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 $N_A \times 1$ vectors $\mathbf{h}_{AB}$, $\mathbf{h}_{BA}$, and $\mathbf{h}_{AE}$ 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
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 $h_{AE}$ from Alice to Eve is correlated with the channel $h_{AB}$ from Alice to Bob—but that physical or other constraints ensure that the antenna separation $d$ between Bob and Eve is at least $d_{\text{min}}$.

Our specific focus is on secret key generation from reciprocal channel estimates [1]–[3]. In this technique, Alice transmits training transmission in order to reduce the effective SNR 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 $h_{AE}$ and reducing the information she has about the established key. The transmit vector $w$ 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 $h_{BA}$ and Bob observes $h_{AB}$ that Eve is unable to guess based on her observation of $h_{AE}$. It is large when $h_{BA}$ and $h_{AB}$ are highly similar and reduced if $h_{AE}$ is similar to $h_{AB}$ and $h_{BA}$. The mathematical form of $I_{SK}$ depends on the application, but for our problem is shown in [10] to assume the form

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

(1)

where

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

(2)

$$\sigma_0^2 = \mathbf{h}_{AE}^H \mathbf{A}_0^H \mathbf{R} \mathbf{A}_0 \mathbf{h}_{AE}$$

(3)

$$\sigma_{BE}^2 = \mathbf{h}_{AB}^H \mathbf{R} \mathbf{h}_{AE}^H$$

(4)

where $\sigma_0^2$ 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 $h_{AE}$. In an LOS scenario, Alice knows the channel $h_{AE}$ 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 $h_{AB}$ to Bob and unknown channel $h_{AE}$ to Eve.

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 $d \geq d_{\text{min}}$. 

$w_1$ $w_2$ $\ldots$ $w_N$ $w_1$ $w_2$ $h_{AB}$ $h_{BA}$ $d_{\text{min}}$ $d$ $h_{AE}$ $\mathbf{A}_0$ $\mathbf{R}$ $\mathbf{h}_{AB}$ $\mathbf{h}_{AE}$
as a function of the distance $d$, meaning that $\sigma_{E}^{2}$, $\sigma_{BE}$, and $\alpha$ 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 $\mathbf{h}_{AE}$ for each cost function evaluation. But recognizing that (1) is monotonic in $\alpha(R)$, we simplify the optimization by instead using the average value of $\alpha(R)$ 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 $\alpha(R)$ is defined as

$$\alpha_{avg} = \frac{\sigma_{E}^{2}}{E[\sigma_{E}]^{2} - E[\sigma_{BE}]^{2}}$$

(5)

where $E[\sigma_{E}]^{2} = \text{Tr} \left( \mathbf{R}_{E} \right)$, $E[\sigma_{BE}]^{2} = \mathbf{h}_{AE}^{\dagger} \mathbf{R}_{E} \mathbf{h}_{AB}$, and $\mathbf{R}_{E} = E[\mathbf{h}_{AE} \mathbf{h}_{AE}^{\dagger}]$. Since $\alpha_{avg}$ depends on Eve’s position, we find the value of $\mathbf{R}$ that maximizes the minimum value of $\alpha_{avg}$ over all of Eve’s possible locations that satisfy $d \geq d_{\text{min}}$. Because this requires Alice to know $\mathbf{R}_{E}$ as a function of $d$ conditioned on her observation of $\mathbf{h}_{AB}$, we specifically discuss the construction of $\mathbf{R}_{E}$ in Section II-C.

Substituting $\alpha_{avg}$ for the instantaneous value $\alpha(R)$ 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 $\alpha_{avg}$, Alice must first construct the correlation matrix $\mathbf{R}_{E}$ for each possible value of $d$ and her observed channel vector $\mathbf{h}_{AB}$, which requires that she determine the statistics of $\mathbf{h}_{AE}$ conditioned on an observation of $\mathbf{h}_{AB}$. Let $\mu_{AB}$ and $\mu_{AE}$ be the vector mean of the multivariate normal channels $\mathbf{h}_{AB}$ and $\mathbf{h}_{AE}$, respectively, and define $\mathbf{h} = [\mathbf{h}_{AB} \mathbf{h}_{AE}]^{\dagger}$ and $\mu = [\mu_{AB}^{\dagger} \mu_{AE}^{\dagger}]^{\dagger}$. Using channel estimation, Alice only learns the channel $\mathbf{h}_{AB}$, 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

