Optimal Array Patterns for Encryption Key Establishment in LOS Channels

Rashid Mehmood, Jon W. Wallace and Michael A. Jensen
Brigham Young University
Provo, UT, USA
E-mail: r.mehmood@ieee.org, wall@ieee.org, jensen@byu.edu

***Abstract*—While the establishment of secret encryption keys based on reciprocal electromagnetic propagation has received recent attention, very limited work has appeared regarding how multiantenna radios should conduct the required channel estimation in the presence of an eavesdropper. This paper demonstrates array beamforming that maximizes the number of bits that can be established when an eavesdropper observes the channel estimation process.**

I. Introduction

The establishment of secret encryption keys based on observations of reciprocal electromagnetic propagation is an intriguing technique that has received recent attention [1]. Strengths of this approach include the fact that it uses a physical random phenomenon as opposed to a pseudo-random number generator for key generation and that it avoids the necessity of protocols such as the Diffie-Hellman exchange. While this technique is interesting, uncertainty remains regarding how the legitimate radios should conduct their channel estimation protocol to minimize the information accessible by an attacker when its channels to the legitimate radios are correlated with the reciprocal channel used for key establishment.

This paper assumes that one of the legitimate nodes possesses a uniform linear array (ULA) and considers the array radiation patterns that should be used for estimation of a line-of-sight (LOS) channel to minimize information leaked to a nearby attacker. Much like for multiple-input multiple-output communication where optimal array pattern synthesis is accomplished by maximizing the mutual information between the transmitted and received signals, in our case the pattern synthesis is performed by maximizing the *secure key rate*, which is an information-theoretic quantity indicating the number of key bits that can be established between the two nodes that are secure from the attacker.

II. Information Theoretic Analysis

Figure 1 shows the communication scenario in which Alice and Bob are legitimate nodes wishing to establish secure communication and Eve is an eavesdropper. In our scenario, Eve and Bob each have a single half-wave dipole while Alice has a ULA of N_a half-wave dipoles. We assume that Bob and Eve lie on the same circle centered at Alice but that Eve cannot lie within a small *exclusion zone* around Bob.

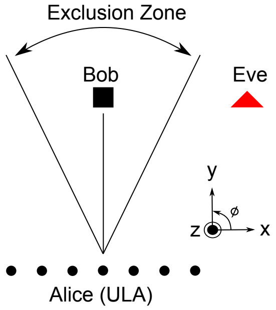

Fig. 1. System diagram where Alice is equipped with a ULA of half-wave dipoles while Eve and Bob each have a single half-wave dipole. Eve is located outside of the exclusion zone.

We define the secure key rate I_SK as the number of key bits that can be generated per channel observation that remain secure from Eve. This quantity is computed using

$$I_\mathrm{SK} = I(\hat{\mathbf{h}}_\mathrm{a}; \hat{\mathbf{h}}_{\mathrm{a}'} | \hat{\mathbf{h}}_\mathrm{b}, \hat{h}_\mathrm{c}) \tag{1}$$

where $I(\cdot;\cdot)$ is the mutual information, $\hat{\mathbf{h}}_\mathrm{a}$ and $\hat{\mathbf{h}}_{\mathrm{a}'}$ are the reciprocal multiantenna channels estimated at Alice and Bob respectively, and $\hat{\mathbf{h}}_\mathrm{b}$ and $\hat{h}_\mathrm{c}$ are Eve's estimates of the channel from Alice and Bob respectively. Because of the geometrical arrangement, the channel $\hat{h}_\mathrm{c}$ does not provide useful information to Eve and is therefore ignored.

If the channel coefficients satisfy Gaussian distributions, then (1) can be computed in closed form based on the covariances of the relevant channels [2]. We can simplify this computation by recognizing that Alice will apply beamformers during the channel estimation process so that the effective channels from Alice to Bob and from Alice to Eve are scalar quantities. We assume that Alice and Bob observe the same signal-to-noise ratio (SNR) and that Eve's receiver is noiseless (worst case). The secure key rate then reduces to

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

$$\beta = \frac{1}{1 + \underbrace{\left[\sigma_\mathrm{a}^2\sigma_\mathrm{b}^2 - |\sigma_\mathrm{ab}|^2\right]/\sigma_\mathrm{b}^2\sigma_0^2}_{\alpha}} \tag{3}$$

where σ_a^2 and σ_b^2 are the variances of the scalar channels to Bob and Eve respectively, σ_ab is the covariance between these scalar channels, and σ_0^2 is the estimation error variance.

Let $\mathbf{w}$ represent the vector of beamforming weights applied to Alice's array with $\mathbf{R} = \mathrm{E}\{\mathbf{w}\mathbf{w}^\dagger\}$ representing the covariance of this transmission vector, where $\mathrm{E}\{\cdot\}$ is an expectation

978-1-4799-3540-6/14/$31.00 ©2014 IEEE

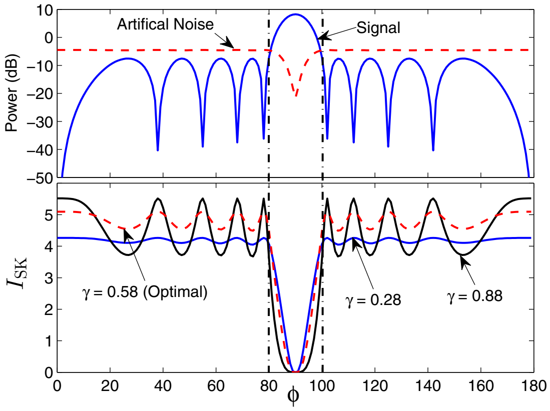

Fig. 2. Illustration of sub-optimal pattern synthesis based on transmitting a channel estimation signal on one pattern and artificial noise on others along with the achieved secure key rate I_{SK} for Bob at broadside ($\phi = 90°$) and Eve at any angle outside the exclusion zone around Bob.

