_{\mathrm{E}}]^T [\hat{y}_{\mathrm{B}},\ \hat{y}_{\mathrm{E}}]^*\} = \begin{bmatrix} \sigma_{\mathrm{B}}^2 + \sigma_0^2 & \sigma_{\mathrm{BE}} \\ \sigma_{\mathrm{BE}}^* & \sigma_{\mathrm{E}}^2 \end{bmatrix} \tag{8}$$

$$\sigma_\xi^2 = \mathrm{E}\{|y_\xi|^2\} = \mathbf{h}_{\mathrm{A}\xi}^T \mathbf{R} \mathbf{h}_{\mathrm{A}\xi}^* \quad (\xi \in \{\mathrm{B}, \mathrm{E}\}) \tag{9}$$

$$\sigma_{\mathrm{BE}} = \mathrm{E}\{y_{\mathrm{B}} y_{\mathrm{E}}^*\} = \mathbf{h}_{\mathrm{AB}}^T \mathbf{R} \mathbf{h}_{\mathrm{AE}}^* \tag{10}$$

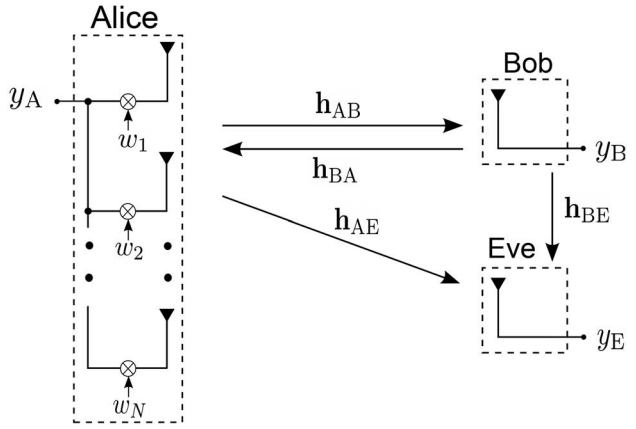

Fig. 3. Signal model for reciprocal channel key establishment.

$|\cdot|$ is the determinant and $\{\cdot\}^*$ is the conjugate. Using (8), (7) becomes

$$I(\mathbf{w};\hat{y}_{\mathrm{B}}|\hat{y}_{\mathrm{E}}) = \log_2 \frac{(\sigma_{\mathrm{B}}^2+\sigma_0^2)\sigma_{\mathrm{E}}^2 - |\sigma_{\mathrm{BE}}|^2}{\sigma_{\mathrm{E}}^2\sigma_0^2} \tag{11}$$

$$= \log_2\left[1 + \underbrace{\frac{\sigma_{\mathrm{B}}^2}{\sigma_0^2}\left(1-\frac{|\sigma_{\mathrm{BE}}|^2}{\sigma_{\mathrm{B}}^2\sigma_{\mathrm{E}}^2}\right)}_{\alpha(\mathbf{R},\phi_{\mathrm{E}})}\right]. \tag{12}$$

Our optimization problem is therefore

$$C_{\mathrm{S}} = \max_{\mathbf{R}:\mathrm{Tr}(\mathbf{AR})\le P_{\mathrm{T}}} \min_{\phi_{\mathrm{E}}} \log_2[1+\alpha(\mathbf{R},\phi_{\mathrm{E}})]. \tag{13}$$

Since $\log_2(\cdot)$ increases monotonically in its argument, we only need to find the transmission strategy that maximizes α, or

$$\alpha_{\mathrm{opt}} = \max_{\mathbf{R}:\mathrm{Tr}(\mathbf{AR})\le P_{\mathrm{T}}} \min_{\phi_{\mathrm{E}}} \alpha(\mathbf{R},\phi_{\mathrm{E}}) \tag{14}$$

where $C_{\mathrm{S}} = \log_2(1+\alpha_{\mathrm{opt}})$.

B. Reciprocal Channel Key Establishment

Another mechanism for secure wireless communication is to encode transmissions using secret keys [1], [8]. To establish keys at the physical layer, Alice and Bob can each transmit known training data from which the other can estimate the channel, and since by reciprocity the two estimates differ only due to measurement errors, they can be quantized to form the encryption key. In a fading environment, the radios can estimate multiple independent channel observations over time and thereby construct long keys [20].

Since the propagation channel does not fade in our LOS scenario, we use beamforming weights to generate random channel observations, much like what has been done using reconfigurable antennas [6], [9]. Referring to Fig. 3, Alice uses a randomly generated weight vector $\mathbf{w}$ to transmit a scalar pilot y_{A}, resulting in received signals y_{B} at Bob and y_{E} at Eve. Next, Bob transmits a scalar pilot $y_{\mathrm{B}'}$, and Eve observes $y_{\mathrm{E}'}$ while Alice weights the received signals by the vector $\mathbf{w}$ to obtain $y_{\mathrm{A}'}$. By randomly changing $\mathbf{w}$ over time, different channel observations can be realized.

The effective end-to-end propagation channels created using this procedure are defined as

$$h_{\mathrm{AB}} = y_{\mathrm{B}}/y_{\mathrm{A}} = \mathbf{h}_{\mathrm{AB}}^T\mathbf{w} \tag{15}$$

$$h_{\mathrm{BA}} = y_{\mathrm{A}'}/y_{\mathrm{B}'} = \mathbf{h}_{\mathrm{BA}}^T\mathbf{w} = h_{\mathrm{AB}} \tag{16}$$

$$h_{\mathrm{AE}} = y_{\mathrm{E}}/y_{\mathrm{A}} = \mathbf{h}_{\mathrm{AE}}^T\mathbf{w}. \tag{17}$$

Since $h_{\mathrm{BE}} = y_{\mathrm{E}'}/y_{\mathrm{B}'}$ is not random (has no information), it is ignored. We assume that only estimates of the channels are obtained, or

$$\hat{h}_{\xi\xi'} = h_{\xi\xi'} + \epsilon_{\xi'} \quad (\xi\xi' \in \{\mathrm{AB},\mathrm{BA},\mathrm{AE}\}) \tag{18}$$

where $\epsilon_{\xi'}$ is zero-mean complex Gaussian noise with $\mathrm{E}\{|\epsilon_{\xi'}|^2\} = \hat{\sigma}_{\xi'}^2$.

The reciprocal fading channels between Alice and Bob can be used to generate secret encryption keys. One secrecy metric for reciprocal channel key establishment is the number of *secure key bits* given by

$$I_{\mathrm{SK}} = I(\hat{h}_{\mathrm{AB}};\hat{h}_{\mathrm{BA}}|\hat{h}_{\mathrm{AE}}). \tag{19}$$