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

(6)

where

$$\mathbf{C}_{E} = E \left\{ (\mathbf{h}_{AE} - \mu_{AE}) (\mathbf{h}_{AE} - \mu_{AE})^{\dagger} \right\}$$

(7)

$$\mathbf{C}_{BE} = E \left\{ (\mathbf{h}_{AB} - \mu_{AB}) (\mathbf{h}_{AE} - \mu_{AE})^{\dagger} \right\} = \mathbf{C}_{EB}^{\dagger}$$

(8)

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

$$\mu_{AE} = \mathbf{C}_{EB} \mathbf{C}_{B}^{-1} (\mathbf{h}_{AB} - \mu_{AB})$$

(9)

$$\mathbf{C}_{E} = \mathbf{C}_{E} - \mathbf{C}_{EB} \mathbf{C}_{B}^{-1} \mathbf{C}_{BE}$$

(10)

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

$$\mathbf{R}_{E} = \tilde{\mathbf{C}}_{E} + \mu_{AE} \mu_{AE}^{\dagger}$$

(11)

It should be emphasized that we use multivariate Gaussian channels $\mathbf{h}_{AB}$ and $\mathbf{h}_{AE}$ in this development because Gaussian channel statistics are: 1) commonly used in channel representations and 2) convenient for determining the statistics of $\mathbf{h}_{AE}$ conditioned on an observation of $\mathbf{h}_{AB}$. However, under the approximations made in arriving at (5), as long as we can construct the correlation matrix $\mathbf{R}_{E}$ as a function of $d$ given an observation of $\mathbf{h}_{AB}$—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 $\mathbf{h}_{AB}$ and $\mathbf{R}_{E}$ 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 $\alpha_{avg}$ computed over all values of $d \geq d_{\text{min}}$ under the constraints.

1) $\text{Tr}(\mathbf{R}) \leq N_{T}$.

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 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 $\mathbf{R}_{E}$ from (11) for each of a large number of values of $d \geq d_{\text{min}}$ (i.e., positions of Eve), and we then use SDP to determine the value of $\mathbf{R}$ that maximizes the minimum value of $\alpha_{avg}$ over all of these values of $d$. 


Once we have determined the optimal transmit covariance $R$, we evaluate (1) by substituting the realized minimum value of $\sigma_{\text{avg}}$ in place of $\alpha(R)$ (and ignoring the maximization operation). Alternatively (and more rigorously), once we have constructed the matrix $R$, we can form random realizations of the channel vectors $h_{\text{AB}}$ and $h_{\text{AE}}$, compute $I_{\text{SK}}$ for each realization, and then compute the average of $I_{\text{SK}}$ 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 $\sigma_{\text{avg}}$ achieves very good average secure key rate.

III. BEAMFORMER SYNTHESIS

The development in Section II determines the covariance $R$ 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 $R$ 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 $\sigma_{\text{B}}^2$, $\sigma_{\text{E}}^2$, and $\sigma_{\text{BE}}$. However, since in the multipath case the propagation channel $h_{\text{AE}}$ between Alice and Eve is understood only statistically ($\sigma_{\text{E}}^2$ and $\sigma_{\text{BE}}$ are random), we compute the average signal power $P_{S,E}$ and noise power $P_{N,E}$ received at Eve by taking expectations, or

\[
\begin{align*}
P_{S,E} &= \mathbb{E}\left\{ |\sigma_{\text{BE}}|^2 \right\} / \sigma_{\text{B}}^2 \quad (12) \\
P_{N,E} &= \mathbb{E}\left\{ \sigma_{\text{E}}^2 \right\} \quad (13)
\end{align*}
\]

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

\[
\begin{align*}
P_{S,E} &= \mathbb{E}\left\{ h_{\text{AE}}^\dagger R_{S} h_{\text{AE}}^* \right\} = \mathbb{E}\left\{ |\sigma_{\text{BE}}|^2 \right\} / \sigma_{\text{B}}^2 \quad (14) \\
P_{N,E} &= \mathbb{E}\left\{ h_{\text{AE}}^\dagger R_{N} h_{\text{AE}}^* \right\} = \mathbb{E}\left\{ \sigma_{\text{E}}^2 \right\} \quad (15)
\end{align*}
\]

