Optimal Array Signaling for Key Establishment in Static Multipath Channels

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

***Abstract*—This paper explores optimal array beamforming for secure communication in static 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. While representative results are presented for a uniform linear array, the optimization procedure can be generalized to any array topology.**

I. Introduction

The broadcast nature of wireless transmission leaves the communication vulnerable to a wide variety of attacks that can compromise security. Generally, data security is ensured by encrypting the communication between the participating nodes using a secret encryption key. While there are different methods to generate encryption keys, one relatively recent proposal is to employ common randomness available in the wireless channel to generate the key, a technique that falls within the broad area of physical layer security. For time-varying propagation conditions, a long encryption key can be generated from multiple channel observations [1]. However such methods have limitations if the propagation channel is static or line-of-sight (LOS) due to the limited randomness available for key generation.

We previously studied key establishment in static LOS channels and showed how an adaptive array can be used to optimally excite the spatial degrees of freedom available, thus enabling the secure establishment of long encryption keys in non-fading channels in the presence of an eavesdropper [2]. In this work, we extend the method to the case of a static *multipath* channel. The channel is modeled by assuming a specific power angular spectrum (PAS) at the nodes, and the optimization procedure maximizes the secure key generation rate for the worst-case position of an eavesdropper.

II. Information Theoretic Analysis

Figure 1 shows the communication scenario in which Alice and Bob are legitimate nodes and Eve is a potential eavesdropper. We assume that Alice employs an adaptive array while Bob and Eve each have only a single antenna. We further assume that Eve is close to Bob such that there can be correlation between the channel from Alice to Bob and the channel from Alice to Eve. Although the method is general with respect to the array topology and antenna types, we will concentrate on an illustrative example where all antennas are half-wave dipoles and Alice's array is a uniform linear array (ULA) with N_a elements and $\lambda/2$ inter-element spacing. Throughout the analysis, it is assumed that the minimum distance between Bob's and Eve's antennas is d_min.

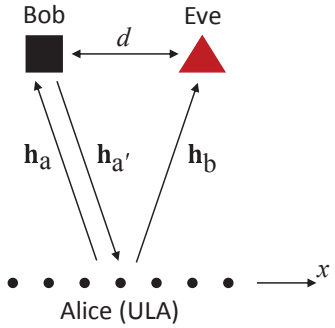

Fig. 1. System diagram where Alice is equipped with a ULA of half-wave dipoles while Eve and Bob each have a single half-wave dipole separated by distance d.

Because we assume static channels, we create channel randomness through Alice's time-variant excitation of the channel spatial degrees of freedom. Let $\mathbf{w}$ represent the vector of beamforming weights applied to Alice's array and $\mathbf{R} = \mathrm{E}\left\{\mathbf{w}\mathbf{w}^\dagger\right\}$ represent its covariance, where $\{\cdot\}^\dagger$ is a conjugate transpose and $\mathrm{E}\{\cdot\}$ is the expectation. Bob and Eve then observe signals with variances $\sigma_\mathrm{a}^2 = \mathbf{h}_\mathrm{a}\mathbf{R}\mathbf{h}_\mathrm{a}^\dagger$ and $\sigma_\mathrm{b}^2 = \mathbf{h}_\mathrm{b}\mathbf{R}\mathbf{h}_\mathrm{b}^\dagger$ respectively and with correlation $\sigma_\mathrm{ab} = \mathbf{h}_\mathrm{a}\mathbf{R}\mathbf{h}_\mathrm{b}^\dagger$. Assuming Gaussian signaling, the number of bits I_SK generated per channel observation that can be kept secure from an eavesdropper for static channels is given as [2] as

$$I_\mathrm{SK} = -\log_2 \beta\,(2-\beta) \tag{1}$$

$$\beta = \frac{1}{1 + \underbrace{\left[\sigma_\mathrm{a}^2\sigma_\mathrm{b}^2 - |\sigma_\mathrm{ab}|^2\right]/\sigma_\mathrm{b}^2\sigma_0^2}_{\alpha}}, \tag{2}$$

where σ_0^2 is the noise variance at Alice and Bob (Eve's receiver is assumed noiseless). Since I_SK depends monotonically on α, maximizing α will maximize I_SK.

