Secure Array Synthesis for Encryption Key Establishment in Multipath Channels

Rashid Mehmood*, Jon W. Wallace†, Michael A. Jensen*
* Electrical and Computer Engineering, Brigham Young University, Provo, UT, USA, r.mehmood@ieee.org, jensen@byu.edu
† Electrical and Computer Engineering, Lafayette College, Easton, PA, USA, wall@ieee.org

***Abstract*—This paper explores optimal array beamforming for establishing secret encryption keys through bidirectional channel estimation in multipath propagation environments. The problem is cast as a convex optimization of the average secure key rate achieved in the presence of a passive eavesdropper, and the optimization is performed using semi-definite programming. Representative results demonstrate that, compared to a conventional but suboptimal beamforming solution, the optimal solution achieves significantly higher key establishment performance, with the relative performance improvement increasing with the transmit correlation.**

I. Introduction

The large volume of sensitive data transmitted over wireless links motivates research on communication security, such as the establishment of secret encryption keys by exploiting the reciprocal nature of electromagnetic propagation [1–3]. Recent work has demonstrated a technique for constructing transmit and receive beamformers that maximize the rate at which secret keys can be established in the presence of an eavesdropper in line-of-sight (LOS) channels [4] or when the eavesdropper is ignored in multipath channels [5]. The objective of this paper is to formulate beamformers for key establishment in multipath channels when the eavesdropper is considered. The approach expresses the secure key rate as a function of the correlation matrix for the multi-antenna channels observed by the legitimate node and a proximate eavesdropper and then finds the optimal transmit covariance matrix using semi-definite programming (SDP) [6]. Numerical results and comparisons with a conventional but suboptimal method demonstrate the effectiveness of the technique.

II. Beamformer Covariance Optimization

Figure 1 shows a scenario in which Alice uses N_{A} antennas to communicate with Bob in the presence of a passive eavesdropper Eve, where Bob and Eve each have a single antenna. The channels $\mathbf{h}_{\mathrm{AB}}$, $\mathbf{h}_{\mathrm{BA}}$, and $\mathbf{h}_{\mathrm{AE}}$ are $N_{\mathrm{A}} \times 1$ vectors that represent the complex baseband channel gains as illustrated in Fig. 1. We assume that Eve is close to Bob but that physical constraints ensure that Eve's antenna is at least a distance $d_{\min}$ from Bob's, effectively constraining the correlation observed between the channels $\mathbf{h}_{\mathrm{AB}}$ and $\mathbf{h}_{\mathrm{AE}}$.

We use $\mathbf{w}$ to represent the complex baseband beamformer vector transmitted from Alice's array with covariance $\mathbf{R} = \mathrm{E}\left\{\mathbf{w}\mathbf{w}^{\dagger}\right\}$, where $\{\cdot\}^{\dagger}$ indicates a conjugate transpose and $\mathrm{E}\{\cdot\}$ is an expectation. We constrain $\mathbf{R}$ to satisfy $\mathrm{Tr}(\mathbf{AR}) \leq P_{\mathrm{T}}$, where $\mathrm{Tr}(\cdot)$ is a trace, $\mathbf{A}$ is a coupling matrix [7], and P_{T} is the available transmit power. Our objective is to find the matrix $\mathbf{R}$ that maximizes the *secure key rate* I_{SK}, which is defined as the maximum number of key bits that can be securely generated per observation of the reciprocal channel in the presence of Eve. Mathematically, I_{SK} is given by [4]

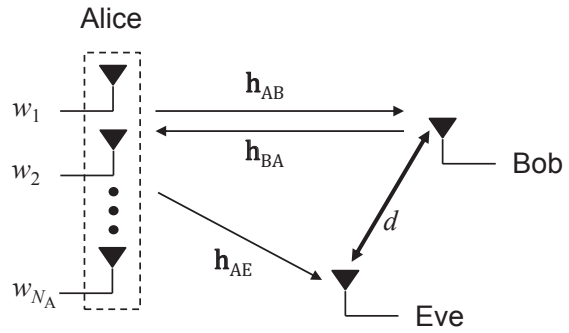

Fig. 1. System diagram where Alice transmits to Bob's single antenna using an antenna array. Eve observes the transmission using a single antenna that is separated from Bob's antenna by the distance d.

