Measured Statistics of Reciprocal Channel Key Generation of Indoor MIMO Channels

Rajesh K. Sharma and Jon W. Wallace*
Jacobs University Bremen
School of Engineering and Science
Campus Ring 1, 28759 Bremen, Germany
ra.sharma@jacobs-university.de, wall@ieee.org

Introduction

There is growing interest in physical-layer security methods that exploit the random nature of the physical propagation channel to strengthen existing crypto-systems. In reciprocal channel key generation (RCKG), legitimate nodes (Alice and Bob) observe a common fluctuating channel to generate keys that are safe from the eavesdropper (Eve). Previous work [1, 2] derived expressions for the available key bits and those safe from an eavesdropper for MIMO systems with correlated complex Gaussian statistics. This paper applies these expressions to new MIMO measurements in indoor LOS and NLOS environments, indicating how propagation effects limit secure key generation and what key generation rates can be expected in practice.

MIMO Security Measurements

MIMO measurements were taken on the first floor of the Research I building on the Jacobs University Campus, depicted in Figure 1. A custom MIMO channel sounder fabricated at Jacobs University was employed that is functionally equivalent to the switched array architecture presented in [3], except for two important enhancements: (1) The new system employs custom FPGA-based A/D, allowing the required FFTs to be performed in real-time and channel data to be streamed continuously to disk. (2) Automatic gain control (AGC) is now purely digital.

Channels were measured with 23 dBm transmit power using a multitone signal with $N_F = 8$ tones and 10 MHz separation, centered at 2.55 GHz. Transmit (TX) and receive (RX) employed 8-element monopole antennas equivalent to those in [3]. At TX, antennas formed an 8-element uniform circular array (5.7 cm=0.47λ interelement spacing, where λ is the free-space wavelength at 2.55 GHz), but in our analysis, only 4 of the TX elements are usually considered (a semi-circle of adjacent elements), simulating Alice and Bob with the same number of antennas. RX antennas were partitioned into two separate 4-element square arrays (5 cm=0.43λ interelement spacing) to represent Alice and Eve.

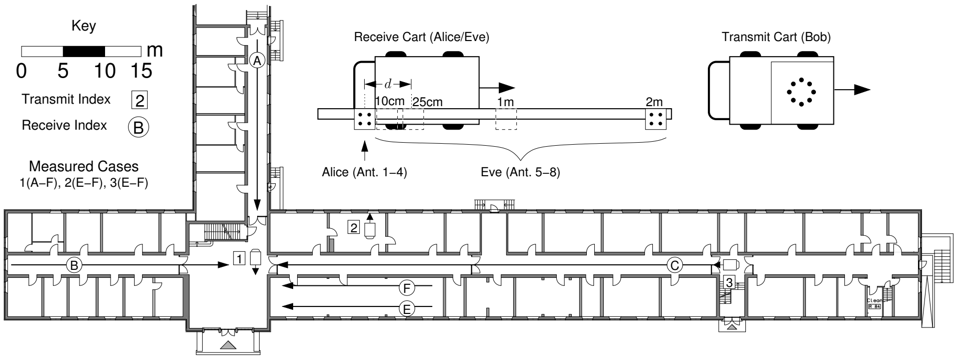

Figure 1: Ground floor of Research I on the Jacobs University campus. Boxed numbers indicate stationary transmit (Bob) positions, while circled letters indicate moving paths for the receiver (Alice/Eve).