Consistent with the scenario in [2], we assume that Eve can be no closer to Bob than d_min, since when Eve is too close, very little additional security is possible using physical layer techniques. However, in the LOS scenario considered in [2], Alice knows the channel that Eve would observe as a function of Eve's position and therefore can optimize the channel estimation to minimize I_SK over *all* possible Eve locations. In contrast, in this multipath channel Alice cannot know the channel to Eve for any of her positions, and therefore Alice must perform her optimization based on the possible statistical *correlation* between the Alice-to-

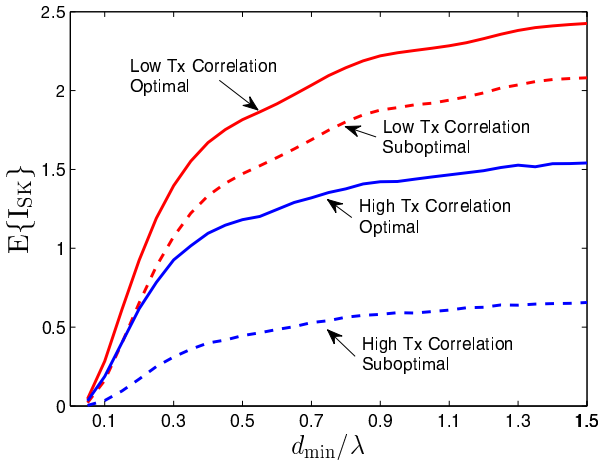

Fig. 2. Average secure key rate for both low and high transmit correlation as a function of minimum distance between Bob and Eve. The dashed lines corresponds to the sub-optimal results.

Bob and Alice-to-Eve channels, meaning that $\sigma_{\rm b}^2$, $\sigma_{\rm ab}$, and $I_{\rm SK}$ are random variables. Although there are many possible optimization criteria, in this work we maximize the minimum expected value of α over all possible locations for Eve, as this should lead to high $I_{\rm SK}$. Mathematically we have

$$\mathrm{E}\{\alpha\} = \frac{\sigma_{\rm a}^2 \mathrm{E}\{\sigma_{\rm b}^2\} - \mathrm{E}\{|\sigma_{\rm ab}|^2\}}{\mathrm{E}\{\sigma_{\rm b}^2\}\sigma_0^2}, \qquad (3)$$

where $\mathrm{E}\{\sigma_{\rm b}^2\} = \mathrm{Tr}\{\mathbf{R}\mathbf{R}_{\rm b}^*\}$, $\mathrm{E}\{|\sigma_{\rm ab}|^2\} = \mathbf{h}_{\rm a}\mathbf{R}\mathbf{R}_{\rm b}^*\mathbf{R}^\dagger\mathbf{h}_{\rm a}^\dagger$, $\mathbf{R}_{\rm b} = \mathrm{E}\{\mathbf{h}_{\rm b}\mathbf{h}_{\rm b}^\dagger\}$, and $\mathrm{Tr}\{\cdot\}$ is the trace.

III. Analysis and Results

The goal of our optimization is to find the value of $\mathbf{R}$ for a fixed $\mathbf{h}_{\rm a}$ that maximizes the minimum value of $\mathrm{E}\{\alpha\}$ over all possible locations of Eve satisfying $d > d_{\rm min}$. To model the correlation between the Alice-to-Bob and Alice-to-Eve channels we use the von Mises distribution for the PAS at Alice and Bob/Eve. This PAS results in a closed form expression for the spatial correlation [3] given by

$$\rho(\Delta) = \frac{I_0(\sqrt{\kappa^2 - 4\pi^2\Delta^2 + j4\pi\kappa\cos(\theta_p)\Delta})}{I_0(\kappa)}, \qquad (4)$$

where Δ is the electrical distance between antennas, κ defines the angular distribution of the multipath departures or arrivals, θ_p is the mean angle of arrival/departure (assumed to be 0 in our analysis) 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. If we have both transmit and receive correlation, the Kronecker model can be used to generate channels with the specified correlation according to