Assuming that the random vector $\mathbf{w}$ is drawn from a zero-mean complex Gaussian distribution and independently realized for each measurement, we have

$$I_{\mathrm{SK}} = \log_2 \frac{|\mathbf{R}_{\mathrm{BA}}||\mathbf{R}_{\mathrm{AB}}|}{\sigma_{\mathrm{B}}^2|\widetilde{\mathbf{R}}|} \tag{20}$$

where

$$\mathbf{R}_{\xi\xi'} = \mathrm{E}\{[\hat{h}_{\xi\xi'},\,\hat{h}_{\mathrm{AE}}]^T[\hat{h}_{\xi\xi'},\,\hat{h}_{\mathrm{AE}}]^*\} \tag{21}$$

$$= \begin{bmatrix} \sigma_{\mathrm{B}}^2+\hat{\sigma}_{\xi'}^2 & \sigma_{\mathrm{BE}} \\ \sigma_{\mathrm{BE}}^* & \sigma_{\mathrm{E}}^2+\hat{\sigma}_{\mathrm{E}}^2 \end{bmatrix} \quad (\xi\xi' \in \{\mathrm{AB},\mathrm{BA}\}) \tag{22}$$

$$\widetilde{\mathbf{R}} = \mathrm{E}\{[\hat{h}_{\mathrm{BA}},\,\hat{h}_{\mathrm{AB}},\,\hat{h}_{\mathrm{AE}}]^T[\hat{h}_{\mathrm{BA}},\,\hat{h}_{\mathrm{AB}},\,\hat{h}_{\mathrm{AE}}]^*\} \tag{23}$$

$$= \begin{bmatrix} \sigma_{\mathrm{B}}^2+\hat{\sigma}_{\mathrm{A}}^2 & \sigma_{\mathrm{B}}^2 & \sigma_{\mathrm{BE}} \\ \sigma_{\mathrm{B}}^2 & \sigma_{\mathrm{B}}^2+\hat{\sigma}_{\mathrm{B}}^2 & \sigma_{\mathrm{BE}} \\ \sigma_{\mathrm{BE}}^* & \sigma_{\mathrm{BE}}^* & \sigma_{\mathrm{E}}^2+\hat{\sigma}_{\mathrm{E}}^2 \end{bmatrix} \tag{24}$$

$$\sigma_{\xi}^2 = \mathrm{E}\{|h_{\mathrm{A}\xi}|^2\} = \mathbf{h}_{\mathrm{A}\xi}^T\mathbf{R}\mathbf{h}_{\mathrm{A}\xi}^* \quad (\xi \in \{\mathrm{B},\mathrm{E}\}) \tag{25}$$

$$\sigma_{\mathrm{BE}} = \mathrm{E}\{h_{\mathrm{AB}}h_{\mathrm{AE}}^*\} = \mathbf{h}_{\mathrm{AB}}^T\mathbf{R}\mathbf{h}_{\mathrm{AE}}^*. \tag{26}$$

Assuming equal estimation error variance at Alice and Bob ($\hat{\sigma}_{\mathrm{A}}^2 = \hat{\sigma}_{\mathrm{B}}^2 = \sigma_0^2$) and a noiseless receiver at Eve ($\epsilon_{\mathrm{E}} = 0$), we can expand the determinants in (20) to obtain

$$I_{\mathrm{SK}} = \log_2 \frac{1}{\sigma_{\mathrm{E}}^2} \frac{[(\sigma_{\mathrm{B}}^2+\sigma_0^2)\sigma_{\mathrm{E}}^2 - |\sigma_{\mathrm{BE}}|^2]^2}{\sigma_{\mathrm{E}}^2(\sigma_0^4+2\sigma_{\mathrm{B}}^2\sigma_0^2) - 2\sigma_0^2|\sigma_{\mathrm{BE}}|^2} \tag{27}$$

$$= \log_2 \frac{[1+\alpha(\mathbf{R},\phi_{\mathrm{E}})]^2}{1+2\alpha(\mathbf{R},\phi_{\mathrm{E}})} \tag{28}$$

where

$$\alpha(\mathbf{R},\phi_{\mathrm{E}}) = \frac{\sigma_{\mathrm{B}}^2}{\sigma_0^2}\left(1-\frac{|\sigma_{\mathrm{BE}}|^2}{\sigma_{\mathrm{B}}^2\sigma_{\mathrm{E}}^2}\right) \tag{29}$$

which is precisely the expression for α obtained in (11) for secrecy capacity. Note that I_{SK} in (28) increases monotonically in $\alpha(\mathbf{R},\phi_{\mathrm{E}}) \ge 0$, and we once again only need to maximize α

according to (14) to obtain $\alpha_{\rm opt}$. The optimal $I_{\rm SK}$ is then given by (28) with $\alpha(\mathbf{R},\phi_{\rm E})=\alpha_{\rm opt}$.

It is remarkable that both secrecy capacity and the number of secure key bits depend monotonically on $\alpha(\mathbf{R},\phi_{\rm E})$, allowing both problems to be solved using the same procedure. This observation further motivates use of the general term *secure array synthesis* for the solution.

III. Optimization Procedure

We now show that our optimization problem in (14) can be written as a standard semidefinite program, indicating that our problem is convex and can be solved efficiently. One form of SDP solves the problem [18]

$$\min_{\mathbf{x}} \mathbf{c}^T\mathbf{x}, \quad \text{s.t.} \quad \mathbf{F}(\mathbf{x})=\mathbf{F}_0+\sum_{m=1}^{M} x_m\mathbf{F}_m \geq 0 \tag{30}$$

where $\mathbf{\Gamma}\geq 0$ indicates that $\mathbf{\Gamma}$ is a positive semidefinite (PSD) matrix. To rewrite our problem in this form, we first transform it to the constrained optimization

$$\alpha'_{\rm opt}=\max_{\gamma,\mathbf{R}}\gamma \quad \text{s.t.} \begin{cases} \text{(i)} & \alpha'(\mathbf{R},\phi_{\rm E})\geq\gamma \quad \forall\phi_{\rm E}\notin[\phi_1,\phi_2] \\ \text{(ii)} & \mathrm{Tr}(\mathbf{AR})\leq P_{\rm T} \\ \text{(iii)} & \mathbf{R}\geq 0 \\ \text{(iv)} & \gamma\geq 0 \end{cases} \tag{31}$$

where $\alpha'_{\rm opt}=\sigma_0^2\alpha_{\rm opt}$ and $\alpha'(\mathbf{R},\phi_{\rm E})=\sigma_0^2\alpha(\mathbf{R},\phi_{\rm E})$. In the following sections, we show how to cast the optimization into the general form of (30) and how each of the constraints (i)–(iv) in (31) can be written as a PSD constraint.

A. Optimization Variables

We first parameterize the unknown covariance matrix $\mathbf{R}$ in terms of a set of unknown coefficients. This can be accomplished by expanding $\mathbf{R}$ using a matrix basis, or

$$\mathbf{R}=\sum_{m=1}^{M-1} r_m\mathbf{R}_m. \tag{32}$$

A suitable set of basis matrices that span all possible PSD matrices is given by the set $S=S_R\cup S_I$, where

$$S_R=\{\mathbf{I}+(\mathbf{E}_{mn}+\mathbf{E}_{nm})/2\}, \quad 1\leq m\leq N_{\rm T}, \quad n\geq m \tag{33}$$

$$S_I=\{\mathbf{I}+j(\mathbf{E}_{mn}-\mathbf{E}_{nm})/2\}, \quad 1\leq m\leq N_{\rm T}, \quad n>m \tag{34}$$

and $\mathbf{E}_{mn}$ is an elementary matrix with 1 at position mn and zeros elsewhere. For $N_{\rm T}=2$, e.g., the basis is

$$S=\left\{\begin{bmatrix}2&0\\0&1\end{bmatrix},\begin{bmatrix}1&0\\0&2\end{bmatrix},\begin{bmatrix}1&\frac{1}{2}\\\frac{1}{2}&1\end{bmatrix},\begin{bmatrix}1&\frac{j}{2}\\-\frac{j}{2}&1\end{bmatrix}\right\}. \tag{35}$$

With this formulation, the unknowns consist of the $M-1$ values of r_m and the value of γ in (31). Therefore, the $M\times 1$ vector of real optimization variables is

$$\mathbf{x}=[r_1,\ r_2,\ldots,r_{M-1},\ \gamma]^T. \tag{36}$$

The maximization in (31) can be cast into the minimization form of (30) using $\mathbf{c}=[0\ldots 0-1]^T$.