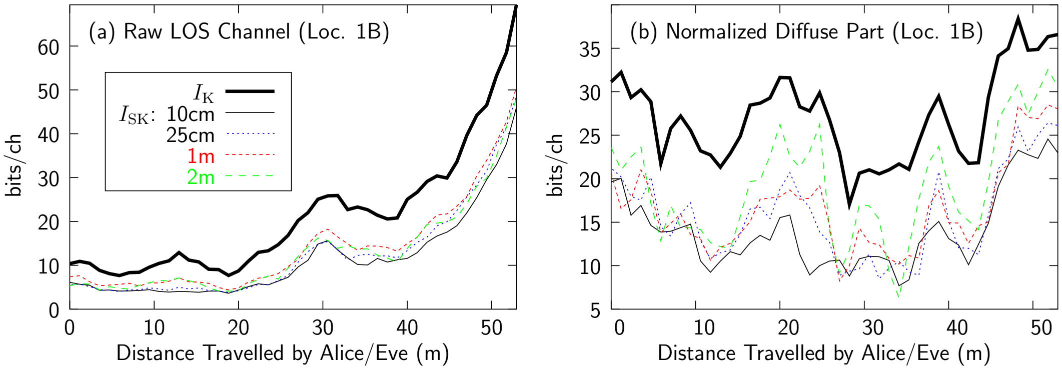

Figure 2: Available (I_{K}) and secret (I_{SK}) key bits for LOS Location 1B: computed for (a) raw channels, and (b) normalized channels with DCR

The sub-arrays were fixed to a long wooden plank 1.6 m off the ground, and Alice-Eve separation distances d of 10 cm, 25 cm, 1 m, and 2 m were investigated. TX remained stationary throughout each measurement and the RX was pushed along a straight path at approximately 0.3 m/s to obtain a time-varying channel response. For each TX/RX position, 8 measurements were taken, consisting of 2 trials for each of the 4 different Alice-Eve separations.

The raw channel snapshot for the ith receiver, jth transmitter, fth frequency, and nth temporal sample is denoted $h_{\mathrm{raw},ij}^{(f,n)}$, where $i \in [1,4]$ is Alice, $i \in [5,8]$ is Eve, and j is Bob's antenna index. $\mathbf{H}_{\mathrm{raw}}^{(f,n)}$ is normalized and possibly processed to obtain $\mathbf{H}^{(f,n)}$. A time series of channel covariances is obtained by dividing temporal snapshots into 10λ blocks having N_B=1297 samples each, and computing the full channel covariance for block n as

$$r_{ij,k\ell}^{(n)} = \frac{1}{N_B N_F} \sum_{f=1}^{N_F} \sum_{m=(n-1)N_B+1}^{nN_B} h_{ij}^{(f,m)} h_{k\ell}^{(f,m)*}. \qquad (1)$$

Key Generation Limits of Measured Channels

Figure 2(a) plots example temporal variation of I_{K} and I_{SK} for the raw channels acquired for Location 1B with four antennas at Alice, Bob, and Eve, where channels are normalized collectively to give an average SISO SNR of 15 dB. In this LOS scenario, RX approaches TX and the number of available and safe key bits both increase with increasing SNR. Also, increasing Alice-Eve separation (d) weakly increases safe key bits. In what follows, raw channels are processed to simulate a real system with power control. Average SISO gain in each block is normalized to 1, and the LOS of component is approximately removed using dominant component removal (DCR), which operates by performing a higher-order singular value decomposition (HOSVD) on the tensor covariance [4], forming the dominant component as the outer product of the dominant singular vectors for transmit and receive, and projecting channels onto the orthogonal complement of this dominant component.

Figure 2(b) plots I_{K} and I_{SK} for Location 1B for normalized channels after DCR for 15 dB SNR. The number of available key bits varies between 20 and 40 bits/ch, which is around half of the theoretical value for rich multipath channels [2]. Note that the highest I_{K} occurs at the end of the path, where the receiver transitions from the hallway to an open foyer. At positions in the hallway with high I_{K}, values for I_{SK} depend more strongly on eavesdropper separation d, similar to observations in [2], where more paths give higher key generation rates, but require larger Alice-Eve separation to be secure.

