Secure Array Synthesis in Multipath Channels

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

***Abstract*—While conventional antenna array synthesis determines the beamforming weights that create a specified antenna radiation pattern, secure array synthesis formulates the beamforming weights that enhance security for wireless transmission of sensitive data. This paper focuses on creating beamformers that improve the generation of secret encryption keys based on bidirectional estimation of the reciprocal electromagnetic propagation channel between two radios. The technique uses semidefinite programming to determine the array weights that maximize the average secure key rate under a constraint on the total transmit power. The numerical implementation of the technique incorporates array mutual coupling, and the results demonstrate that the technique outperforms a conventional beamforming solution, with the improvement becoming significant for certain channel correlation conditions.**

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

I. Introduction

SECURING sensitive data transmitted over wireless links is an essential aspect of modern radio systems, with privacy typically addressed through encryption of binary data using secret keys. While these encryption keys are generally established through secure exchange protocols, recent research has identified physical layer [1] key establishment protocols based on the observations of the reciprocal propagation channel that recently have gained increased attention [2]–[6].

Implementing multiantenna transmission for channel-based key establishment requires a technique for determining the beamforming vectors that enhance privacy from potential eavesdroppers. We measure the effectiveness of such techniques by the information theoretic *key rate*, which is the maximum number of key bits that can be established from a single observation of the reciprocal propagation channel, and the *secure key rate*, which is the number of those bits that are secure from an eavesdropper. Past work has formulated methods for constructing beamformers that maximize the key rate for arbitrary channel propagation conditions [7]–[9], but these methods do not consider the information made available to an eavesdropper. We have developed an array synthesis method to optimize the secure key rate in line-of-sight (LOS) propagation conditions, where the eavesdropper locations are known to lie at least a certain angular distance away from the legitimate radio [10], but the technique is not applicable to communication over multipath channels. Without the development of a technique for constructing the array weights that maximize the secure key rate in multipath propagation channels typical of most mobile communication environments, this concept of propagation channel-based key establishment has limited practical application.

Motivated by these observations, we extend our prior work on secure array synthesis for key establishment [10] to multipath environments. To accomplish this, we express the secure key rate in terms of: 1) the correlation between the channel observed at the legitimate receiver and the channel observed at the eavesdropper and 2) the covariance matrix of the multiantenna signal that excites the transmit array. We then use semidefinite programming (SDP) [11] to determine the transmit signal covariance matrix that maximizes this secure key rate under a constraint on the total transmitted power. This covariance is decomposed to identify the array beamforming weights that should be applied during key establishment. The technique can accommodate practical antenna considerations such as array mutual coupling. Simulation results demonstrate that the secure key rate achieved with the method significantly outperforms that obtained using beamformers constructed from a conventional approach for multipath channels that have medium to high levels of spatial correlation. While preliminary versions of the ideas and results contained in this paper have appeared recently [12], [13], the initial papers contain very limited explanations of the technique, only a single representative simulation of achievable performance, and no inclusion of electromagnetic coupling effects in the antenna arrays. This paper therefore provides the additional detail required to fully explain the concepts, develop the algorithms, and demonstrate the achievable performance.

II. Beamformer Covariance Optimization

A. System Model

Fig. 1 shows legitimate radios Alice and Bob participating in secure communication with the passive eavesdropper Eve attempting to intercept their transmissions. We assume that Alice has an array of N_{A} antennas while Bob and Eve each have a single antenna. The $N_{\mathrm{A}} \times 1$ vectors $\mathbf{h}_{\mathrm{AB}}$, $\mathbf{h}_{\mathrm{BA}}$, and $\mathbf{h}_{\mathrm{AE}}$ represent the complex baseband transfer functions from each element of Alice's array to Bob's antenna, from Bob's antenna to each element of Alice's array, and from each element of

Manuscript received January 26, 2017; revised January 31, 2018; accepted April 6, 2018. Date of publication April 24, 2018; date of current version July 3, 2018. *(Corresponding author: Michael A. Jensen.)*

R. Mehmood was with the Electrical and Computer Engineering Department, Brigham Young University, Provo, UT 84602 USA. He is now with the Research Department, Wavetronix, Provo, UT 84606 USA (e-mail: r.mehmood@ieee.org).

J. W. Wallace is with the Electrical and Computer Engineering Department, Lafayette College, Easton, PA 18042 USA (e-mail: wall@ieee.org).

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

Digital Object Identifier 10.1109/TAP.2018.2829838

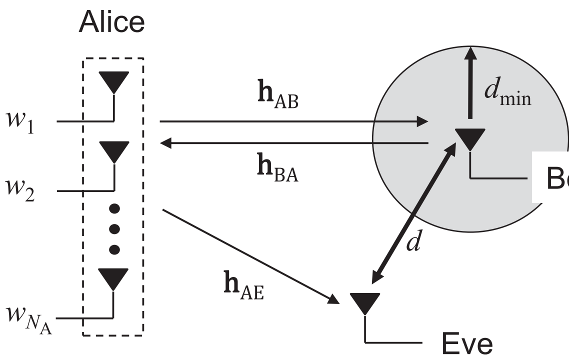


Fig. 1. System diagram where Alice's antenna array transmits to Bob's single antenna in the presence of a passive single-antenna eavesdropper Eve. The antenna separation d between Bob and Eve is constrained such that $d \geq d_{\min}$.

Alice's array to Eve's antenna, respectively. While Fig. 1 shows Alice with a uniform linear array (ULA), she may have any arbitrary array topology. We further assume that Eve is close to Bob—so that the vector channel $\mathbf{h}_{AE}$ from Alice to Eve is correlated with the channel $\mathbf{h}_{AB}$ from Alice to Bob—but that physical or other constraints ensure that the antenna separation d between Bob and Eve is at least $d_{\min}$.

Our specific focus is on secret key generation from reciprocal channel estimates [1]–[3]. In this technique, Alice transmits training data to Bob from which Bob estimates the vector of channel transfer functions from Alice's N_A antennas to Bob's single antenna. Similarly, Bob transmits training data to Alice, from which Alice can estimate the vector of transfer functions. Assuming all antennas and the propagation medium are reciprocal and in the absence of channel estimation errors, Alice's channel estimates will be identical to those of Bob. Therefore, Alice and Bob can quantize their respective estimates to form encryption keys that will match without transmitting any information about the formed key.

During this exchange, Eve will observe different channel estimates as long as her antenna is displaced from Bob's. However, if Eve's and Bob's channel estimates are correlated, Eve has information to help her determine the established key. Correlation between the elements of $\mathbf{h}_{AB}$ and $\mathbf{h}_{AE}$ is a function of time, frequency, and distance between the two channel observations [14], [15]. However, $\mathbf{h}_{AB}$ and $\mathbf{h}_{AE}$ are estimated at the same time and frequency, and we therefore are concerned only with the correlation as a function of the distance d. The physical constraint that Eve's antenna is displaced from Bob's antenna by at least $d_{\min}$ limits the maximum correlation observed between elements of the channels $\mathbf{h}_{AB}$ and $\mathbf{h}_{AE}$. If $d_{\min} = 0$ so that Bob's and Eve's antennas are essentially colocated, then the approach considered in this paper cannot offer any significant level of security.