B. Constraint (i): Minimum α Threshold

We refer to constraint (i) in (31) as a minimum α threshold, since its purpose is to ensure that α is no lower than a certain minimum level for all possible Eve angles. One difficulty is that (i) represents an infinite number of constraints, one at each possible value of $\phi_{\rm E}$ outside of the exclusion sector. We replace this with a finite set of K constraints by uniformly sampling Eve's possible angle at K values outside of the exclusion sector, which we denote $\phi_{{\rm E},k}$, where $\phi_{{\rm E},k}\notin[\phi_1,\phi_2]$. This results in the set of constraints

$$\sigma_0^2\alpha(\mathbf{R},\phi_{{\rm E},k})\geq\gamma, \quad k=1,\ldots,K. \tag{37}$$

Substituting the basis expansion (32) into (29)

$$\sigma_0^2\alpha(\mathbf{R},\phi_{\rm E})=\frac{\sigma_{\rm B}^2\sigma_{\rm E}^2-|\sigma_{\rm BE}|^2}{\sigma_{\rm E}^2} \tag{38}$$

$$=\frac{\mathbf{h}_{\rm AB}^T\mathbf{R}\mathbf{h}_{\rm AB}^*\mathbf{h}_{\rm AE}^T\mathbf{R}\mathbf{h}_{\rm AE}^*-\mathbf{h}_{\rm AB}^T\mathbf{R}\mathbf{h}_{\rm AE}^*\mathbf{h}_{\rm AE}^T\mathbf{R}\mathbf{h}_{\rm AB}^*}{\mathbf{h}_{\rm AE}^T\mathbf{R}\mathbf{h}_{\rm AE}^*} \tag{39}$$

$$=\frac{\mathbf{u}^T\mathbf{r}\mathbf{v}^{(k)T}\mathbf{r}-\mathbf{z}^{(k)T}\mathbf{r}\mathbf{z}^{(k)H}\mathbf{r}}{\mathbf{v}^{(k)T}\mathbf{r}} \tag{40}$$

where

$$u_m=\mathbf{h}_{\rm AB}^T\mathbf{R}_m\mathbf{h}_{\rm AB}^* \tag{41}$$

$$v_m^{(k)}=\mathbf{h}_{\rm AE}(\phi_{{\rm E},k})^T\mathbf{R}_m\mathbf{h}_{\rm AE}(\phi_{{\rm E},k})^* \tag{42}$$

$$z_m^{(k)}=\mathbf{h}_{\rm AB}^T\mathbf{R}_m\mathbf{h}_{\rm AE}(\phi_{{\rm E},k})^*. \tag{43}$$

The constraint (37) can therefore be written as

$$\mathbf{v}^{(k)T}\mathbf{r}(\mathbf{u}^T\mathbf{r}-\gamma)-(\mathbf{z}^{(k)T}\mathbf{r})(\mathbf{z}^{(k)H}\mathbf{r})\geq 0, \quad k=1,\ldots,K \tag{44}$$

which can be written as the determinant constraint

$$\underbrace{\begin{vmatrix}\mathbf{u}^T\mathbf{r}-\gamma & \mathbf{z}^{(k)T}\mathbf{r}\\ \mathbf{z}^{(k)H}\mathbf{r} & \mathbf{v}^{(k)T}\mathbf{r}\end{vmatrix}}_{\mathbf{F}_{\rm E}^{(k)}}\geq 0. \tag{45}$$

This is equivalent to the PSD constraint $\mathbf{F}_{\rm E}^{(k)}\geq 0$. We can expand the matrix $\mathbf{F}_{\rm E}^{(k)}$ in terms of the unknown optimization variables $\mathbf{r}$ and γ as

$$\mathbf{F}_{\rm E}^{(k)}=\sum_{m=1}^{M-1}\underbrace{\begin{bmatrix}u_m & z_m^{(k)}\\ z_m^{(k)*} & v_m^{(k)}\end{bmatrix}}_{\mathbf{F}_{{\rm E},m}^{(k)}}r_m+\underbrace{\begin{bmatrix}-1&0\\0&0\end{bmatrix}}_{\mathbf{F}_{{\rm E},M}^{(k)}}\gamma \tag{46}$$

$$=\mathbf{F}_{{\rm E},0}^{(k)}+\sum_{m=1}^{M}x_m\mathbf{F}_{{\rm E},m}^{(k)}\geq 0 \tag{47}$$

where $\mathbf{F}_{{\rm E},0}^{(k)}$ is the zero matrix.

C. Constraint (ii): Power Constraint

Substituting the basis expansion (32) into the power constraint (ii) gives

$$\mathrm{Tr}(\mathbf{AR})=\sum_{m=1}^{M-1}r_m\mathrm{Tr}(\mathbf{AR}_m)\leq P_{\rm T} \tag{48}$$

or

$$\underbrace{P_{\mathrm{T}}}_{F_{\mathrm{P},0}} + \sum_{m=1}^{M-1} r_m \underbrace{[-\mathrm{Tr}(\mathbf{A}\mathbf{R}_m)]}_{F_{\mathrm{P},m}} \geq 0. \tag{49}$$

To write this in the form of (30), we must define $F_{\mathrm{P},M} = 0$.

D. Constraint (iii): PSD Constraint on $\mathbf{R}$

Note that although each of the basis matrices is Hermitian and PSD, a linear combination of these matrices is still Hermitian but not necessarily PSD. To represent an admissible solution, the transmit covariance must be PSD, or

$$\mathbf{R} = \sum_{m=1}^{M-1} r_m \mathbf{R}_m \geq 0 \tag{50}$$

which is in the form of (30) with

$$\mathbf{F}_{\mathrm{C},m} = \begin{cases} \mathbf{0}, & m = 0, m = M \\ \mathbf{R}_m, & 1 \leq m \leq M-1. \end{cases} \tag{51}$$

E. Constraint (iv): Nonnegativity Constraint on γ

The constraint $\gamma \geq 0$ is in the form of (30) with

$$F_{\gamma,m} = \begin{cases} 0, & 0 \leq m \leq M-1 \\ 1, & m = M. \end{cases} \tag{52}$$

F. Solution Using MAXDET

Solutions to our SDP problem are found using the freely available MAXDET package [21] that solves (30).[1] While many of our constraint matrices are complex, MAXDET and many other SDP solvers require that the constraint matrices be real. Fortunately, it can be shown that a square complex matrix $\mathbf{F}$ satisfies

$$\mathbf{F} \geq 0 \quad \text{if and only if} \quad \underline{\mathbf{F}} \geq 0 \tag{53}$$

where

$$\underline{\mathbf{F}} \triangleq \begin{bmatrix} \mathrm{Re}\{\mathbf{F}\} & -\mathrm{Im}\{\mathbf{F}\} \\ \mathrm{Im}\{\mathbf{F}\} & \mathrm{Re}\{\mathbf{F}\} \end{bmatrix}. \tag{54}$$

Therefore, our complex-valued PSD constraints can be expressed in the equivalent real-valued form

$$\underline{\mathbf{F}}(\mathbf{x}) = \underline{\mathbf{F}}_0 + \sum_{m=1}^{M} x_m \underline{\mathbf{F}}_m \geq 0. \tag{55}$$

Given this, the $K+3$ PSD constraints given in Sections III-B–III-E can be combined into a single PSD constraint using the block diagonal matrix

$$\underline{\mathbf{F}}_m = \mathrm{diag}\left(\left[\underline{\mathbf{F}}_{\mathrm{E},m}^{(1)},\ \underline{\mathbf{F}}_{\mathrm{E},m}^{(2)}, \ldots,\ \underline{\mathbf{F}}_{\mathrm{E},m}^{(K)},\ F_{\mathrm{P},m},\ \underline{\mathbf{F}}_{\mathrm{C},m},\ F_{\gamma,m}\right]\right) \tag{56}$$

where $\mathrm{diag}(\cdot)$ creates a matrix with the vector elements arranged on the main diagonal.