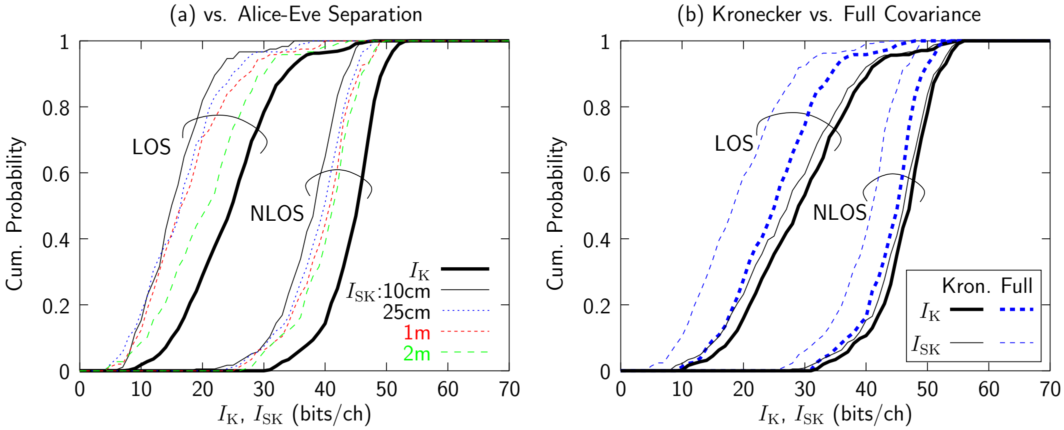

Figure 3: CDFs of I_{K} and I_{SK} for 15 dB SNR for all LOS and NLOS scenarios comparing (a) different Alice-Eve separations and (b) using Kronecker (solid) or full (dashed) covariance

LOS vs. NLOS – Figure 3(a) plots the key generation statistics for I_{K} and I_{SK} for LOS and NLOS scenarios with $N = 4$ antennas for Alice, Bob, and Eve and SNR=15 dB. LOS channels exhibit about half of the available key bits compared to NLOS, likely due to power control (equal SNR) and power reduction by DCR. Although for the widest separation of 2 m, there is still a gap of around 4 bits/ch between I_{SK} and I_{K}, this is only 10-20% of the total available key bits, indicating that most key bits are actually safe under practical conditions.

Impact of Using Separable Covariances – In real systems with limited CSI, separate (Kronecker) transmit and receive covariances are more easily computed than full covariance. Figure 3(b) shows how I_{K} and I_{SK} computed with Kronecker covariances compare with the true values computed with the full covariance, where each node has 4 antennas, 15 dB SNR, and I_{SK} is the average value for 1 and 2 m separation. Although the Kronecker model somewhat overestimates the number of available key bits, perhaps more importantly it suggests that nearly all key bits are secure, when a significant gap is present for the full covariance. This result is in harmony with previous MIMO capacity studies that show that the Kronecker model creates spurious non-physical paths that inflate the richness (diversity order) of channels.

Dependence on Number of Antennas – Figure 4(a) plots key generation statistics for varying numbers of antennas for NLOS scenarios only, where curves for (N_1, N_2) indicate N_1 antennas each at Alice and Eve and N_2 at Bob. For few antennas at Alice and Bob, I_{K} is near the theoretical maximum for i.i.d. Gaussian channels and most key bits are safe ($I_{\mathrm{SK}} \approx I_{\mathrm{K}}$). However, for increasing numbers of antennas, the gap between ideal i.i.d. I_{K} and actual I_{K} widens dramatically, which is reasonable since increasing antennas for limited multipath will lead to high correlation. Also, the gap between I_{K} and I_{SK} increases moderately with additional antennas. Similar trends are seen for LOS scenarios.