Given this scenario, our objective is to find Alice's array signaling strategy that maximizes the ability for Alice and Bob to generate a secret key from their channel estimates while minimizing Eve's ability to obtain information that will allow her to more easily determine that key. We represent the complex baseband vector that is transmitted from Alice's array to produce scalar signals at Bob and Eve as $\mathbf{w}$. We assume that $\mathbf{w}$ is formed as a linear combination of beamforming vectors weighted by zero-mean complex Gaussian random variables so that the transmit vector statistics are completely specified by the covariance $\mathbf{R} = \mathrm{E}\left\{\mathbf{w}\mathbf{w}^\dagger\right\}$, where $\{\cdot\}^\dagger$ and $\mathrm{E}\{\cdot\}$ indicate conjugate transpose and expectation, respectively. We constrain $\mathbf{R}$ to limit the power transmitted, or $\mathrm{Tr}(\mathbf{AR}) \leq P_T$, where $\mathrm{Tr}(\cdot)$ is a trace, $\mathbf{A}$ is a coupling matrix [16], and P_T is the available transmit power.

Note that while Bob and Eve have single antennas in our scenario, these antennas may represent arrays that can be used to enhance the gain of the link and therefore the observed signal-to-noise ratio (SNR). However, as our objective is array beamforming synthesis, we do not consider multiple-stream (multiple-input multiple-output) communication. Therefore, any SNR enhancement created by antenna arrays at Bob or Eve can be accommodated in the technique by specifying the realized gain values in the multiantenna channel vectors.

B. Optimization Criterion

Beamforming allows Alice to transmit a training signal to Bob on one radiation pattern while transmitting artificial noise on patterns that are orthogonal to that used for the training transmission in order to reduce the effective SNR at Eve, creating more error in her estimate of $\mathbf{h}_{AE}$ and reducing the information she has about the established key. The transmit vector $\mathbf{w}$ represents the composite signal and noise transmission. The performance of the key establishment based on the obtained channel estimates in the presence of Eve is measured by the *secure key rate* I_{SK}. Qualitatively, I_{SK} indicates the maximum number of bits that Alice and Bob can generate when Alice observes $\mathbf{h}_{BA}$ and Bob observes $\mathbf{h}_{AB}$ that Eve is unable to guess based on her observation of $\mathbf{h}_{AE}$. It is large when $\mathbf{h}_{BA}$ and $\mathbf{h}_{AB}$ are highly similar and reduced if $\mathbf{h}_{AE}$ is similar to $\mathbf{h}_{AB}$ and $\mathbf{h}_{BA}$. The mathematical form of I_{SK} depends on the application, but for our problem is shown in [10] to assume the form

$$I_{SK} = \max_{\mathbf{R}\,:\,\mathrm{Tr}(\mathbf{AR})\leq P_T} \log_2 \frac{[1+\alpha(\mathbf{R})]^2}{1+2\alpha(\mathbf{R})} \tag{1}$$

$$\alpha(\mathbf{R}) = \frac{\sigma_B^2}{\sigma_0^2}\left(1 - \frac{|\sigma_{BE}|^2}{\sigma_B^2\sigma_E^2}\right) \tag{2}$$

$$\sigma_\xi^2 = \mathbf{h}_{A\xi}^T \mathbf{R} \mathbf{h}_{A\xi}^* \quad (\xi \in [\mathrm{B}, \mathrm{E}]) \tag{3}$$

$$\sigma_{BE} = \mathbf{h}_{AB}^T \mathbf{R} \mathbf{h}_{AE}^*, \tag{4}$$

where σ_0^2 is the channel estimation error variance and $\{\cdot\}^T$ and $\{\cdot\}^*$ indicate transpose and conjugate, respectively.

We see from (1) that I_{SK} depends monotonically on $\alpha(\mathbf{R})$, and therefore optimization of I_{SK} can be accomplished by determining the covariance $\mathbf{R}$ that maximizes $\alpha(\mathbf{R})$ given Alice's observation of $\mathbf{h}_{AB}$. In an LOS scenario, Alice knows the channel $\mathbf{h}_{AE}$ as a function of Eve's angular position and therefore can optimize the beamforming to maximize the minimum value of $\alpha(\mathbf{R})$ realized over all of Eve's possible angular positions [10]. In contrast, in a multipath channel, Alice can only know the statistical *correlation* between the known channel $\mathbf{h}_{AB}$ to Bob and unknown channel $\mathbf{h}_{AE}$ to Eve as a function of the distance d, meaning that σ_{E}^2, σ_{BE}, and α are random variables in the optimization.

These observations suggest using a statistical measure of performance, such as the average secure key rate, as the optimization cost function. We can estimate the expectation of (1) from a sample mean of a large ensemble of random realizations of $\mathbf{h}_{\mathrm{AE}}$ for each cost function evaluation. But recognizing that (1) is monotonic in $\alpha(\mathbf{R})$, we simplify the optimization by instead using the *average* value of $\alpha(\mathbf{R})$ as our cost function, with the average approximated by taking the ratio of the expectations of the numerator and denominator of (2). The resulting average value of $\alpha(\mathbf{R})$ is defined as

$$\alpha_{\mathrm{avg}} = \frac{\sigma_{\mathrm{B}}^2 \mathrm{E}\{\sigma_{\mathrm{E}}^2\} - \mathrm{E}\{|\sigma_{\mathrm{BE}}|^2\}}{\mathrm{E}\{\sigma_{\mathrm{E}}^2\}\sigma_0^2} \tag{5}$$

where $\mathrm{E}\left\{\sigma_{\mathrm{E}}^2\right\} = \mathrm{Tr}(\mathbf{R}\mathbf{R}_{\mathrm{E}}^*)$, $\mathrm{E}\left\{|\sigma_{\mathrm{BE}}|^2\right\} = \mathbf{h}_{\mathrm{AB}}^{\mathrm{T}}\mathbf{R}\mathbf{R}_{\mathrm{E}}^*\mathbf{R}\mathbf{h}_{\mathrm{AB}}^*$, and $\mathbf{R}_{\mathrm{E}} = \mathrm{E}\left\{\mathbf{h}_{\mathrm{AE}}\mathbf{h}_{\mathrm{AE}}^{\dagger}\right\}$. Since α_{avg} depends on Eve's position, we find the value of $\mathbf{R}$ that maximizes the minimum value of α_{avg} over all of Eve's possible locations that satisfy $d \geq d_{\min}$. Because this requires Alice to know $\mathbf{R}_{\mathrm{E}}$ as a function of d conditioned on her observation of $\mathbf{h}_{\mathrm{AB}}$, we specifically discuss the construction of $\mathbf{R}_{\mathrm{E}}$ in Section II-C.

Substituting α_{avg} for the instantaneous value $\alpha(\mathbf{R})$ when evaluating (1) is a common approximation in mutual information evaluation [17], [18], and through Jensen's inequality, the resulting expression represents an upper bound to the average mutual information [17]. The additional approximation in (5) of taking the expectation of the numerator and denominator separately has been used successfully in similar studies of mutual information [18]. What is most important about these approximations, however, is whether or not maximizing the approximation leads to an approximate maximization of the actual average key rate. The results presented in Section IV demonstrate strong performance of the optimization, suggesting that the approach is reasonable.