[1] MAXDET actually minimizes $\mathbf{c}^T\mathbf{x} + \log_2 |\mathbf{G}(\mathbf{x})|^{-1}$ where $\mathbf{G} = \mathbf{G}_0 + \sum_m x_m \mathbf{G}_m > 0$. We let $G_0 = 1$ and $G_m = 0$ for $m > 1$.

IV. Patterns and Transmit Weights

Once the optimal covariance matrix $\mathbf{R}$ has been found using the outlined secure array synthesis procedure, it is desirable to visualize the solution. While one can simply plot the secrecy metric C_{S} or I_{SK} with respect to Eve's angle, such plots only indicate what security is *possible* and give no insight into how it is *achieved*. We here provide a more constructive visualization by decomposing the transmit power pattern into two patterns: one each for transmission of signal and noise. We also decompose the transmit covariance into signal and noise subspaces, revealing how to practically achieve the noise and signal patterns.

A. Signal/Noise Patterns

Since Gaussian signaling is used, Eve's observed quantity y_{E} (or h_{AE}) for a fixed angle ϕ_{E} can be decomposed into a sum of two terms as

$$y_{\mathrm{E}} = \beta_{\mathrm{C}} y_{\mathrm{B}} + y_{\mathrm{UC}} \tag{57}$$

where the first term is a Gaussian random variable that is perfectly correlated with Bob's signal (β_{C} is a constant) and the second term y_{UC} is a Gaussian random variable that is uncorrelated with Bob's signal. While Eve can extract useful information from the *signal* $\beta_{\mathrm{C}} y_{\mathrm{B}}$, the *noise* y_{UC} has no useful information content and serves to confuse Eve. Therefore, we define the signal and noise power observed by Eve as

$$P_{\mathrm{S}} = |\beta_{\mathrm{C}}|^2 \mathrm{E}\{|y_{\mathrm{B}}|^2\} \tag{58}$$

$$P_{\mathrm{N}} = \mathrm{E}\{|y_{\mathrm{UC}}|^2\} \tag{59}$$

respectively, which can be plotted as a function of Eve's angle.

To compute these quantities from the solution $\mathbf{R}$ obtained from the SDP optimization, we recognize that

$$\mathrm{E}\{|y_{\mathrm{E}}|^2\} = \sigma_{\mathrm{E}}^2 = |\beta_{\mathrm{C}}|^2 \mathrm{E}\{|y_{\mathrm{B}}|^2\} + \mathrm{E}\{|y_{\mathrm{UC}}|^2\} \tag{60}$$

$$\mathrm{E}\{y_{\mathrm{B}} y_{\mathrm{E}}^*\} = \sigma_{\mathrm{BE}} = \beta_{\mathrm{C}}^* \mathrm{E}\{|y_{\mathrm{B}}|^2\} \tag{61}$$

where we have used $\mathrm{E}\{y_{\mathrm{B}} y_{\mathrm{UC}}^*\} = 0$ based on our definition of y_{UC}. Using (8), we can solve (60) and (61) to obtain

$$P_{\mathrm{S}} = |\sigma_{\mathrm{BE}}|^2 / \sigma_{\mathrm{B}}^2 \tag{62}$$

$$P_{\mathrm{N}} = \sigma_{\mathrm{E}}^2 - |\sigma_{\mathrm{BE}}|^2 / \sigma_{\mathrm{B}}^2. \tag{63}$$

We emphasize that the signal/noise pattern interpretation in (62) and (63) provides the information required to compute C_{S} and I_{SK}. To see this, we write

$$\alpha(\mathbf{R}, \phi_{\mathrm{E}}) = \frac{\sigma_{\mathrm{B}}^2}{\sigma_0^2 \sigma_{\mathrm{E}}^2} \left(\sigma_{\mathrm{E}}^2 - \frac{|\sigma_{\mathrm{BE}}|^2}{\sigma_{\mathrm{B}}^2} \right) \tag{64}$$

$$= \frac{\sigma_{\mathrm{B}}^2}{\sigma_0^2} \frac{P_{\mathrm{N}}}{P_{\mathrm{S}} + P_{\mathrm{N}}} = \frac{\mathrm{SNR}_{\mathrm{Bob}}}{1 + \mathrm{SNR}_{\mathrm{Eve}}}. \tag{65}$$

B. Signal/Noise Weights

While the decomposition of the power pattern into signal and noise portions allows visualization of the results, it does not

specify the beamformer weights that achieve these patterns. Our objective here is to decompose the optimal transmit covariance as $\mathbf{R} = \mathbf{R}_{\mathrm{S}} + \mathbf{R}_{\mathrm{N}}$ where

$$P_{\mathrm{S}}(\phi_{\mathrm{E}}) = \mathbf{h}_{\mathrm{AE}}^{T}(\phi_{\mathrm{E}})\mathbf{R}_{\mathrm{S}}\mathbf{h}_{\mathrm{AE}}^{*}(\phi_{\mathrm{E}}) \tag{66}$$

$$P_{\mathrm{N}}(\phi_{\mathrm{E}}) = \mathbf{h}_{\mathrm{AE}}^{T}(\phi_{\mathrm{E}})\mathbf{R}_{\mathrm{N}}\mathbf{h}_{\mathrm{AE}}^{*}(\phi_{\mathrm{E}}). \tag{67}$$

These expressions indicate that if we transmit either signal or noise with respective covariances $\mathbf{R}_{\mathrm{S}}$ and $\mathbf{R}_{\mathrm{N}}$, Eve observes only the signal or noise pattern, respectively. Equating (62) and (66) and using the definitions of σ_{BE} and σ_{B}^2 lead to

$$\frac{(\mathbf{h}_{\mathrm{AE}}^{T}\mathbf{R}\mathbf{h}_{\mathrm{AB}}^{*})(\mathbf{h}_{\mathrm{AB}}^{T}\mathbf{R}\mathbf{h}_{\mathrm{AE}}^{*})}{\mathbf{h}_{\mathrm{AB}}^{T}\mathbf{R}\mathbf{h}_{\mathrm{AB}}^{*}} = \mathbf{h}_{\mathrm{AE}}^{T}\mathbf{R}_{\mathrm{S}}\mathbf{h}_{\mathrm{AE}}^{*} \tag{68}$$

where the dependence on Eve's angle is now implicit. This equation can be satisfied with the choice

$$\mathbf{R}_{\mathrm{S}} = \frac{\mathbf{R}\mathbf{h}_{\mathrm{AB}}^{*}\mathbf{h}_{\mathrm{AB}}^{T}\mathbf{R}}{\mathbf{h}_{\mathrm{AB}}^{T}\mathbf{R}\mathbf{h}_{\mathrm{AB}}^{*}}. \tag{69}$$

The transmit signal vector that produces this rank-1 matrix is

$$\mathbf{w}_{\mathrm{S}} = \frac{\mathbf{R}\mathbf{h}_{\mathrm{AB}}^{*}}{\sqrt{\mathbf{h}_{\mathrm{AB}}^{T}\mathbf{R}\mathbf{h}_{\mathrm{AB}}^{*}}}s = \mathbf{w}_{\mathrm{S0}}s \tag{70}$$

where s follows a unit-variance complex Gaussian distribution.