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

\[
\begin{align*}
\mathbb{E}\left\{ h_{\text{AE}}^\dagger R_{S} h_{\text{AE}}^* \right\} &= \mathbb{E}\left\{ |\sigma_{\text{BE}}|^2 \right\} / \sigma_{\text{B}}^2 = \mathbb{E}\left\{ R_{S} R_{E}^* \right\} \quad (16) \\
R_{S} &= \frac{R_{S} h_{\text{AE}}^\dagger R_{E}}{h_{\text{AE}}^\dagger R_{E} h_{\text{AE}}^*} \quad (17)
\end{align*}
\]

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

\[
\begin{align*}
P_{S,B} &= h_{\text{AE}}^\dagger R_{S} h_{\text{AE}} \quad (18) \\
P_{N,B} &= h_{\text{AE}}^\dagger R_{N} h_{\text{AE}} \quad (19)
\end{align*}
\]

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

\[
w_{S} = \frac{R_{S} h_{\text{AE}}^*}{\sqrt{h_{\text{AE}}^\dagger R_{S} h_{\text{AE}}}} \quad (20)
\]

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

\[
w_{N} = U_{N} z_{N} \quad (21)
\]

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

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

\[
a_{i}(\theta, \phi) = e^{jk(x_{i} \sin \theta \cos \phi + y_{i} \sin \theta \sin \phi + z_{i} \cos \theta)} \quad (22)
\]

where $(x_{i}, y_{i}, z_{i})$ is the position of Alice’s $i$th antenna element and $k$ is the wavenumber. The average signal pattern is

\[
F_{S}(\theta, \phi) = E\left\{ a^\dagger(\theta, \phi) w_{S} w_{S}^\dagger a(\theta, \phi) \right\} = a^\dagger(\theta, \phi) R_{S} a(\theta, \phi) \quad (23)
\]

Similarly, the average noise pattern is

\[
F_{N}(\theta, \phi) = a^\dagger(\theta, \phi) R_{N} a(\theta, \phi) \quad (24)
\]

B. Suboptimal Array Synthesis

Recognizing the role of transmitting artificial noise to reduce Eve’s ability to estimate her channel $h_{\text{AE}}$ 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 $h_{\text{AB}}$ and ignores any information about channel spatial correlation. To construct these beamformers, we compute the singular value decomposition (SVD) $h_{\text{AB}} = U_{A} \Sigma_{A} V_{A}^\dagger$, where $U$ and $V$ are the unitary singular vector.
matrices and \( \Lambda \) is the diagonal matrix of singular values. Note that, since \( \mathbf{h}_{AB} \) 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 \( \gamma \) and \( \gamma' = (P_T - \gamma)/(N_A - 1) \) represent the transmitted power devoted to the signal and each noise beamforming vector, respectively. We can therefore construct the transmit covariance as

\[
\mathbf{R} = \mathbf{U} \Lambda' \mathbf{U}^\dagger
\]

where

\[
\Lambda' = \begin{bmatrix}
\gamma & 0 & \cdots & 0 \\
0 & \gamma' & \cdots & 0 \\
& \ddots & \ddots & \ddots \\
0 & \cdots & 0 & \gamma'
\end{bmatrix}
\] (26)

The performance of this approach is optimized by numerically searching for the value of \( \gamma \) that maximizes \( \alpha_{\text{avg}} \) for each realization of \( \mathbf{h}_{AB} \) under the constraint that \( \text{Tr}(\Lambda') \leq P_T \).