Effect of Eavesdropper Advantage – Eavesdroppers with a significant SNR and/or array size advantage may limit the security of key generation when Eve's channel is correlated with the Alice-Bob channel. Figure 4(b) depicts statistics for LOS scenarios with SNR=15 dB for two cases, illustrating where eavesdropper advantage appears to have minimum and maximum effect. Advantage appears to have minimal effect for small arrays that are balanced at Alice and Bob ($N_1 = N_2 = 1$). In this case the plot shows that at 2 m separation, a larger array ($N_3 = 4$) and SNR advantage (35 dB) help Eve negligibly. On the other hand, for unbalanced arrays ($N_1 = 1$, $N_2 = 8$), having more antennas at Eve reduces security significantly, as depicted by the arrow. These results are logical, since for a larger array Eve can estimate more multipath components and obtain a better estimate of the Alice-Bob

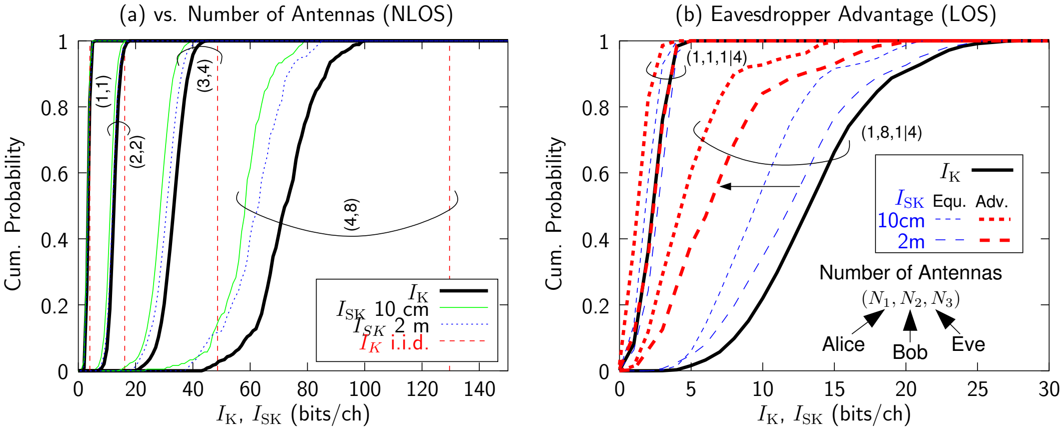

Figure 4: CDFs for I_{K} and I_{SK} for (a) NLOS scenarios with a varying number of antennas and (b) LOS scenarios without (Equ.) and with (Adv.) eavesdropper advantage

channel. In general, we have observed that having an antenna advantage appears to help Eve more than even a very large SNR advantage.

Conclusion

This paper explored the idea of secret key generation exploiting reciprocal MIMO channel fluctuations in an indoor environment, indicating that such methods are both secure and practical. LOS and NLOS measurements were performed for eavesdropper separations ranging from 10 cm to 2 m. The data was used to compute the actual number of available and secret key bits, where the effects of array size, eavesdropper separation and advantage, and covariance model were investigated. Even though for moderately sized arrays (4 elements or less) the number of available key bits is somewhat smaller than for i.i.d. channels, most bits are safe for reasonable eavesdropper separation, even with eavesdropper advantage.

Acknowledgment

This work was supported in part by a grant from the German Science Foundation (DFG) under the COIN program.

References

[1] J. Wallace, C. Chen, and M. Jensen, “Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits,” in *3rd European Conference on Antennas and Propagation (EuCAP ’09)*, (Berlin, Germany), pp. 1499 – 1503, Mar. 23-27, 2009.

[2] J. Wallace, “Secure physical layer key generation schemes: Performance and information theoretic limits,” in *IEEE International Conference on Communications (ICC ’09)*, (Dresden, Germany), pp. 1–5, June 14-18, 2009.

[3] B. T. Maharaj, J. W. Wallace, M. A. Jensen, and L. P. Linde, “A low-cost open-hardware wideband multiple-input multiple-output (MIMO) wireless channel sounder,” *IEEE Trans. Instrum. Meas.*, vol. 57, pp. 2283 – 2289, Oct. 2008.

[4] J. Wallace and B. Maharaj, “Accurate MIMO channel modeling: Correlation tensor vs. directional approaches,” in *Proc. 2007 IEEE Global Telecomm. Conf.*, (Washington, D.C.), pp. 3750–3754, 26-30 Nov., 2007.