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

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

where $\sigma_{\xi}^2 = \mathbf{h}_{\mathrm{A}\xi}^{\mathrm{T}}\mathbf{R}\mathbf{h}_{\mathrm{A}\xi}^{*}$ for $\xi \in [\mathrm{B},\mathrm{E}]$, $\sigma_{\mathrm{BE}} = \mathbf{h}_{\mathrm{AB}}^{\mathrm{T}}\mathbf{R}\mathbf{h}_{\mathrm{AE}}^{*}$, $\{\cdot\}^{\mathrm{T}}$ and $\{\cdot\}^{*}$ respectively indicate transpose and conjugate, and σ_0^2 is the channel estimation error variance.

Optimizing I_{SK} requires finding the covariance $\mathbf{R}$ that maximizes $\alpha(\mathbf{R})$. Since in a multipath channel Alice cannot know the channel to Eve, Alice must perform her optimization based on the possible statistical *correlation* between the known $\mathbf{h}_{\mathrm{AB}}$ and unknown $\mathbf{h}_{\mathrm{AE}}$, suggesting that we use the average of I_{SK} as our optimization criterion. Rather than approximating the expectation of (1) using a costly sample mean over a large number of random channel realizations, we resort to a simpler optimization objective: finding the beamformer covariance $\mathbf{R}$ *for a fixed* $\mathbf{h}_{\mathrm{AB}}$ that maximizes the minimum *average* value of $\alpha(\mathbf{R})$ over all possible locations of Eve satisfying $d > d_{\min}$. This optimization uses the correlation matrix $\mathbf{R}_{\mathrm{E}} = \mathrm{E}\left\{\mathbf{h}_{\mathrm{AE}}\mathbf{h}_{\mathrm{AE}}^{\dagger}\right\}$ which is based on the statistics of $\mathbf{h}_{\mathrm{AE}}$ conditioned on a specific observation of $\mathbf{h}_{\mathrm{AB}}$.

We have previously demonstrated how to use SDP to determine the beamformer covariance $\mathbf{R}$ that maximizes the minimum value of $\alpha(\mathbf{R})$ observed over all possible angular positions of Eve for the LOS propagation environment and under the constraint that $\mathbf{R}$ is positive semi-definite and $\mathrm{Tr}(\mathbf{AR}) \leq P_{\mathrm{T}}$ [4]. For the multipath scenario of interest in this work, we can use the identical SDP framework, with the objective of optimizing the average value of $\alpha(\mathbf{R})$. Specifically, we construct the correlation matrix $\mathbf{R}_{\mathrm{E}}$ for each of a large set of positions for Eve (i.e. values of $d > d_{\min}$), and we then use SDP to determine the value of $\mathbf{R}$ that maximizes the minimum value of $\mathrm{E}\{\alpha(\mathbf{R})\}$ over all values of d.

We also create a suboptimal array synthesis approach in which the training data used for channel estimation is transmitted using the beamformer that maximizes power at Bob and artificial noise is transmitted uniformly on the orthogonal complement to the signal beamformer. The beamformer and its orthogonal complement are found using the singular value decomposition $\mathbf{h}_{\mathrm{AB}} = \mathbf{U}\mathbf{\Lambda}\mathbf{V}^{\dagger}$. The transmit covariance is then formed according to $\mathbf{R} = \mathbf{U}\mathbf{\Lambda}'\mathbf{U}^{\dagger}$, where $\mathbf{\Lambda}' = \mathrm{diag}(\gamma, \gamma', \ldots, \gamma')$, $\gamma' = (1-\gamma)/(N_{\mathrm{a}}-1)$, γ is the signal power and γ' is the noise power applied to each noise beamforming vector. The performance of the suboptimal approach is maximized by numerically finding γ for each realization of $\mathbf{h}_{\mathrm{AB}}$ under the constraint that $\mathrm{Tr}(\mathbf{\Lambda}') \leq P_{\mathrm{T}}$.