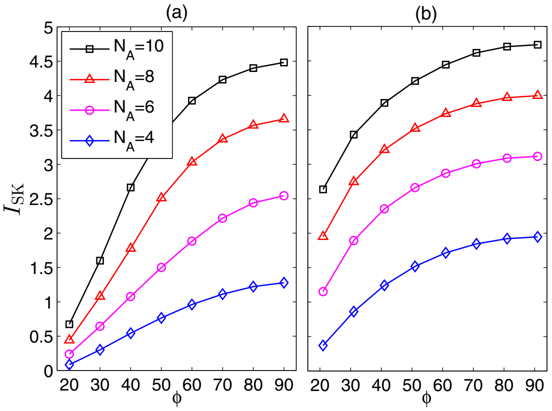

Fig. 3. Minimum value of I_{SK} as a function of the angle of Bob's position for different numbers of antenna elements N_{a} in Alice's array: (a) sub-optimal pattern synthesis and (b) optimal pattern synthesis based on semi-definite programming.

and $\{\cdot\}^{\dagger}$ is a conjugate transpose. We can express α in (3) directly in terms of $\mathbf{R}$, and our objective is to determine the form of $\mathbf{R}$ that achieves some optimal behavior of I_{SK}.

III. Analysis and Results

The objective of finding an effective form of $\mathbf{R}$ is perhaps best illustrated using a simple yet sub-optimal example. Specifically, we form the unit-length vector $\mathbf{w}_{\mathrm{s}}$ as the normalized Dolph-Chebyshev weights that steer the pattern main beam toward Bob and apply a signal to this beamformer with average power p_{s} from which the nodes can estimate their channels. We then form $N_{\mathrm{a}} - 1$ orthonormal vectors that are orthogonal to $\mathbf{w}_{\mathrm{s}}$ and apply artificial noise signals to each of these beamformers with average power $p_{\mathrm{n}}/(N_{\mathrm{a}} - 1)$, with this artificial noise designed to reduce Eve's ability to estimate her channel. The vector $\mathbf{w}$ is taken as the signal-weighted sum of these vectors from which $\mathbf{R}$ can be computed. We then numerically find the ratio $\gamma = p_{\mathrm{s}}/p_{\mathrm{n}}$ that maximizes the minimum value of I_{SK} when Eve's angle is swept over the range outside of the exclusion zone.

The top plot in Figure 2 plots the pattern used for the channel estimation signal assuming Bob is broadside to the array ($\phi = 90°$) and the weighted sum of the other radiation patterns for $N_{\mathrm{a}} = 10$ elements in the ULA, a 20° exclusion zone, and $\gamma = 0.58$ (optimal). As can be seen, Bob observes more signal power than artificial noise while Eve observes more artificial noise than signal power over her entire range of possible angles. The bottom plot shows the value of I_{SK} for different values of γ, revealing that the optimal value of $\gamma = 0.58$ achieves the largest minimum value of I_{SK} outside the exclusion zone.

Figure 3(a) plots the minimum value of I_{SK} observed over all of Eve's possible angles as a function of Bob's angle with respect to the array ($\phi = 90°$ for broadside and $\phi = 0°$ for endfire) for several values of N_{a}. The results demonstrate that as the beamforming capabilities of the array are reduced through reduction in the number of elements N_{a} or because Bob moves towards the endfire direction, I_{SK} decreases.

This approach does not guarantee an optimal solution, and we therefore develop an optimal solution by forming $\mathbf{R}$ as a weighted sum over a complete set of basis matrices and expressing α in terms of the sum coefficients. We then densely sample this expression with respect to Eve's angle, producing a system of equations that can be formulated for solution using semi-definite programming [3]. The solution that maximizes the minimum value of α (and therefore I_{SK}) is obtained using the *Maxdet* programming package [4].

Figure 3(b) repeats the computation shown in Figure 3(a) using the optimal solution approach. When Bob is near broadside, the sub-optimal but simpler approach yields results that are similar to those obtained using the optimal synthesis method. However, as Bob moves toward endfire, the optimal pattern synthesis produces dramatically improved values of I_{SK}, with achieved values as much as 4 times larger than those obtained from the sub-optimal approach.

IV. Conclusion

This paper demonstrates an optimal approach for synthesizing array radiation patterns that maximize the secure key rate achieved in a LOS channel when an eavesdropper observes the key establishment protocol. By using semi-definite programming, the convex optimization can be efficiently completed, with the results obtained showing dramatic improvement over results achieved using a simple intuitive key establishment approach. Future work involves extending this analysis to other array configurations and multipath propagation environments.

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 and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 381–392, 2010.

[3] L. Vandenberghe and S. Boyd, "Semidefinite programming," *SIAM Review*, vol. 38, pp. 49–95, 1996.

[4] S. P. Wu, L. Vandenberghe, and S Boyd, "Software for determinant maximization problems," http://www.stanford.edu/~boyd/old_software/maxdet/, 1996.