C. Channel Covariance Computation

To implement an optimization of α_{avg}, Alice must first construct the correlation matrix $\mathbf{R}_{\mathrm{E}}$ for each possible value of d and her observed channel vector $\mathbf{h}_{\mathrm{AB}}$, which requires that she determine the statistics of $\mathbf{h}_{\mathrm{AE}}$ conditioned on an observation of $\mathbf{h}_{\mathrm{AB}}$. Let $\boldsymbol{\mu}_{\mathrm{AB}}$ and $\boldsymbol{\mu}_{\mathrm{AE}}$ be the vector mean of the multivariate normal channels $\mathbf{h}_{\mathrm{AB}}$ and $\mathbf{h}_{\mathrm{AE}}$, respectively, and define $\mathbf{h} = [\mathbf{h}_{\mathrm{AB}}^{\mathrm{T}} \;\; \mathbf{h}_{\mathrm{AE}}^{\mathrm{T}}]^{\mathrm{T}}$ and $\boldsymbol{\mu} = [\boldsymbol{\mu}_{\mathrm{AB}}^{\mathrm{T}} \;\; \boldsymbol{\mu}_{\mathrm{AE}}^{\mathrm{T}}]^{\mathrm{T}}$. Using channel estimation, Alice only learns the channel $\mathbf{h}_{\mathrm{AB}}$, but if Bob is mobile or has an array, then Alice can estimate channels for different receiver locations and estimate the covariance for two channels as a function of the distance between receive antennas. Alternatively, this covariance can be estimated based on prior measurements for the environment or based on correlations of common validated channel models [19]. Alice therefore can construct the covariance matrix of $\mathbf{h}$ that can be expressed as

$$\mathbf{C}_{\mathrm{h}} = \mathrm{E}\left\{(\mathbf{h}-\boldsymbol{\mu})(\mathbf{h}-\boldsymbol{\mu})^{\dagger}\right\} = \begin{bmatrix} \mathbf{C}_{\mathrm{B}} & \mathbf{C}_{\mathrm{BE}} \\ \mathbf{C}_{\mathrm{EB}} & \mathbf{C}_{\mathrm{E}} \end{bmatrix} \tag{6}$$

where

$$\mathbf{C}_{\xi} = \mathrm{E}\left\{(\mathbf{h}_{\mathrm{A}\xi}-\boldsymbol{\mu}_{\mathrm{A}\xi})(\mathbf{h}_{\mathrm{A}\xi}-\boldsymbol{\mu}_{\mathrm{A}\xi})^{\dagger}\right\} \tag{7}$$

$$\mathbf{C}_{\mathrm{BE}} = \mathrm{E}\left\{(\mathbf{h}_{\mathrm{AB}}-\boldsymbol{\mu}_{\mathrm{AB}})(\mathbf{h}_{\mathrm{AE}}-\boldsymbol{\mu}_{\mathrm{AE}})^{\dagger}\right\} = \mathbf{C}_{\mathrm{EB}}^{\dagger} \tag{8}$$

for $\xi \in [\mathrm{B}, \mathrm{E}]$. The mean and covariance matrix of the multivariate normal distribution of $\mathbf{h}_{\mathrm{AE}}$ conditioned on a specific observation of $\mathbf{h}_{\mathrm{AB}}$ are then [20]

$$\bar{\boldsymbol{\mu}}_{\mathrm{AE}} = \boldsymbol{\mu}_{\mathrm{AE}} + \mathbf{C}_{\mathrm{EB}}\mathbf{C}_{\mathrm{B}}^{-1}(\mathbf{h}_{\mathrm{AB}}-\boldsymbol{\mu}_{\mathrm{AB}}) \tag{9}$$

$$\bar{\mathbf{C}}_{\mathrm{E}} = \mathbf{C}_{\mathrm{E}} - \mathbf{C}_{\mathrm{EB}}\mathbf{C}_{\mathrm{B}}^{-1}\mathbf{C}_{\mathrm{BE}}. \tag{10}$$

Since $\bar{\mathbf{C}}_{\mathrm{E}} = \mathrm{E}\left\{(\mathbf{h}_{\mathrm{AE}}-\bar{\boldsymbol{\mu}}_{\mathrm{AE}})(\mathbf{h}_{\mathrm{AE}}-\bar{\boldsymbol{\mu}}_{\mathrm{AE}})^{\dagger}\right\}$, the correlation matrix of the channel $\mathbf{h}_{\mathrm{AE}}$ can be expressed as

$$\mathbf{R}_{\mathrm{E}} = \bar{\mathbf{C}}_{\mathrm{E}} + \bar{\boldsymbol{\mu}}_{\mathrm{AE}}\bar{\boldsymbol{\mu}}_{\mathrm{AE}}^{\dagger}. \tag{11}$$

It should be emphasized that we use multivariate Gaussian channels $\mathbf{h}_{\mathrm{AB}}$ and $\mathbf{h}_{\mathrm{AE}}$ in this development because Gaussian channel statistics are: 1) commonly used in channel representations and 2) convenient for determining the statistics of $\mathbf{h}_{\mathrm{AE}}$ conditioned on an observation of $\mathbf{h}_{\mathrm{AB}}$. However, under the approximations made in arriving at (5), as long as we can construct the correlation matrix $\mathbf{R}_{\mathrm{E}}$ as a function of d given an observation of $\mathbf{h}_{\mathrm{AB}}$—either numerically, in closed form, or from measurements—any statistical channel description can be used with the framework. Ultimately, the performance of the beamformer synthesis proposed in Section III-A that is based on this framework depends on our ability to find a value of $\mathbf{R}$ that can properly balance what is received by Bob and Eve. With reference to (5), this is entirely determined by the relationship between $\mathbf{h}_{\mathrm{AB}}$ and $\mathbf{R}_{\mathrm{E}}$ that depends strongly on the richness and angle spread of the multipath propagation and the distance between Bob and Eve and perhaps less on the statistical distribution used to describe the channels.

D. Semidefinite Programming Optimization

We are now prepared to determine the transmit beamformer covariance $\mathbf{R}$ that maximizes the minimum value of α_{avg} computed over all values of $d \geq d_{\min}$ under the constraints.

1) $\mathrm{Tr}(\mathbf{A}\mathbf{R}) \leq P_{\mathrm{T}}$.
2) $\mathbf{R}$ is positive semidefinite (property of a covariance).

Transforming this problem to a form that can be solved using SDP [10] offers two key benefits. First, being able to cast the problem into the SDP form ensures that the optimization is convex. Second, solving the problem via SDP includes the constraints in a natural way, as it can be difficult to incorporate successfully the power and the semidefinite covariance constraints into the cost function for gradient search or other similar optimization methods. These benefits coupled with the potential computational efficiency of SDP have motivated the use of similar techniques for array synthesis for radiation pattern shaping [21], [22]. We therefore follow the approach of using SDP to optimize the cost function as detailed in [10]. In this approach, we compute $\mathbf{R}_{\mathrm{E}}$ from (11) for each of a large number of values of $d \geq d_{\min}$ (i.e., positions of Eve), and we then use SDP to determine the value of $\mathbf{R}$ that maximizes the minimum value of α_{avg} over all of these values of d.