$$\begin{bmatrix}\mathbf{h}_{\rm a} \\ \mathbf{h}_{\rm b}\end{bmatrix} = \mathbf{R}_{\rm r}^{1/2}\mathbf{H}'\mathbf{R}_{\rm t}^{1/2} \qquad (5)$$

where $\mathbf{R}_{\rm t}$ and $\mathbf{R}_{\rm r}$ are $N_{\rm a} \times N_{\rm a}$ transmit and 2×2 receive correlation matrices, respectively, and $\mathbf{H}'$ is a $2 \times N_{\rm a}$ zero-mean complex Gaussian distributed random matrix. We emphasize that the separation between Alice's antennas is fixed at $\lambda/2$ while the distance d between Eve's antenna and Bob's antenna is variable.

In this analysis, we use $\kappa = 0$ (low transmit correlation) and $\kappa = 10$ (high transmit correlation) at Alice. At Bob/Eve we assume that $\kappa = 2$. We then use semidefinite programming (SDP) to find the optimal value of $\mathbf{R}$ when $d > d_{\rm min}$. To achieve this SDP solution, we express $\mathbf{R}$ as a weighted sum over a complete set of basis matrices and find the basis weights that maximize the minimum value of $\mathrm{E}\{\alpha\}$. The final solution is obtained using the *Maxdet* programming package [4]. Figure 2 presents the resulting value of $I_{\rm SK}$ averaged over 1000 realizations of $\mathbf{h}_{\rm a}$ as a function of $d_{\rm min}$ for both high and low transmit correlation. As expected, an increase in the distance between Bob and Eve increases $I_{\rm SK}$ by reducing the receive correlation between $\mathbf{h}_{\rm a}$ and $\mathbf{h}_{\rm b}$. The results further show that high transmit correlation notably reduces $I_{\rm SK}$.

We compare our results to those from a suboptimal approach in which signal (the secret key) is transmitted on the dominant dimension of the Alice-to-Bob channel and artificial noise is transmitted uniformly on the orthogonal complement to the dominant dimension, where the dominant dimension and its orthogonal complement are found using the singular value decomposition (SVD) $\mathbf{h}_{\rm a} = \mathbf{U}\mathbf{\Lambda}\mathbf{V}^\dagger$. The transmit covariance is then formed according to $\mathbf{R} = \mathbf{V}\mathbf{\Lambda}'\mathbf{V}^\dagger$, where $\mathbf{\Lambda}' = \mathrm{diag}(\gamma, \gamma', \ldots, \gamma')$, and $\gamma' = (1-\gamma)/(N_{\rm a}-1)$. The performance of the suboptimal approach is maximized by numerically searching for the optimal value of γ for each realization of $\mathbf{h}_{\rm a}$. Figure 2 compares the optimal solution found using SDP to that obtained from this suboptimal SVD approach. The results show that the optimal approach significantly outperforms the suboptimal approach, with the relative improvement increasing with the transmit correlation.

IV. Conclusion

The objective of this work is to use array beamforming to maximize the average secure key rate for two nodes communicating in a static multipath environment in the presence of a passive eavesdropper. The solution is formed by using semidefinite programming to maximize an auxiliary parameter that in turn impacts the key rate. Comparison of results produced by this optimization with those obtained from a suboptimal approach demonstrates that the optimization can significantly improve the realized secure key rate in realistic multipath scenarios.

Acknowledgement

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

References

[1] Ueli M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, Aug. 1993.

[2] Rashid Mehmood, Jon W. Wallace, and Michael A. Jensen, "Optimal array patterns for encryption key establishment in LOS channels," in *2014 IEEE Antennas and Propagation Society International Symposium (APS'14)*, Memphis, TN, USA, July 6-11, 2014, pp. 478–479.

[3] Ali Abdi, Janet A. Barger, and Mostafa 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.

[4] S. P. Wu, L. Vandenberghe, and S. Boyd, *Software for Determinant Maximization Problems*, 1996.