Given this development, the noise covariance is constructed from $\mathbf{R}_{\mathrm{N}} = \mathbf{R} - \mathbf{R}_{\mathrm{S}}$. If we compute the eigenvalue decomposition $\mathbf{R}_{\mathrm{N}} = \mathbf{U}_{\mathrm{N}}\mathbf{\Sigma}_{\mathrm{N}}\mathbf{U}_{\mathrm{N}}^{H}$, we can form the transmitted noise vector from

$$\mathbf{w}_{\mathrm{N}} = \sum_{n=1}^{N} \mathbf{u}_{\mathrm{N},n} z_n \tag{71}$$

where $\mathbf{u}_{\mathrm{N},n}$ is the nth column of $\mathbf{U}_{\mathrm{N}}$ and the scalar z_n follows a complex Gaussian distribution with variance $\Sigma_{\mathrm{N},ii}$ (ith diagonal element of $\mathbf{\Sigma}_{\mathrm{N}}$). The transmission achieving optimal security is then given as $\mathbf{w} = \mathbf{w}_{\mathrm{S}} + \mathbf{w}_{\mathrm{N}}$.

Now that we have practical weights to separately generate signal and noise, we may replace the Gaussian random variable s in (70) with an information-bearing signal that employs standard modulation. Although it is expected that the same weight vector $\mathbf{w}_{\mathrm{S0}}$ obtained assuming Gaussian signaling will also give good performance for practical modulation, the resulting performance is strictly suboptimal. An optimal solution for non-Gaussian signaling requires a reformulation of the secure array synthesis problem using capacity or key rate expressions appropriate for that modulation.

For wideband operation, one possible practical solution is to apply the weights that are optimal at the center frequency to all frequency bins, although this approach will be decreasingly optimal as the bandwidth increases. Although not detailed here, an alternative approach is to extend the SDP solution by modifying the max–min problem, where minimum security with respect to ϕ_{E} and frequency is maximized with respect to a single $\mathbf{R}$ (and therefore weights) used at all frequencies.

C. Suboptimal Synthesis for Uniform Linear Arrays (ULAs)

The concept of signal and noise patterns suggests a simple but suboptimal array synthesis approach for achieving security. Specifically, for a ULA, we compute the Dolph–Chebyshev beam weights $\hat{\mathbf{w}}_{\mathrm{S0}}$ that place maximum gain in the direction of Bob (angle ϕ_{B}) for a specified sidelobe level L_{SL}. We then compute the singular value decomposition of $\hat{\mathbf{w}}_{\mathrm{S0}}$ as

$$\hat{\mathbf{w}}_{\mathrm{S0}} = \mathbf{U}\mathbf{\Lambda}\mathbf{V}^{H} = [\mathbf{u}_1\mathbf{U}_0]\begin{bmatrix}\lambda_1 & 0\\ 0 & \mathbf{0}\end{bmatrix}\begin{bmatrix}\mathbf{v}_1^{H}\\ \mathbf{V}_0^{H}\end{bmatrix} \tag{72}$$

where $\mathbf{u}_1$ is a unit-length version of the vector $\hat{\mathbf{w}}_{\mathrm{S0}}$ and the matrix $\mathbf{U}_0$ consists of unit-length, mutually orthogonal column vectors that are orthogonal to $\mathbf{u}_1$. Based on our discussion in Section IV-B, we use a scaled version of $\mathbf{u}_1$ for the signal transmission and a weighted sum of the vectors in $\mathbf{U}_0$ for the noise transmission.

Let ζ and $\bar{\zeta}$ represent the fraction of transmit power devoted to the signal vector and the fraction of power devoted to each noise vector, respectively, so that $\bar{\zeta} = (1-\zeta)/(N_{\mathrm{T}}-1)$. The covariance of the transmit signals is then given by

$$\mathbf{R}' = \mathbf{U}\mathbf{\Sigma}'\mathbf{U}^{H} \tag{73}$$

where $\mathbf{\Sigma}' = \mathrm{diag}\left(\left[\zeta,\ \bar{\zeta},\ \bar{\zeta},\ldots,\bar{\zeta}\right]\right)$. Finally, we scale $\mathbf{R}'$ to ensure satisfaction of the transmit power constraint using

$$\mathbf{R} = \mathbf{R}'/\mathrm{Tr}(\mathbf{A}\mathbf{R}'). \tag{74}$$

Using this form of the covariance $\mathbf{R}$, α in (29) can be computed as a function of L_{SL} and ζ. A brute-force search on $\zeta \in [0,1]$ and $L_{\mathrm{SL}} \in [0,20]$ dB is used to determine the values of ζ and L_{SL} that maximize the minimum value of α for all values of ϕ_{E} outside the exclusion sector.

V. Numerical Examples

This section illustrates application of the secure array synthesis method to some practical examples. While we use a ULA and a uniform circular array (UCA) of idealized patch antennas for these examples, the method is general and can be used for any array topology. Note that ideal omnidirectional radiators are assumed at Bob and Eve. If Bob's antenna gain is changed, this changes the value of the achieved security metric, but does not change the optimizing weights. On the other hand, changing the antenna gain at Eve has no effect on the results since she is assumed to have infinite SNR. The interelement spacing for all cases is assumed to be $\lambda/2$, where λ is the free-space wavelength.

Since both I_{SK} and C_{S} are monotonic with α, we only consider I_{SK} in our analysis. Simulations are performed by varying the exclusion sector (ϕ_{X}), location of Bob (ϕ_{B}) and Eve (ϕ_{E}), and the number of transmit antennas at Alice (N_{T}). In all simulations, angles for Eve outside of the exclusion sector are sampled uniformly in 1° increments on $\phi_{\mathrm{E}} \in [0,\phi_1] \cup [\phi_2, 180°]$ for the ULA and $\phi_{\mathrm{E}} \in [0,\phi_1] \cup [\phi_2, 360°]$ for the UCA. The element pattern used for the patches is

$$g(\phi) = \frac{2\sin\left[(k_0 h/2)\sin\phi\right]}{k_0 h \sin\phi}\cos\left(\frac{k_0 L}{2}\cos\phi\right) \tag{75}$$

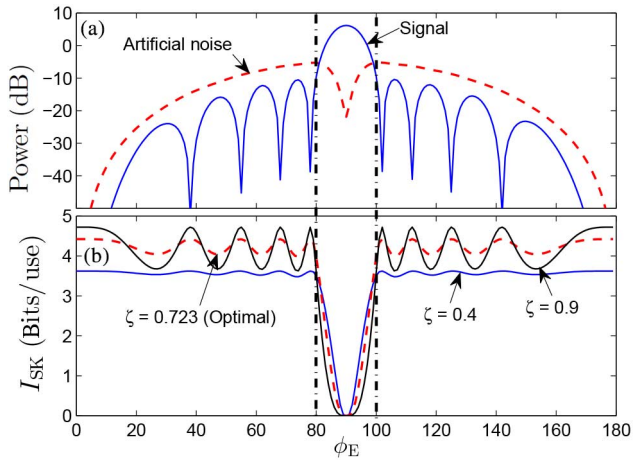

Fig. 4. Suboptimal method for secure array synthesis employing a ULA with $N_T = 10$, $\phi_B = 90°$, and $\phi_X = 20°$. (a) Power allocation to signal and noise patterns. (b) Achieved I_{SK} performance for different power allocations.