Once we have determined the optimal transmit covariance $\mathbf{R}$, we evaluate (1) by substituting the realized minimum value of α_{avg} in place of $\alpha(\mathbf{R})$ (and ignoring the maximization operation). Alternatively (and more rigorously), once we have constructed the matrix $\mathbf{R}$, we can form random realizations of the channel vectors $\mathbf{h}_{\text{AB}}$ and $\mathbf{h}_{\text{AE}}$, compute I_{SK} for each realization, and then compute the average of I_{SK} over the ensemble of realizations. In the results presented, we show the achieved performance for both of these techniques to demonstrate that optimizing the value of α_{avg} achieves very good average secure key rate.

III. Beamformer Synthesis

The development in Section II determines the covariance $\mathbf{R}$ that optimizes the average link security. However, this optimization does not specify the actual beamformers that should be used for channel estimation. We therefore now modify the approach originally developed in [10] for the LOS channel to construct the transmit beamformer based on the optimized covariance for the multipath channel. We also develop a more conventional beamforming approach based on signal and noise transmissions whose performance will be compared with that of the optimal synthesis technique.

A. Optimal Array Synthesis

Section II-B indicates that the covariance $\mathbf{R}$ incorporates the transmission of useful signal from which Bob (and Eve) can estimate the channel as well as artificial noise designed to confuse Eve, and therefore we must separate the beamformer weights used for each of the transmissions. The first step in the construction of the relevant beamformers is to write the expressions for the signal and noise power observed at Eve due to the transmission from Alice. In the LOS case, the procedure in [10] produces expressions for these quantities in terms of σ_{B}^2, σ_{E}^2, and σ_{BE}. However, since in the multipath case the propagation channel $\mathbf{h}_{\text{AE}}$ between Alice and Eve is understood only statistically (σ_{E}^2 and σ_{BE} are random), we compute the average signal power $P_{\text{S,E}}$ and noise power $P_{\text{N,E}}$ received at Eve by taking expectations, or

$$P_{\text{S,E}} = \text{E}\left\{|\sigma_{\text{BE}}|^2\right\}/\sigma_{\text{B}}^2 \tag{12}$$

$$P_{\text{N,E}} = \text{E}\left\{\sigma_{\text{E}}^2\right\} - \text{E}\left\{|\sigma_{\text{BE}}|^2\right\}/\sigma_{\text{B}}^2. \tag{13}$$

Next, we decompose the optimal transmit covariance using $\mathbf{R} = \mathbf{R}_{\text{S}} + \mathbf{R}_{\text{N}}$, where $\mathbf{R}_{\text{S}}$ and $\mathbf{R}_{\text{N}}$ represent the covariance of the signal and noise transmissions, respectively. Using these definitions, we can write the signal and noise powers as

$$\begin{aligned} P_{\text{S,E}} &= \text{E}\left\{\mathbf{h}_{\text{AE}}^{\text{T}}\mathbf{R}_{\text{S}}\mathbf{h}_{\text{AE}}^*\right\} \\ &= \text{E}\left\{\text{Tr}\left(\mathbf{h}_{\text{AE}}^{\text{T}}\mathbf{R}_{\text{S}}\mathbf{h}_{\text{AE}}^*\right)\right\} = \text{Tr}\left(\mathbf{R}_{\text{S}}\mathbf{R}_{\text{E}}^*\right) \end{aligned} \tag{14}$$

$$P_{\text{N,E}} = \text{E}\left\{\mathbf{h}_{\text{AE}}^{\text{T}}\mathbf{R}_{\text{N}}\mathbf{h}_{\text{AE}}^*\right\} = \text{Tr}\left(\mathbf{R}_{\text{N}}\mathbf{R}_{\text{E}}^*\right) \tag{15}$$

where the second equality in (14) is allowed because the argument of the trace is a scalar and the third arises from rearranging the matrix-vector products under the trace [the identical sequence is used to construct (15)]. Using the definitions of (3) and (4) in (12), invoking the rules regarding the trace indicated above, and equating the result to (14) leads to

$$\frac{\text{Tr}\left(\mathbf{R}\mathbf{h}_{\text{AB}}^*\mathbf{h}_{\text{AB}}^{\text{T}}\mathbf{R}\mathbf{R}_{\text{E}}^*\right)}{\mathbf{h}_{\text{AB}}^{\text{T}}\mathbf{R}\mathbf{h}_{\text{AB}}^*} = \text{Tr}\left(\mathbf{R}_{\text{S}}\mathbf{R}_{\text{E}}^*\right) \tag{16}$$

or

$$\mathbf{R}_{\text{S}} = \frac{\mathbf{R}\mathbf{h}_{\text{AB}}^*\mathbf{h}_{\text{AB}}^{\text{T}}\mathbf{R}}{\mathbf{h}_{\text{AB}}^{\text{T}}\mathbf{R}\mathbf{h}_{\text{AB}}^*}. \tag{17}$$

The noise covariance is then $\mathbf{R}_{\text{N}} = \mathbf{R} - \mathbf{R}_{\text{S}}$. With $\mathbf{R}_{\text{S}}$ and $\mathbf{R}_{\text{N}}$ determined, we can compute the signal and noise power received at Bob using, respectively

$$P_{\text{S,B}} = \mathbf{h}_{\text{AB}}^{\text{T}}\mathbf{R}_{\text{S}}\mathbf{h}_{\text{AB}}^* \tag{18}$$

$$P_{\text{N,B}} = \mathbf{h}_{\text{AB}}^{\text{T}}\mathbf{R}_{\text{N}}\mathbf{h}_{\text{AB}}^*. \tag{19}$$

The signal covariance is given by $\mathbf{R}_{\text{S}} = \text{E}\left\{\mathbf{w}_{\text{S}}\mathbf{w}_{\text{S}}^\dagger\right\}$ where $\mathbf{w}_{\text{S}}$ is the signal transmission vector. Comparison of this expression with (17) shows that the signal transmission can be expressed as

$$\mathbf{w}_{\text{S}} = \frac{\mathbf{R}\mathbf{h}_{\text{AB}}^*}{\sqrt{\mathbf{h}_{\text{AB}}^{\text{T}}\mathbf{R}\mathbf{h}_{\text{AB}}^*}}\, s = \mathbf{w}_{\text{S0}}\, s \tag{20}$$

where s satisfies a zero-mean unit-variance complex Gaussian distribution. Using the eigenvalue decomposition $\mathbf{R}_{\text{N}} = \mathbf{U}_{\text{N}}\Sigma_{\text{N}}\mathbf{U}_{\text{N}}^\dagger$, the noise transmission can be written as

$$\mathbf{w}_{\text{N}} = \mathbf{U}_{\text{N}}\mathbf{z}, \tag{21}$$

where the ith element of the vector $\mathbf{z}$ follows a zero-mean complex Gaussian distribution with variance $\Sigma_{\text{N},ii}$ (the ith diagonal element of Σ_{N}). The composite beamformer is then given as $\mathbf{w} = \mathbf{w}_{\text{S}} + \mathbf{w}_{\text{N}}$.