III. Results

While our optimization is general for any channel, here we assume that 1) the channels are zero-mean Gaussian random variables and 2) the power angular spectrum defining the propagation environment at Alice, Bob, and Eve satisfies the von Mises distribution, leading to closed-form expression of the required spatial correlation matrices [8]. We first form the $N_{\mathrm{A}} \times N_{\mathrm{A}}$ correlation matrix $\mathbf{R}_{\mathrm{A}}$ for Alice's array and the 2×2 matrix $\mathbf{R}_{\mathrm{BE}}$ representing the correlation between Bob's and Eve's antennas. Since our channels are zero-mean, we write $\mathbf{C}_{\mathrm{h}} = \mathbf{R}_{\mathrm{BE}} \otimes \mathbf{R}_{\mathrm{A}}$, where $\otimes$ is a Kronecker product, and form $\mathbf{C}_{\mathrm{B}}$ as the upper left $N_{\mathrm{A}} \times N_{\mathrm{A}}$ partition of $\mathbf{C}_{\mathrm{h}}$. Finally, we generate a specific 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, unit-variance complex Gaussian random variables. In our model, κ controls the angular distribution of the multipath departures/arrivals, and we use either $\kappa = 2$ (medium transmit correlation) or $\kappa = 10$ (high transmit correlation) when constructing $\mathbf{R}_{\mathrm{A}}$ at Alice and $\kappa = 2$ when constructing $\mathbf{R}_{\mathrm{BE}}$ at Bob and Eve. Furthermore, Alice has a ULA with element separation of $\lambda/2$ (λ is the wavelength).

Figure 2 presents the secure key rate I_{SK} averaged over 1000 realizations of $\mathbf{h}_{\mathrm{AB}}$ as a function of $d_{\min}$ for both high and medium correlation at Alice. As expected, an increase in the distance between Bob and Eve increases I_{SK} by reducing the correlation between $\mathbf{h}_{\mathrm{AB}}$ and $\mathbf{h}_{\mathrm{AE}}$. The results further show that 1) high correlation at Alice increases the correlation between $\mathbf{h}_{\mathrm{AB}}$ and $\mathbf{h}_{\mathrm{AE}}$ and therefore reduces I_{SK} and 2) the optimal solution obtained using SDP significantly outperforms the suboptimal approach, with the relative improvement increasing with the transmit correlation.

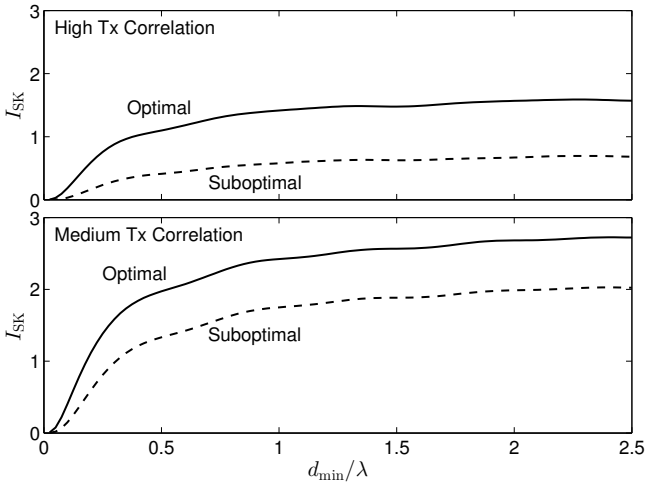

Fig. 2. Average secure key rate for both high and medium transmit correlation as a function of minimum distance $d_{\min}$ between Bob and Eve.

IV. Conclusion

This paper demonstrates an approach for synthesizing optimal transmit beamformers that maximize the secure key rate achieved when using reciprocal channel estimates for secret key establishment. The method casts the key rate as a convex optimization and then uses semi-definite programming to find the transmit covariance matrix that maximizes a bound on the average secure key rate. Results demonstrate that the beamforming technique is effective at increasing the key rate over a practical but suboptimal transmission approach, particularly when the transmit correlation is high.

Acknowledgement

This work was supported in part by the U. S. Army Research Office under Grant # W911NF-12-1-0469.

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] J. W. Wallace, C. Chen, and M. A. Jensen, "Key generation exploiting MIMO channel evolution: algorithms and theoretical limits," in *3rd European Conference on Antennas and Propagation*, Berlin, Germany, Mar. 23-27 2009.

[3] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Computing*, vol. 10, pp. 205–215, Feb. 2011.

[4] R. Mehmood, J. W. Wallace, and M. A. Jensen, "Secure array synthesis," *IEEE Trans. Antennas Propag.*, vol. 63, pp. 3887–3896, Sep. 2015.

[5] B. T. Quist and M. A. Jensen, "Optimal channel estimation in beamformed systems for common-randomness-based secret key establishment," *IEEE Trans. Inf. Forensics and Security*, vol. 8, pp. 1211–1220, Jul. 2013.

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

[7] J. W. Wallace and M. A. Jensen, "Mutual coupling in MIMO wireless systems: A rigorous network theory analysis," *IEEE Trans. Wireless Commun.*, vol. 3, pp. 1317–1325, July 2004.

[8] 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 Transactions on Vehicular Technology*, vol. 51, no. 3, pp. 425–434, May 2002.