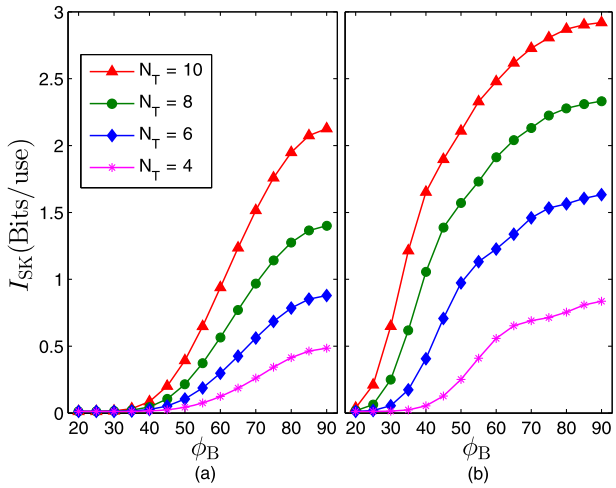

Fig. 5. Performance of the (a) suboptimal and (b) optimal methods for a ULA at Alice with $\phi_X = 10°$. Performance is shown with respect to the number of antennas at Alice (N_T) and the transmit angle to Bob (ϕ_B).

where $h = 0.003\lambda$ and $L = 0.5\lambda$, and the direction of maximum radiation is $\phi = 90°$. The single-antenna SNR of the Alice–Bob link is set to 10 dB by assuming unit transmit power ($P_T = 1$), setting $\sigma_0^2 = 0.1$, and normalizing the patch gain to a maximum of 0 dB.

A. *Uniform Linear Array*

We first apply the suboptimal procedure to a ten-element ULA at Alice with Bob at $\phi_B = 90°$ (broadside to the ULA) and an exclusion sector around Bob of $\phi_X = 20°$. The brute-force search produces $\zeta = 0.723$ and $L_{SL} = 15.6$ dB for this scenario. Fig. 4(a) plots the signal (Dolph–Chebyshev) pattern scaled by the signal power fraction ζ as well as the linear combination of the equally weighted noise patterns for the optimal parameter values. As expected, Bob observes more signal than noise, while an eavesdropper outside of the exclusion sector observes more noise than signal. Note that although the signal pattern array factor has equal sidelobes, the overall signal and noise patterns are shaped by the patch element pattern. Fig. 4(b), which plots I_{SK} for different values of ζ, demonstrates how the optimal value of $\zeta = 0.723$ maximizes the minimum value of I_{SK}.

Fig. 5(a) and (b) plots the performance achieved using the suboptimal and optimal approaches, respectively, as a function of Bob's angle ϕ_B ranging from near-array endfire ($\phi_B = 0°$) to broadside ($\phi_B = 90°$) for an exclusion sector of $\phi_X = 10°$ and different values of N_T. The results for the suboptimal technique show that the worst-case value of I_{SK} is reduced significantly when either Bob moves toward the endfire direction or the size of Alice's array is reduced because of the inferior beamforming capabilities of the ULA under these conditions. While similar trends appear in the results for the optimal solution, the secure array beamforming technique provides performance gains of nearly 50% for the smallest array when Bob is close to the broadside direction. Furthermore, the optimal beamforming technique maintains higher values of I_{SK} as Bob moves toward endfire.

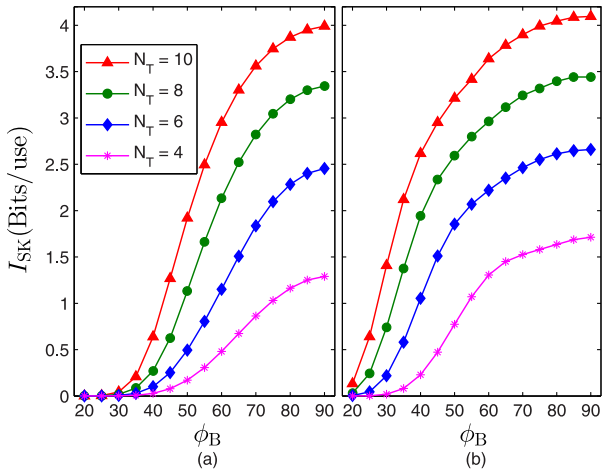

Fig. 6. Achieved I_{SK} for a varying number of antennas in Alice's ULA and different transmit angles to Bob for $\phi_X = 20°$. (a) Suboptimal solution. (b) Optimal solution.

Fig. 6 repeats the analysis of Fig. 5 for a larger exclusion sector of $\phi_X = 20°$. In this case, the performance of the suboptimal and optimal solutions is similar for large array sizes when Bob is at array broadside. However, as Bob moves toward array endfire, I_{SK} falls more rapidly for the suboptimal than for the optimal method. This highlights the fact that the secure array synthesis approach has the potential to offer significant performance gains over heuristic methods in a dynamic system where Bob's position is variable.

It is instructive to use the signal/noise pattern analysis developed in Section IV to further understand the behavior of the two solutions. Fig. 7(a) and (b) plots the number of secure key bits, signal power, and noise power as a function of Eve's angle ϕ_E for the suboptimal and optimal solutions, respectively, for $N_T = 10$, $\phi_X = 10°$, and $\phi_B = 90°$. The straight horizontal line in each plot shows the minimum value of I_{SK} obtained outside of the exclusion sector. At Bob's position, both solutions place a peak in the signal power and null in the noise power as

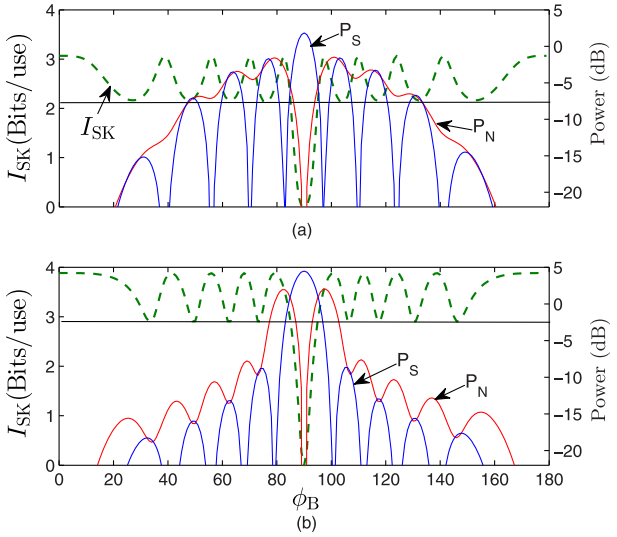

Fig. 7. Comparison of radiated signal (P_S) and noise (P_N) for the (a) suboptimal and (b) optimal approaches for a ULA at Alice with $N_T = 10$ elements, $\phi_X = 10°$, and $\phi_B = 90°$. The horizontal line is the minimum I_{SK} outside of the exclusion sector.

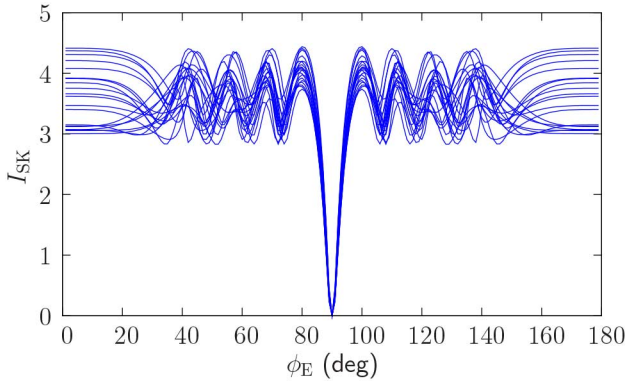

Fig. 8. Effect of nonequal gain on I_{SK} obtained with secure array synthesis. The gains of Alice's antennas are randomly varied from -3 to 3 dB for each of 20 realizations.