The average radiation patterns associated with the signal and noise beamformers can be formed by introducing the steering vector $\mathbf{a}(\theta,\phi)$ whose ith element, $1 \le i \le N_{\text{A}}$, is

$$a_i(\theta,\phi) = e^{jk(x_i \sin\theta\cos\phi + y_i \sin\theta\sin\phi + z_i\cos\theta)} \tag{22}$$

where (x_i, y_i, z_i) is the position of Alice's ith antenna element and k is the wavenumber. The average signal pattern is

$$\begin{aligned} F_{\text{S}}(\theta,\phi) &= E\left\{\mathbf{a}^{\text{T}}(\theta,\phi)\,\mathbf{w}_{\text{S}}\,\mathbf{w}_{\text{S}}^\dagger\,\mathbf{a}^*(\theta,\phi)\right\} \\ &= \mathbf{a}^{\text{T}}(\theta,\phi)\,\mathbf{R}_{\text{S}}\,\mathbf{a}^*(\theta,\phi). \end{aligned} \tag{23}$$

Similarly, the average noise pattern is

$$F_{\text{N}}(\theta,\phi) = \mathbf{a}^{\text{T}}(\theta,\phi)\,\mathbf{R}_{\text{N}}\,\mathbf{a}^*(\theta,\phi). \tag{24}$$

B. Suboptimal Array Synthesis

Recognizing the role of transmitting artificial noise to reduce Eve's ability to estimate her channel $\mathbf{h}_{\text{AE}}$ allows us to formulate an alternate array synthesis procedure. Specifically, we transmit training data using the beamformer that maximizes the signal power observed by Bob and then transmit artificial noise on the orthogonal complement to the signal beamformer. In this approach, Alice constructs beamformers based on her knowledge of $\mathbf{h}_{\text{AB}}$ and ignores any information about channel spatial correlation. To construct these beamformers, we compute the singular value decomposition (SVD) $\mathbf{h}_{\text{AB}} = \mathbf{U}\Lambda\mathbf{V}^\dagger$, where $\mathbf{U}$ and $\mathbf{V}$ are the unitary singular vector matrices and Λ is the diagonal matrix of singular values. Note that, since $\mathbf{h}_{\mathrm{AB}}$ is a vector, only one singular value is nonzero, and we arrange the SVD such that this nonzero singular value is in the first position. This means that the first column of $\mathbf{U}$ provides the desired signal beamformer, and the remaining columns of $\mathbf{U}$ provide the desired orthogonal complement. Let γ and $\gamma' = (P_{\mathrm{T}} - \gamma)/(N_{\mathrm{A}} - 1)$ represent the transmitted power devoted to the signal and each noise beamforming vector, respectively. We can therefore construct the transmit covariance as

$$\mathbf{R} = \mathbf{U}\Lambda'\mathbf{U}^{\dagger} \tag{25}$$

where

$$\Lambda' = \begin{bmatrix} \gamma & 0 & \cdots & 0 \\ 0 & \gamma' & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \gamma' \end{bmatrix}. \tag{26}$$

The performance of this approach is optimized by numerically searching for the value of γ that maximizes α_{avg} for each realization of $\mathbf{h}_{\mathrm{AB}}$ under the constraint that $\mathrm{Tr}(\Lambda') \leq P_{\mathrm{T}}$.

IV. Results

Solving the problem under the constraint that the distance $d \geq d_{\min}$ requires that we specify a model for the elements of $\mathbf{C}_{\mathrm{h}}$ as a function of d, Alice's array geometry, and the propagation conditions. While the optimization provided here is general for any model, for the computations shown we assume that 1) the channels are zero-mean Gaussian random variables ($\boldsymbol{\mu}_{\mathrm{AE}} = \boldsymbol{\mu}_{\mathrm{AB}} = \mathbf{0}$) and 2) the power angular spectrum (PAS) defining the propagation conditions at Alice, Bob, and Eve is uniform in elevation angle θ while satisfying the von Mises distribution in azimuth angle ϕ [23], or

$$\mathrm{PAS}(\theta, \phi) = \frac{\exp[\kappa \cos(\phi - \phi_p)]}{2\pi I_0(\kappa)} \tag{27}$$

where κ specifies the angular distribution of the multipath departures or arrivals, ϕ_p is the mean angle of departure/arrival (assumed to be 0), and I_0 is the zero-order modified Bessel function. Note that the von Mises distribution is uniform for $\kappa = 0$ and becomes more Gaussian as κ increases. As the multipath environment becomes more directional with increasing κ, the correlation between channels observed on different antennas increases.

The relationship between the cross-channel correlation and propagation directionality has important implications for beamforming. The optimal algorithm uses knowledge of the channel $\mathbf{h}_{\mathrm{AB}}$ and the channel correlation, which incorporates the average channel directionality, as a basis for beamformer construction. When the average behavior has directional selectivity (higher correlation), Alice can exploit this directionality in addition to her knowledge of $\mathbf{h}_{\mathrm{AB}}$ to beamform to give Bob an advantage over Eve. However, when the average propagation is more uniform in angle, Alice must mostly rely on her knowledge of $\mathbf{h}_{\mathrm{AB}}$ for beamforming, and the performance of the optimal solution approaches that of the suboptimal synthesis method of Section III-B. Given this observation, the simulations specify the PAS using either $\kappa = 2$ (medium transmit correlation) or $\kappa = 10$ (high transmit correlation) in order to highlight the relative benefit of the optimal synthesis algorithm. While results for low correlation are not included, it is noteworthy that our extensive simulations show that the optimal solution performance always remains equal to or better than that of the suboptimal solution.

For all examples shown, Alice's array is a ULA of $N_{\mathrm{A}} = 5$ half-wave dipoles with element separation $\lambda/2$, where λ is the wavelength, and therefore we neglect effects of mutual coupling on her array. The elements of the 5×5 correlation matrix $\mathbf{R}_{\mathrm{A}}$ for Alice's array can then be computed in closed form [23]. In contrast, since Bob and Eve can be close together, we consider the impact of mutual coupling on their radiation patterns and on the correlation between their channel observations. Specifically, we use NEC to compute the pattern for Bob's half-wave dipole in the presence of Eve's (open circuited) dipole as well as for Eve's antenna in the presence of Bob's. We then construct the 2×2 matrix $\mathbf{R}_{\mathrm{BE}}$ using the technique detailed in [24] based on these radiation patterns and the PAS with $\kappa = 2$. Note that while the antenna termination impedances can impact the observed correlation, our objective is to determine the performance of the array synthesis technique. We therefore avoid the complication of considering a range of impedance terminations in addition to the other relevant parameters and consider only the correlation computed from radiation patterns obtained when the neighboring antenna is unterminated (open circuit).

Using a ULA at Alice along with a PAS that is uniform in elevation means that our beamforming is confined to the azimuthal plane. However, applying the method to multidimensional arrays and a PAS that varies in azimuth and elevation will produce beamforming in both angular dimensions.