IV. RESULTS

Solving the problem under the constraint that the distance \( d \geq d_{\text{min}} \) requires that we specify a model for the elements of \( \mathbf{C}_h \) 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 \( (\mu_{AE} = \mu_{AB} = 0) \) and 2) the power angular spectrum (PAS) defining the propagation conditions at Alice, Bob, and Eve is uniform in elevation angle \( \theta \) while satisfying the von Mises distribution in azimuth angle \( \phi \) [23], or

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

where \( \kappa \) specifies the angular distribution of the multipath departures or arrivals, \( \phi_p \) 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 \( \kappa \) increases. As the multipath environment becomes more directional with increasing \( \kappa \), 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 \( \mathbf{h}_{AB} \) 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 \( \mathbf{h}_{AB} \) 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 \( \mathbf{h}_{AB} \) 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 \( N_A = 5 \) half-wave dipoles with element separation \( \lambda/2 \), where \( \lambda \) is the wavelength, and therefore we neglect effects of mutual coupling on her array. The elements of the \( 5 \times 5 \) correlation matrix \( \mathbf{R}_A \) 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 \( 2 \times 2 \) matrix \( \mathbf{R}_{BE} \) 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 terminated (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]

\[
\mathbf{C}_h = \mathbf{R}_{BE} \otimes \mathbf{R}_A
\] (28)

where \( \otimes \) is a Kronecker product. Extracting \( \mathbf{C}_B \) from this result according to (6) and using the definition of \( \mathbf{C}_B \) in (7) indicates that we can form a random realization of \( \mathbf{h}_{AB} \) using \( \mathbf{h}_{AB} = \mathbf{C}^{1/2} \mathbf{h}_0 \), where \( \mathbf{h}_0 \) is an \( N_A \times 1 \) vector of independent, zero-mean, and unit-variance complex Gaussian random variables. Computing \( \mathbf{R}_E \) from \( \mathbf{C}_h \) and the realization of \( \mathbf{h}_{AB} \), 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 \( \mathbf{h}_{AB} \) (each with its corresponding \( \mathbf{R}_E \) as a function of \( d \)).

As mentioned in Section II-D, as part of our analysis, we wish to compare the value \( I_{SK}(\alpha_{\text{avg}}) \) obtained by substituting \( \alpha_{\text{avg}} \) in place of \( \alpha(\mathcal{R}) \) in (1) with the value \( E[I_{SK}] \) 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 \( \mathbf{h}_{AE} \) and averaging the resulting values of \( I_{SK} \). To obtain \( E[I_{SK}] \), we therefore must create multiple realizations of \( \mathbf{h}_{AE} \) conditioned on a single realization of \( \mathbf{h}_{AB} \). We do this by
computing $\bar{\mu}_{AE}$ and $\bar{C}_E^{1/2}$ from (9) to (10) and then creating channel realizations using $h_{AE} = \bar{C}_E^{1/2}h_0 + \bar{\mu}_{AE}$, where $h_0$ is an $N_A \times 1$ vector of independent, zero-mean, and unit-variance complex Gaussian random variables. In the results that follow, we realize 1000 channels $h_{AE}$ for each realization of $h_{AB}$.

All simulations use an available transmit power of $P_T = 1$ 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 $h_{AB}$ 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 $h_{AB}$. 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 $h_{AB}$ and $h_{AE}$ 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 $h_{AB}$ and $h_{AE}$ 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 $I_{SK}(\alpha_{avg})$ is close to the actual average $E\{I_{SK}\}$ 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 $E\{P_S\}$ and $E\{P_N\}$, respectively, for the same cases used in Fig. 2, where $P_S = \text{Tr}(R_S)$, $P_N = \text{Tr}(R_N)$, and the expectation is approximated using the sample mean over 1000 realizations of $h_{AB}$. These quantities, which should not be confused with the average signal and noise powers $P_{S,\xi}$ and $P_{N,\xi}$, $\xi \in \{B,E\}$, 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 $h_{AB}$. Because the elements of $h_{AB}$ are zero-mean unit-variance complex Gaussian random variables, $E\{|h_{AB}|^2\} = 5$, which accounts for received power levels greater than the transmit power level ($P_T = 1$). 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 $F_S(\phi)$ in (23) and noise pattern $F_N(\phi)$ in (24) as a function of the
azimuthal angle $\phi$ for a single representative channel $\mathbf{h}_{AB}$ with $d_{\text{min}} = 2.5\lambda$ 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 $P_{N,B} = 0$.

The suboptimal solution deliberately transmits the noise on the subspace orthogonal to the channel $\mathbf{h}_{AB}$, 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.

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 $\mathbf{h}_{AB}$ and that Eve will have inferior estimates of her channel $\mathbf{h}_{AE}$ and therefore less information regarding $\mathbf{h}_{AB}$ 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.