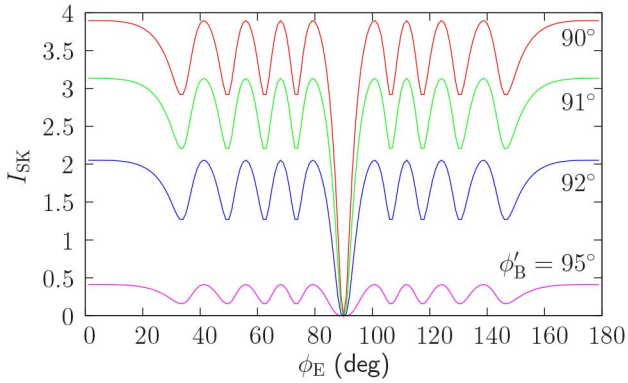

Fig. 9. Effect of error in the relative Alice–Bob angle on I_{SK} for assumed angle $\phi_B = 90°$ and actual angles of $\phi'_B = \{90°, 91°, 92°, 95°\}$.

expected, leading to compromised security if Eve moves inside the exclusion sector.

Outside of the exclusion sector, we see that a null in P_S corresponds to a peak in I_{SK}, which is intuitive since no signal power reaches Eve for these angles. Conversely, a minimum value in I_{SK} coincides with the peak of each sidelobe in P_S, with the noise pattern P_N placing sufficient noise power at these points to keep I_{SK} at or above the minimum value (horizontal line). We observe that compared to the optimal synthesis, the suboptimal synthesis directs more signal energy outside of the exclusion sector, resulting in a smaller minimum value of I_{SK}. Furthermore, the optimal method achieves an exact equal ripple response (the minima of I_{SK} touch the I_{SK} lower threshold), whereas the suboptimal approach only approximately achieves this condition.

As explained previously, antenna gain at Bob and Eve plays a minor role in the synthesis, although unequal gains across Alice's array may lead to reduced performance. To study this degradation, we vary Alice's element gains randomly with a uniform distribution on $[-3, 3]$ dB, but we assume that the realized gain values are known during the optimization. Fig. 8 shows I_{SK} for each of 20 realizations, with the results indicating that the method compensates for gain differences and achieves nearly the same minimum I_{SK} [which is the same as the minimum I_{SK} for the ideal case shown in Fig. 7(b)] for all cases.

The secure array synthesis problem was posed assuming that Bob and Alice know their relative angle exactly, and the solution places a null in the noise pattern and a peak in the signal pattern in that direction. Any error in estimating that angle will lead to leakage of synthetic noise and reduced power to the legitimate node and therefore reduced SNR. This degradation can be characterized by first computing the optimal signaling and resulting signal and noise patterns assuming a relative Alice–Bob angle of ϕ_B, and then extending the expression in (65) to

$$\alpha(\mathbf{R}, \phi_E, \phi'_B) = \frac{\mathrm{SNR}'_{\mathrm{Bob}}}{1 + \mathrm{SNR}_{\mathrm{Eve}}} \tag{76}$$

$$= \frac{P_S(\phi'_B)}{\sigma_0^2 + P_N(\phi'_B)} \left[1 + \frac{P_S(\phi_E)}{P_N(\phi_E)}\right]^{-1} \tag{77}$$

where ϕ'_B is the actual Alice–Bob angle. Notice that if $\phi_B = \phi'_B$, the expression reduces to (65).

Fig. 9 plots I_{SK} using (77) for the ULA case considered previously with $N_T = 10$, $\phi_X = 10°$, and $\phi_B = 90°$ for $\phi'_B = \{90°, 91°, 92°, 95°\}$. The results indicate that the performance degradation is sensitive to the error, with moderate degradation for errors that are a small fraction of the exclusion sector.

B. Uniform Circular Array

To demonstrate that secure array synthesis can be applied to any array topology, we demonstrate its application to a UCA. Since the suboptimal approach is based on Dolph–Chebyshev synthesis for a ULA, it is not considered here.

Fig. 10 plots the average achieved minimum value of I_{SK} as a function of N_T for different values of ϕ_X, where the average is taken over $\phi_B \in [90°, 180°]$ with a step size of 1°. As expected, I_{SK} increases with the number of antennas and the

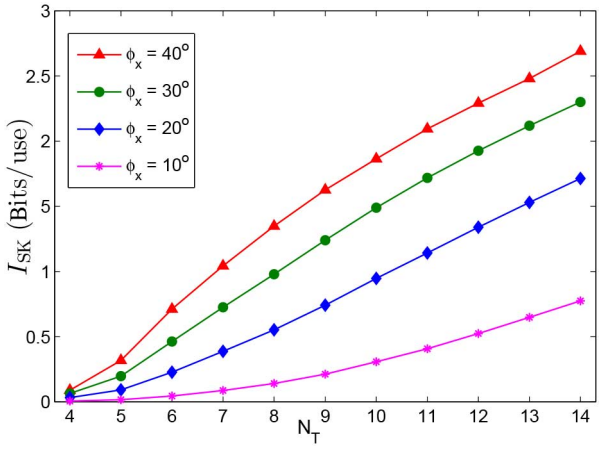

Fig. 10. I_{SK} for a UCA at Alice as the size of the exclusion sector and the number of antennas at Alice are varied.

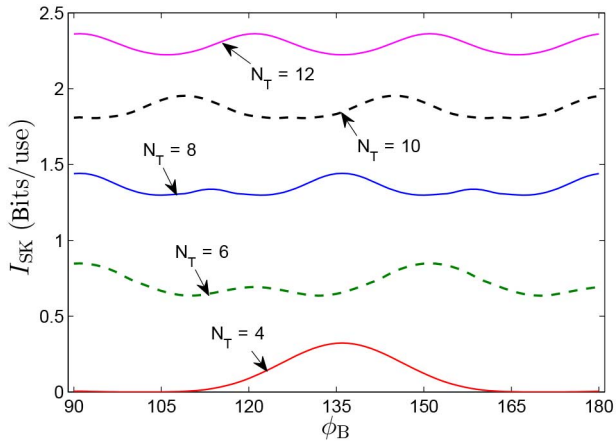

Fig. 11. I_{SK} for a varying number of antennas in Alice's UCA and different transmit directions to Bob for $\phi_X = 40°$.

exclusion sector angle. Fig. 11 plots I_{SK} as a function of Bob's location for $\phi_X = 40°$ and several values of N_T. These results show that the relative variation with ϕ_B is significant for small arrays and less significant as N_T increases. Finally, Fig. 12 analyzes the optimal solution using signal and noise patterns. Although the I_{SK} ripple with angle is less regular for the UCA than for the ULA, the synthesized array still ensures that I_{SK} remains above a minimum value. Within the exclusion sector, the behavior of the signal and noise patterns follow the trends previously observed for the ULA.

C. Computational Complexity of SDP Optimization

SDP is a powerful but computationally complex optimization technique. While the secure array synthesis problem proposed here can naturally be extended to large arrays, wideband operation, and 3-D radiation, such extensions increase the size of the optimization. We explore the issue of complexity by examining the SDP (MAXDET) run time for secure array synthesis with an exclusion sector of 10° with ULAs consisting of 5, 10, or 20 antennas and for the sampling of Eve's position ranging between 50 and 1000 angles. Fig. 13 plots the result when

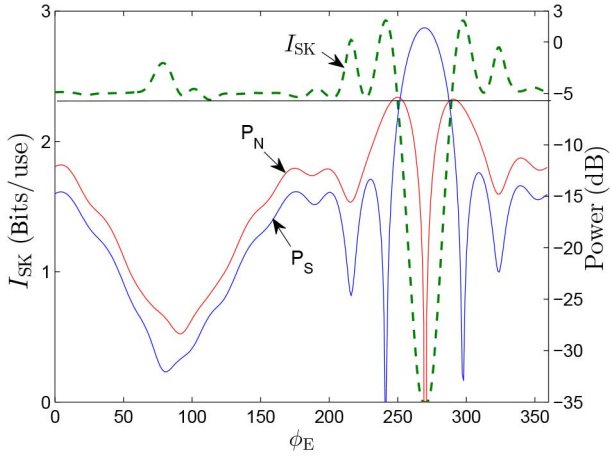

Fig. 12. I_{SK}, P_S, and P_N with respect to Eve's location for a UCA at Alice with $N_T = 12$ elements, $\phi_X = 40°$, and $\phi_B = 270°$.