Because our channels are zero-mean, the covariance of $\mathbf{h}$ in (6) can be written [25]

$$\mathbf{C}_{\mathrm{h}} = \mathbf{R}_{\mathrm{BE}} \otimes \mathbf{R}_{\mathrm{A}} \tag{28}$$

where $\otimes$ is a Kronecker product. Extracting $\mathbf{C}_{\mathrm{B}}$ from this result according to (6) and using the definition of $\mathbf{C}_{\mathrm{B}}$ in (7) indicates that we can form a random realization of $\mathbf{h}_{\mathrm{AB}}$ using $\mathbf{h}_{\mathrm{AB}} = \mathbf{C}_{\mathrm{B}}^{1/2}\mathbf{h}_0$, where $\mathbf{h}_0$ is an $N_{\mathrm{A}} \times 1$ vector of independent, zero-mean, and unit-variance complex Gaussian random variables. Computing $\mathbf{R}_{\mathrm{E}}$ from $\mathbf{C}_{\mathrm{h}}$ and the realization of $\mathbf{h}_{\mathrm{AB}}$, as detailed in Section II-C, allows us to use the cost function in (5) with SDP to determine the desired transmit covariance $\mathbf{R}$. Where average quantities are shown in the results, the averages are taken over 1000 random realizations of $\mathbf{h}_{\mathrm{AB}}$ (each with its corresponding $\mathbf{R}_{\mathrm{E}}$ as a function of d).

As mentioned in Section II-D, as part of our analysis, we wish to compare the value $I_{\mathrm{SK}}(\alpha_{\mathrm{avg}})$ obtained by substituting α_{avg} in place of $\alpha(\mathbf{R})$ in (1) with the value $\mathrm{E}\{I_{\mathrm{SK}}\}$ computed by applying the beamformers to the signal and artificial noise transmissions obtained from the optimal value of $\mathbf{R}$ (see Section III-A) to an ensemble of random realizations of $\mathbf{h}_{\mathrm{AE}}$ and averaging the resulting values of I_{SK}. To obtain $\mathrm{E}\{I_{\mathrm{SK}}\}$, we therefore must create multiple realizations of $\mathbf{h}_{\mathrm{AE}}$ conditioned on a single realization of $\mathbf{h}_{\mathrm{AB}}$. We do this by

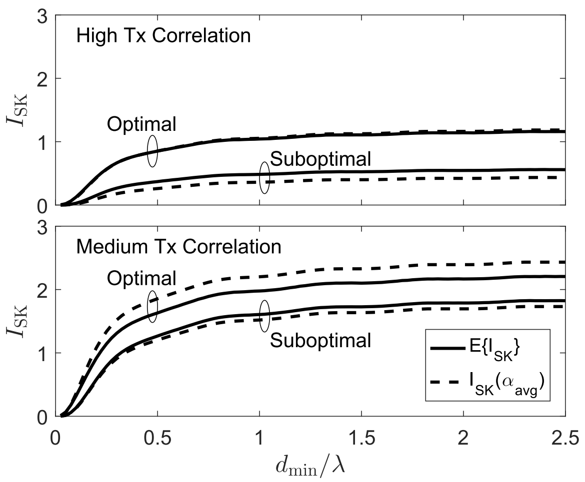


Fig. 2. Average secure key rate computed using two different methods for high and medium transmit correlation as a function of the minimum distance $d_{\min}$ between Bob and Eve.

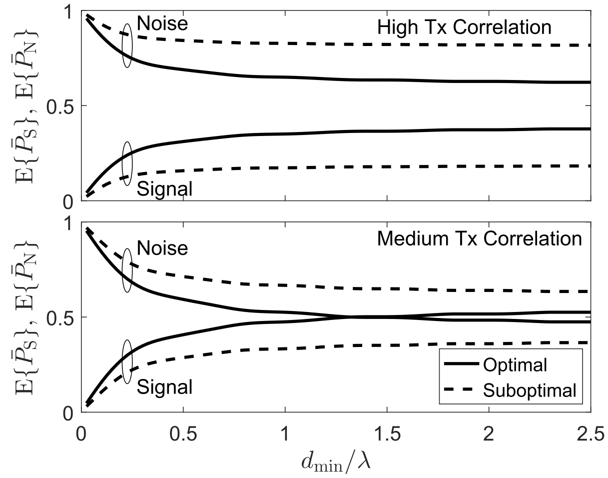


Fig. 3. Average transmitted signal and noise powers for high and medium transmit correlation as a function of the minimum distance $d_{\min}$ between Bob and Eve.

computing $\bar{\boldsymbol{\mu}}_{\mathrm{AE}}$ and $\bar{\mathbf{C}}_{\mathrm{E}}^{1/2}$ from (9) to (10) and then creating channel realizations using $\mathbf{h}_{\mathrm{AE}} = \bar{\mathbf{C}}_{\mathrm{E}}^{1/2}\mathbf{h}_0' + \bar{\boldsymbol{\mu}}_{\mathrm{AE}}$, where $\mathbf{h}_0'$ is an $N_{\mathrm{A}} \times 1$ vector of independent, zero-mean, and unit-variance complex Gaussian random variables. In the results that follow, we realize 1000 channels $\mathbf{h}_{\mathrm{AE}}$ for each realization of $\mathbf{h}_{\mathrm{AB}}$.

All simulations use an available transmit power of $P_{\mathrm{T}} = 1$ and a variance of the channel estimation error due to thermal noise of $\sigma_0^2 = 0.1$.

A. Secure Key Rate

Fig. 2 presents the average secure key rate I_{SK} obtained from 1000 realizations of $\mathbf{h}_{\mathrm{AB}}$ as a function of $d_{\min}$ for both high and medium correlation at Alice, with results presented for both the methods of computing the average secure key rate for each value of $\mathbf{h}_{\mathrm{AB}}$. Several key observations from this result deserve particular mention.

1) As expected, as the distance $d_{\min}$ between Bob and Eve increases, the correlation between $\mathbf{h}_{\mathrm{AB}}$ and $\mathbf{h}_{\mathrm{AE}}$ decreases, resulting in higher realized I_{SK}.
2) Comparing the results for different correlation conditions at Alice (*Tx Correlation*), we observe that high transmit correlation increases the correlation between $\mathbf{h}_{\mathrm{AB}}$ and $\mathbf{h}_{\mathrm{AE}}$ and therefore reduces I_{SK}.
3) The secure key rate achieved with the optimal beamformers is significantly better than that obtained with the suboptimal synthesis, with the relative improvement increasing with the transmit correlation.
4) As discussed in Section II-B, substituting our optimization cost function (5) into (1) represents a bound on performance, and therefore using this as our optimization criterion is not guaranteed to offer the desired outcome. However, the significant performance improvement over the suboptimal approach suggests that optimizing this bound is a reasonable approach for synthesizing array weights that improve performance. Furthermore, the results generally show that the bound $I_{\mathrm{SK}}(\alpha_{\mathrm{avg}})$ is close to the actual average $\mathrm{E}\{I_{\mathrm{SK}}\}$ for most the cases, with the largest discrepancy occurring with medium Tx correlation and the optimal solution.

