Network Model for Evaluating the Performance of Reciprocal Channel-Based Key Establishment with Coupled Antennas

Attiya Mahmood and Michael A. Jensen

Department of Electrical and Computer Engineering, Brigham Young University
459 Clyde Building, Provo, UT 84602, USA
Email: attiya@byu.edu, jensen@byu.edu

Abstract

Prior work on multi-antenna wireless communication has produced practical yet rigorous signal models that can account for the impact of antenna array mutual coupling and sophisticated circuit noise contributions. However, these models have not yet been extended to the case of systems that generate secret encryption keys based on the reciprocal electromagnetic propagation of multipath channels. This work performs this extension, building upon previously developed network models and augmenting them to accommodate considerations unique to the key establishment protocol. Simulation results demonstrate the impact on the achievable performance of mutual coupling and of the impedance matching network that interfaces the coupled array to the accompanying circuitry.

1. Introduction

Theoretical analyses and practical protocol implementations have demonstrated the concept of using reciprocal electromagnetic propagation as a basis for establishing secret encryption keys [1, 2]. Recent studies have shown that when multiple-antenna radios are used for such key establishment, the *key rate*, or the number of bits that can be generated for each channel estimate, can be increased [2, 3]. However, these prior studies have largely ignored the impact of antenna mutual coupling on the achievable key establishment performance.

This paper formulates a network model for coupled antennas based on the work in [4] and applies the model to analyze the impact of mutual coupling and impedance matching between the array and the terminations on the key rate. Results for a 2×2 multiple-input multiple-output (MIMO) system using half-wave dipole antennas demonstrate that high coupling significantly changes the performance and makes the achievable key rate highly dependent on the impedance matching objective.

2. Network Model

Figure 1 shows the network model used in the analysis detailed in this paper. To maintain simplicity, the transmitter is assumed to consist of a single uniform linear array of half-wave dipoles with half-wavelength element spacing. The receive array is also a uniform linear array of dipoles, but the element spacing can vary. The transmit and receive dipole arrays are characterized in terms of their open-circuit radiation patterns and the full impedance matrix using NEC. The radiation patterns are used in conjunction with a path-based propagation model to construct the channel transfer matrix $\mathbf{H}$, each element of which represents the channel transfer function between the open-circuit voltage at the mth receive antenna and the current applied to the nth transmit antenna with all other antennas terminated in an open circuit. The computed impedance matrices are then used to construct the S-parameter matrices $\mathbf{S}_{TT}$ and $\mathbf{S}_{RR}$ for the transmit and receive arrays, respectively.

Each block in the diagram of Figure 1 is characterized by a matrix of S-parameters. The receiver amplifiers and loads are assumed uncoupled so that their S-parameter matrices are block diagonal. However, because the S-parameter matrix for the receive array is in general a full matrix, we allow the matching network to also have an S-parameter matrix that is in general full to potentially compensate for the impacts of antenna array coupling.

The nth element of the vector $\mathbf{v}_T$ represents the voltage applied to the nth transmit antenna, while the mth element of the vector $\mathbf{i}_L$ represents the current flowing through the mth receive load. Because reciprocity applies between transmit voltages and receive currents, the network formulation generates a transfer admittance matrix between these quantities. The model incorporates a realistic representation of the amplifier noise that results in some spatial noise correlation as a result of coupling through the antennas [4].

978-1-4673-5225-3/14/$31.00 ©2014 IEEE

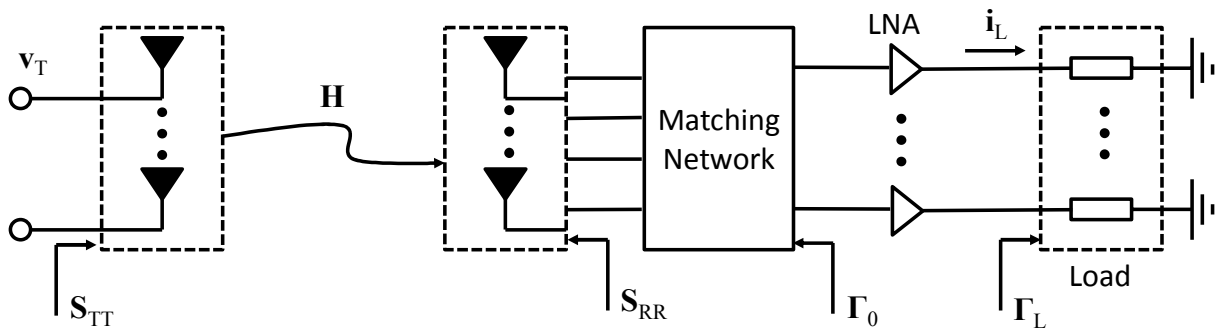

Figure 1: Block diagram of the network model used in the analysis of key rate performance with receive array mutual coupling.

To formulate the key rate, which is the number of bits that can be generated from an observed channel, we need to translate the signal and noise characteristics at the receiver to the covariance of the error between the true channel transfer admittance and the estimated channel. This can be accomplished using the Cramer-Rao Bound, which has been formulated for this MIMO scenario [5]. This coupled with the spatial covariance of the end-to-end channel allows computation of the key rate.