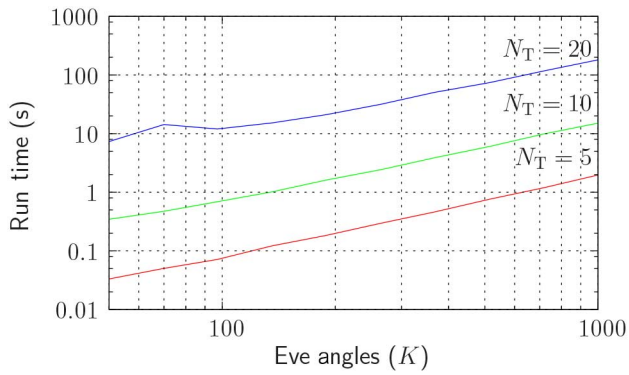

Fig. 13. Run time for SDP (MAXDET) solution of secure array synthesis for various array sizes at Alice and number of quantized Eve angles.

the single-threaded code is run on a 3.6-GHz Intel i7 processor with 32 GB of RAM (usage remained below 1 GB for all cases). Although run time increases moderately with the number of constraints (Eve angles), it increases quite dramatically with the number of antennas. This is partially due to the number of SDP unknowns increasing quadratically with the number of antennas ($M = N_T^2 + 1$), which for 5, 10, and 20 antennas gives 26, 101, and 401 unknowns, respectively. This suggests that more efficient optimization methods are needed to extend secure array synthesis to wideband or large arrays.

VI. Conclusion

This paper poses the problem of secure array synthesis that maximizes the information transmitted to a desired location while minimizing the information leaked to an eavesdropper at all possible locations outside a specified exclusion sector. Whereas traditional array synthesis focuses on a single pattern, secure array synthesis involves joint optimization of two radiation patterns: one that transmits useful signal and another that transmits artificial noise. The synthesis problem is solved by casting the problem into a form suitable for existing SDP solvers.

This paper also formulates a simple yet suboptimal pattern synthesis approach that creates a Dolph–Chebyshev pattern for

the signal and transmits noise on the orthogonal complement to the signal pattern. Numerical examples for a ULA reveal that although in some cases, the performance of the suboptimal approach is similar to that achieved with the optimal secure array synthesis, in other cases, the performance of the suboptimal approach is dramatically inferior. Application of the method to a UCA demonstrates the generality of the secure array synthesis approach.

REFERENCES

[1] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[2] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[3] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, 2008, pp. 3013–3016.

[4] W. Tzu-Han Chou, S. C. Draper, and A. M. Sayeed, "Secret key generation from sparse wireless channels: Ergodic capacity and secrecy outage," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1751–1764, Sep. 2013.

[5] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6, Jan. 1995.

[6] T. Aono, K. Higuchi, M. Taromaru, T. Ohira, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.

[7] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.

[8] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 381–392, Sep. 2010.

[9] R. Mehmood, J. Wallace, and M. Jensen, "Key establishment employing reconfigurable antennas: Impact of antenna complexity," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6300–6310, Nov. 2014.

[10] G. Zheng, P. Arapoglou, and B. Ottersten, "Physical layer security in multibeam satellite systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 852–863, Feb. 2012.

[11] W. Saad, X. Zhou, Z. Han, and H. V. Poor, "On the physical layer security of backscatter wireless systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3442–3451, Jun. 2014.

[12] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun. Mag.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[13] C. A. Balanis, *Antenna Theory: Analysis and Design*. Hoboken, NJ, USA: Wiley, 1997.

[14] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[15] X. Zhou and M. R. McKay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation," in *Proc. IEEE Int. Conf. Signal Process. Commun. Syst.*, 2009, pp. 1–5.

[16] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Physical layer security of MIMO–OFDM systems by beamforming and artificial noise generation," *Phys. Commun.*, vol. 4, no. 4, pp. 313–321, Dec. 2011.

[17] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[18] L. Vandenberghe and S. Boyd, "Semidefinite programming," *SIAM Rev.*, vol. 38, no. 1, pp. 49–95, Mar. 1996.

[19] J. W. Wallace and M. A. Jensen, "Mutual coupling in MIMO wireless systems: A rigorous network theory analysis," *IEEE Trans. Wireless Commun.*, vol. 3, no. 4, pp. 1317–1325, Jul. 2004.

[20] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, Feb. 2011.

[21] L. Vandenberghe, S. Boyd, and S.-P. Wu, "Determinant maximization with linear matrix inequality constraints," *SIAM J. Matrix Anal. Appl.*, vol. 19, no. 2, pp. 499–533, 1998.

Rashid Mehmood (S'05) received the B.Sc. (*cum laude*) degree in communication systems engineering from the Institute of Space Technology (IST), Islamabad, Pakistan, in 2007, the M.Sc. degree in electrical engineering from Jacobs University Bremen (JUB), Bremen, Germany, 2010, and the Ph.D. degree in electrical engineering from Brigham Young University, Provo, UT, USA, in 2015.

Currently, he is a Research Associate with Wavetronix, LLC, Provo, UT, USA. His research interests include reconfigurable antennas, optimization techniques, physical layer security, and wireless communications.

Dr. Mehmood was a recipient of the IEEE AP-S Undergraduate Research Award in 2009 and the Brigham Young University High Impact Doctoral Research Assistantship Award in 2012.

Jon W. Wallace (S'99–M'03–SM'13) received the B.S. (*summa cum laude*) and Ph.D. degrees in electrical engineering from Brigham Young University (BYU), Provo, UT, USA, in 1997 and 2002, respectively.

From 2006 to 2013, he was with Jacobs University, Bremen, Germany, and from 2013 to 2014, Wavetronix, LLC, Provo, UT, USA. Since 2014, he has been with the Department of Electrical and Computer Engineering, Lafayette College, Easton, PA, USA. His research interests include physical layer security, MIMO communications and radar, and reconfigurable antennas.

Dr. Wallace has served as an Associate Editor of the IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION and the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He was a recipient of the National Science Foundation Graduate Fellowship in 1998. In 2002, he received the Harold A. Wheeler Applications Prize Paper Award in the IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION.

Michael A. Jensen (S'93–M'95–SM'01–F'08) received the B.S. and M.S. degrees from Brigham Young University (BYU), Provo, UT, USA, in 1990 and 1991, respectively, and the Ph.D. degree from the University of California, Los Angeles, in 1994, all in electrical engineering.

Since 1994, he has been with the Electrical and Computer Engineering Department, BYU, where he is currently a University Professor. His research interests include antennas and propagation for communications, microwave circuit design, multiantenna signal processing, and physical layer security.

Dr. Jensen is currently the President-Elect of the IEEE Antennas and Propagation Society. He was previously the Editor-in-Chief of the IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION, as well as an Associate Editor for the same journal and for the *IEEE Antennas and Wireless Propagation Letters*. He has been a member and Chair of the Joint Meetings Committee for the IEEE Antennas and Propagation Society, a member of the society AdCom, a member of the society Publications Committee, and Co-Chair or Technical Program Chair for six society-sponsored symposia. He was the recipient of the Harold A. Wheeler Applications Prize Paper Award in the IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION in 2002.