B. Transmit Power Allocation

Fig. 3 plots the average *transmitted* signal and noise powers $\mathrm{E}\left\{\bar{P}_{\mathrm{S}}\right\}$ and $\mathrm{E}\left\{\bar{P}_{\mathrm{N}}\right\}$, respectively, for the same cases used in Fig. 2, where $\bar{P}_{\mathrm{S}} = \mathrm{Tr}(\mathbf{R}_{\mathrm{S}})$, $\bar{P}_{\mathrm{N}} = \mathrm{Tr}(\mathbf{R}_{\mathrm{N}})$, and the expectation is approximated using the sample mean over 1000 realizations of $\mathbf{h}_{\mathrm{AB}}$. These quantities, which should not be confused with the average signal and noise powers $P_{\mathrm{S},\xi}$ and $P_{\mathrm{N},\xi}$, $\xi \in \{\mathrm{B}, \mathrm{E}\}$, *received* by Bob and Eve that are discussed in Section III-A, indicate how much of the transmit power is devoted to useful signal or to artificial noise. We observe from these results that when compared with the suboptimal solution, the optimal beamforming solution allocates more of the available transmit power to the useful training signal. This means that Bob will have a higher effective SNR for completing his channel estimation, a fact that generally improves I_{SK}. The results also show that lower transmit correlation allows Alice to allocate a higher fraction of the power to the signal, since the reduced transmit correlation makes it less likely that the signal power designated for Bob will reach Eve.

C. Received Power and Radiation Patterns

Figs. 4 and 5 plot the average signal power at Bob and the average signal and noise powers at Eve as a function of $d_{\min}$ for high and medium transmit correlation, respectively. The expectation of power is approximated as a sample mean over 1000 realizations of $\mathbf{h}_{\mathrm{AB}}$. Because the elements of $\mathbf{h}_{\mathrm{AB}}$ are zero-mean unit-variance complex Gaussian random variables, $\mathrm{E}\left\{\mathbf{h}_{\mathrm{AB}}^{\dagger}\mathbf{h}_{\mathrm{AB}}\right\} = 5$, which accounts for received power levels greater than the transmit power level ($P_{\mathrm{T}} = 1$). This nonphysical outcome is inconsequential, as the secure key rate largely depends on the relative received power levels.

In discussing these results, it is also useful to consider Fig. 6, which plots the signal pattern $F_{\mathrm{S}}(\phi)$ in (23) and noise pattern $F_{\mathrm{N}}(\phi)$ in (24) as a function of the

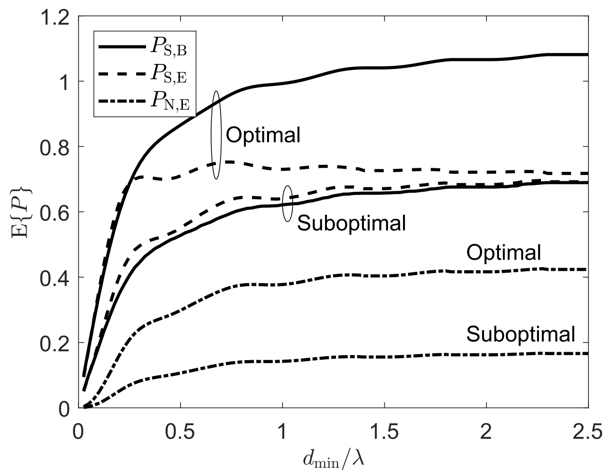


Fig. 4. Average signal power at Bob and Eve and average noise power at Eve as a function of the minimum distance $d_{\min}$ between Bob and Eve for high transmit correlation.

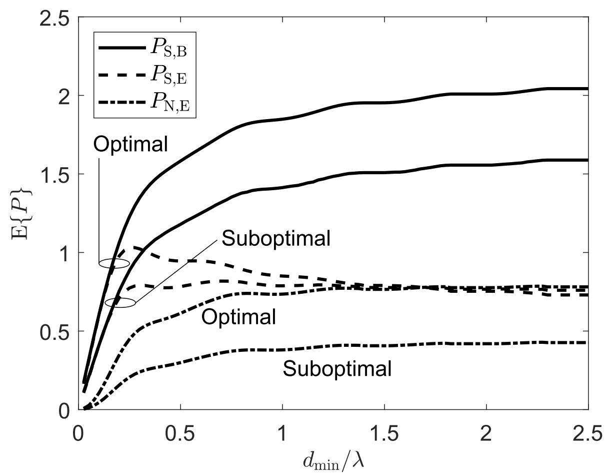


Fig. 5. Average signal power at Bob and Eve and average noise power at Eve as a function of the minimum distance $d_{\min}$ between Bob and Eve for medium transmit correlation.

azimuthal angle ϕ for a single representative channel $\mathbf{h}_{\mathrm{AB}}$ with $d_{\min} = 2.5\lambda$ and high transmit correlation. The results, obtained both with the optimal and suboptimal synthesis techniques, show that the suboptimal synthesis distributes the noise relatively uniformly outside of the region, where most of the signal is directed. In contrast, because beamforming in a multipath scenario establishes certain desired outcomes at a *point* in space rather than over an angular sector, the optimal synthesis is able to more advantageously direct both the signal and noise transmissions for this channel. While not shown here, when $\kappa = 0$, we find that the optimal and suboptimal synthesis techniques yield nearly identical patterns.

The results in Figs. 4–6 lead to several key observations:

1) For all the cases, the noise power at Bob is $P_{\mathrm{N,B}} = 0$. The suboptimal solution deliberately transmits the noise on the subspace orthogonal to the channel $\mathbf{h}_{\mathrm{AB}}$, and the optimal solution achieves the same result. It is interesting that, with reference to Fig. 6, the two solutions achieve this outcome using different signal beamformers.

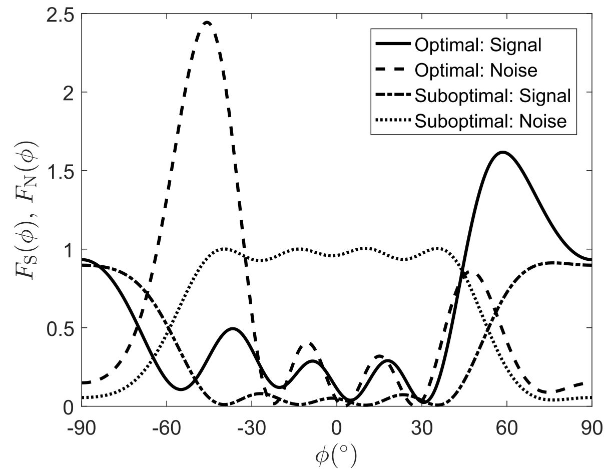


Fig. 6. Signal and noise patterns obtained from the optimal and suboptimal synthesis methods for a single representative realization of $\mathbf{h}_{\mathrm{AB}}$ with high transmit correlation and $d_{\min} = 2.5\lambda$.

2) We learned from Fig. 3 that the optimal solution allocates a higher fraction of the transmit power to signal, and we see here that this significantly increases the signal power at Bob. While this also increases the signal power at Eve, the relative increase is notably lower than that observed at Bob.
3) Because the optimal solution strategically transmits the noise, it is able to allocate a smaller fraction of the transmit power to the noise but result in notably higher noise power at Eve.