3. Results

All computations assume two transmit and two receive antennas. The transfer admittance matrix is computed for the case where the transmit and receive antenna elements are spaced 10λ apart, where λ is the free-space wavelength. Assuming that the output reflection coefficient matrix of the matching network is $\mathbf{\Gamma}_0 = 0$, we find the normalization constant such that the average of the squares of the computed transfer admittance matrix elements is unity. We then compute the amplifier noise parameters to achieve a signal-to-noise ratio (SNR) of 15 dB. The normalization constant is then applied to other antenna separation and receiver matching conditions so that the results include the impact of these parameters on key rate performance. The computations use 10,000 realizations of the channel where a channel consists of a set of multipaths each characterized by an angle of departure, angle of arrival, and complex gain drawn from statistical distributions. The results represent averages taken over the channel realizations.

Figure 2(a) plots the key rate as a function of receive antenna element spacing for the case where no mutual impedance is assumed (taking the diagonal elements of the impedance matrix only) and where the full mutual impedance matrix is used. The results assume 20 multipaths are used in the simulation and that the output reflection coefficient $\mathbf{\Gamma}_0$ is designed to achieve either minimum amplifier noise figure (*Optimal NF*) or maximum power transfer to the loads (*Optimal PT*). As can be seen, designing for minimum noise figure dramatically increases the achieved performance, as this minimizes the error in the resulting channel estimate. Furthermore, at small antenna spacing, the performance is notably impacted by the antenna mutual coupling. Figure 2(b) plots the same results as a function of the number of multipaths used assuming an antenna spacing of λ/4. These results reinforce the prior observation about the impact of mutual coupling and further demonstrate that increased multipath richness can increase the key rate performance.

4. Conclusion

This work has demonstrated the extension of network models accommodating antenna array mutual coupling for MIMO communications to the case of systems that extract secret key information from the reciprocal electromagnetic propagation channel. Simulation results using the technique show the impact of coupling and antenna impedance matching on the key establishment performance.

5. Acknowledgments

This work has been supported in part by the US Army Research Office through grant #W911NF-12-1-0469.

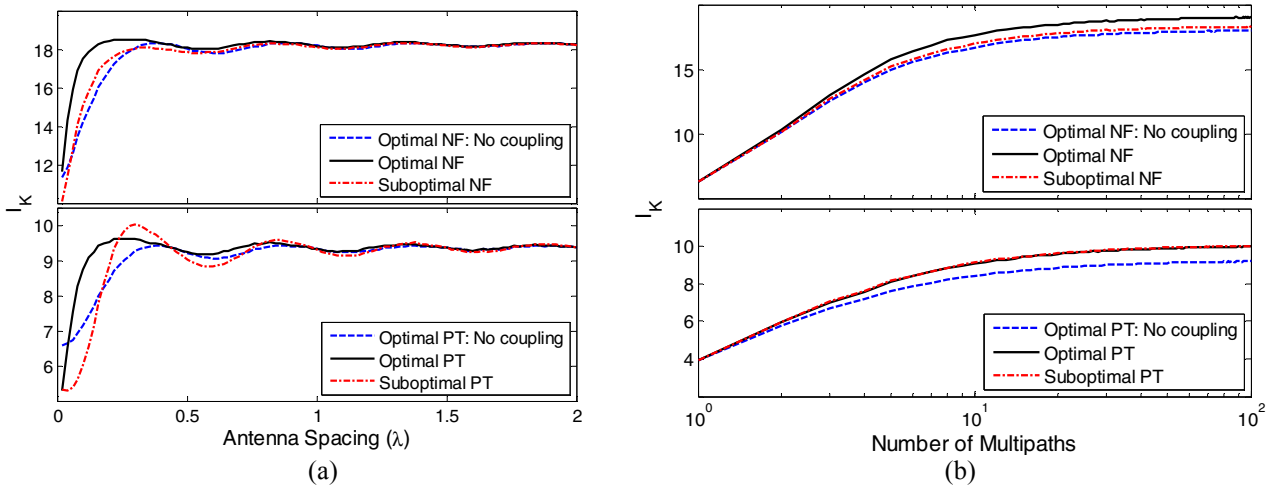

Figure 2: Key rate as a function of (a) receive antenna spacing assuming 20 multipaths and (b) number of multipaths assuming λ/4 receive antenna spacing for different receiver matching configurations and an SNR of 15 dB.

6. References

[1] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: measurement and analysis," *IEEE Trans. Inf. Forensics and Security*, vol. 5, pp. 381-392, Mar. 2010.

[2] 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.

[3] 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.

[4] M. L. Morris and M. A. Jensen, "Network model for MIMO systems with coupled antennas and noisy amplifiers," *IEEE Trans. Antennas Propag.*, vol. 53, pp. 545-552, Feb. 2005.

[5] T. K. Moon and W. C. Stirling, *Mathematical Methods and Algorithms for Signal Processing*, Prentice-Hall, 2000.