The ultimate conclusion from this is simply that the optimal beamforming solution places more signal power at Bob and creates a lower SNR at Eve than the suboptimal solution. This means that Bob will have better estimates of $\mathbf{h}_{\mathrm{AB}}$ and that Eve will have inferior estimates of her channel $\mathbf{h}_{\mathrm{AE}}$ and therefore less information regarding $\mathbf{h}_{\mathrm{AB}}$ that is the basis for generating the encryption key.

V. Conclusion

This paper develops an array synthesis technique useful when generating secret encryption keys from reciprocal wireless channel estimates in a multipath channel. The approach formulates a bound on the average secure key rate and then uses SDP to find the transmit covariance matrix that maximizes the minimum value of this bound over all possible positions of an eavesdropper who is constrained to be at least a certain distance away from the legitimate radio. This transmit covariance is then separated into array weights that either carry useful training signal for estimating the channels or artificial noise designed to confuse the eavesdropper. The implementation incorporates the impact of antenna mutual coupling between the antenna on one of the legitimate nodes and the antenna on the proximate eavesdropper. Simulation results reveal that the key rate obtained from the array synthesis technique is significantly higher than that obtained with an intuitive but suboptimal synthesis procedure, with the relative benefit improving as the transmit correlation created by the channel propagation conditions increases.

References

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

[2] 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.

[3] 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.

[4] J. W. Wallace, C. Chen, and M. A. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *Proc. 3rd Eur. Conf. Antennas Propag.*, Berlin, Germany, Mar. 2009, pp. 1499–1503.

[5] 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.

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

[7] B. T. Quist and M. A. Jensen, "Optimal channel estimation in beamformed systems for common-randomness-based secret key establishment," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1211–1220, Jul. 2013.

[8] B. T. Quist and M. A. Jensen, "Bound on the key establishment rate for multi-antenna reciprocal electromagnetic channels," *IEEE Trans. Antennas Propag.*, vol. 62, no. 3, pp. 1378–1385, Mar. 2014.

[9] B. T. Quist and M. A. Jensen, "Maximization of the channel-based key establishment rate in MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5565–5573, Oct. 2015.

[10] R. Mehmood, J. W. Wallace, and M. A. Jensen, "Secure array synthesis," *IEEE Trans. Antennas Propag.*, vol. 63, no. 9, pp. 3887–3896, Sep. 2015.

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

[12] R. Mehmood, J. W. Wallace, and M. A. Jensen, "Optimal array signaling for key establishment in static multipath channels," in *Proc. Eur. Conf. Antennas Propag. (EuCAP)*, Lisbon, Portugal, Apr. 2015, pp. 1–2.

[13] R. Mehmood, J. W. Wallace, and M. A. Jensen, "Secure array synthesis for encryption key establishment in multipath channels," in *Proc. Eur. Conf. Antennas Propag. (EuCAP)*, Davos, Switzerland, Apr. 2016, pp. 1–2.

[14] J. G. Proakis, *Digital Communications*, 4th ed. New York, NY, USA: McGraw-Hill, 2001.

[15] R. Vaughan and J. B. Andersen, *Channels, Propagation and Antennas for Mobile Communications*. London, U.K.: IEE, 2003.

[16] 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.

[17] S. Loyka and A. Kouki, "On the use of Jensen's inequality for MIMO channel capacity estimation," in *Proc. Can. Conf. Elect. Comput. Eng.*, vol. 1. Toronto, ON, Canada, May 2001, pp. 475–480.

[18] F. K. Sharifabad, M. A. Jensen, and A. L. Anderson, "Array beamforming synthesis for point-to-point MIMO communication," *IEEE Trans. Antennas Propag.*, vol. 63, no. 9, pp. 3878–3886, Sep. 2015.

[19] R. B. Ertel *et al.*, "Overview of spatial channel models for antenna array communication systems," *IEEE Pers. Commun.*, vol. 5, no. 1, pp. 10–22, Feb. 1998.

[20] M. L. Eaton, *Multivariate Statistics: A Vector Space Approach*, vol. 198, no. 3. New York, NY, USA: Wiley, 1983.

[21] T. Isernia, P. D. Iorio, and F. Soldovieri, "An effective approach for the optimal focusing of array fields subject to arbitrary upper bounds," *IEEE Trans. Antennas Propag.*, vol. 48, no. 12, pp. 1837–1847, Dec. 2000.

[22] T. Isernia, A. Massa, A. F. Morabito, and P. Rocca, "On the optimal synthesis of phase-only reconfigurable antenna arrays," in *Proc. Eur. Conf. Antennas Propag.*, Rome, Italy, Apr. 2011, pp. 2074–2077.

[23] A. Abdi, J. A. Barger, and M. Kaveh, "A parametric model for the distribution of the angle of arrival and the associated correlation function and power spectrum at the mobile station," *IEEE Trans. Veh. Technol.*, vol. 51, no. 3, pp. 425–434, May 2002.

[24] F. K. Sharifabad, M. A. Jensen, and Z. Yun, "Closed-form evaluation of the MIMO channel spatial covariance," *IEEE Trans. Antennas Propag.*, vol. 61, no. 2, pp. 901–909, Feb. 2013.

[25] J.-P. Kermoal, L. Schumacher, K. I. Pedersen, P. E. Mogensen, and F. Frederiksen, "A stochastic MIMO radio channel model with experimental validation," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 6, pp. 1211–1226, Aug. 2002.

Rashid Mehmood (S'05–M'16) received the B.Sc. degree *(cum laude)* in communication systems engineering from the Institute of Space Technology, Islamabad, Pakistan, in 2007, and the M.Sc. degree in electrical engineering from Jacobs University Bremen, Bremen, Germany, in 2010, and the Ph.D. degree in electrical and computer engineering from Brigham Young University, Provo, UT, USA, in 2015.

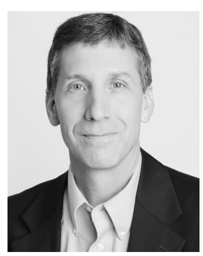
He currently leads the Radar Systems Research Group, Wavetronix, Provo, UT, USA. His current research interests include over-the-air testing, reconfigurable antennas, optimization techniques, MIMO communications and radar, and physical layer security.

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

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, Provo, UT, USA, in 1997 and 2002, respectively.

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

Dr. Wallace 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. He has served as an Associate Editor of the IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and the IEEE TRANSACTIONS ON AEROSPACE AND ELECTRONIC SYSTEMS.



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, CA, USA, 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 and the Dean of the Ira A. Fulton College of Engineering and Technology. His current research interests include antennas and propagation for communications, microwave circuit design, multiantenna signal processing, and physical layer security.

Dr. Jensen was a Past President of the IEEE Antennas and Propagation Society. He was elevated to the grade of IEEE Fellow in 2008 in recognition of his research on multiantenna communication. In 2002, he received the Harold A. Wheeler Applications Prize Paper Award in the IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION. He was the Editor-in-Chief and an Associate Editor of the IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION and an Associate Editor of the IEEE ANTENNAS AND WIRELESS PROPAGATION LETTERS. He has been a member and the Chair of the Joint Meetings Committee of the IEEE Antennas and Propagation Society, a member of the society AdCom, the society Publications Committee, and the co-chair or the technical program chair for six society-sponsored symposia.