Key Generation Exploiting MIMO Channel Evolution: Algorithms and Theoretical Limits

Jon W. Wallace [1], Chan Chen [2], Michael A. Jensen [2]

[1]*School of Engineering and Science, Jacobs University Bremen*
Campus Ring 1, 28759 Bremen, Germany
wall@ieee.org

[2]*Dept. of Electrical and Computer Engineering, Brigham Young University*
Provo, UT 84602, USA
chanchen.cc@gmail.com, jensen@ee.byu.edu

Abstract— **An emerging area of research in wireless communications is the generation of secret encryption keys based on the shared (or common) randomness of the wireless channel between two legitimate nodes in a communication network. However, to date, little work has appeared on methods to use the increased randomness available when the network nodes have multiple antennas. This paper provides theoretical performance bounds associated with using multi-antenna communications and proposes two practical methods for generating secret keys exploiting the increased randomness. Performance simulations reveal the efficiency of the methods.**

I. Introduction

While there remain some problems to be solved in the broad arena of multiple-input multiple-output (MIMO) communication over multipath channels, much of the research in antennas and propagation has been completed, leaving the community ready to find new and clever ways in which MIMO can be applied. One such emerging area, which spans the gap between channel characterization and information theory, is the generation of secret encryption keys based on shared knowledge of a fluctuating reciprocal channel in wireless networks [1]–[3]. Such methods require only that the node-to-eavesdropper channels be independent from the node-to-node channel for perfect secrecy, rather than the average or opportunistic quality advantage in other methods [4], [5]. So far, however, exploiting the increased randomness afforded by MIMO channels remains an elusive task. This work presents practical methods for key generation using MIMO channels and analyzes their performance.

This paper has three main contributions. First, assuming the legitimate and eavesdropper channels to be correlated multivariate Gaussian, the theoretical limit on the number of key bits per random channel realization is derived along with the number of these bits that are "safe" from an eavesdropper. Second, two practical algorithms for key generation are presented. Third, the performance of the methods is analyzed using path-based cluster models to illustrate the realizable key length for realistic environments.

II. System Model

Figure 1 depicts the model for a wireless communications system. Nodes 1 and 2 are legitimate users that would like to communicate securely, while node 3 is a potential eavesdropper. Reciprocal vector channels $\mathbf{h}_a = \mathbf{h}_{a'}$ are referred to as the *forward* and *reverse* channels for legitimate communications and are estimated by nodes 2 and 1, respectively. Channels $\mathbf{h}_b$ and $\mathbf{h}_c$, on the other hand, convey information to (and are estimated by) the eavesdropper. Due to noise, the nodes have imperfect estimates of the channels, or

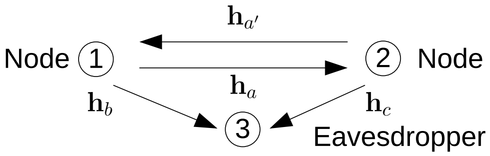

Fig. 1. System model for a wireless communications scenario

$$\hat{\mathbf{h}}_a = \mathbf{h}_a + \boldsymbol{\epsilon}_2,\ \ \hat{\mathbf{h}}_{a'} = \mathbf{h}_{a'} + \boldsymbol{\epsilon}_1,\ \ \hat{\mathbf{h}}_b = \mathbf{h}_b + \boldsymbol{\epsilon}_3,\ \ \hat{\mathbf{h}}_c = \mathbf{h}_c + \boldsymbol{\epsilon}_3, \tag{1}$$

where $\boldsymbol{\epsilon}_i$ is zero-mean complex Gaussian estimation error at node i having variance σ_i^2. Note that for MIMO communications, $\mathbf{h}$ represents a stacked channel matrix. We assume zero-mean correlated complex Gaussian random processes for the channels, characterized by the covariances

$$\mathbf{R}_{rp} = \mathrm{E}\left\{\mathbf{h}_r \mathbf{h}_p^H\right\} \qquad \hat{\mathbf{R}}_{rp} = \mathrm{E}\left\{\hat{\mathbf{h}}_r \hat{\mathbf{h}}_p^H\right\}, \tag{2}$$

where $\{r, p\} \in \{a, a', b, c\}$.

III. Information Theoretic Analysis

The estimated channels $\hat{\mathbf{h}}_{a'}$ and $\hat{\mathbf{h}}_a$ are observed by nodes 1 and 2, respectively, and the maximum number of information bits extracted from this process for key generation is $I_{\mathrm{K}} = I(\hat{\mathbf{h}}_a; \hat{\mathbf{h}}_{a'})$. The number of secure bits is the remaining mutual information when the eavesdropper channels are already known or $I_{\mathrm{SK}} = I(\hat{\mathbf{h}}_a; \hat{\mathbf{h}}_{a'} | \hat{\mathbf{h}}_b, \hat{\mathbf{h}}_c)$. Depending on the random variables, conditioning can theoretically increase the mutual information leading to $I_{\mathrm{SK}} > I_{\mathrm{K}}$, which means that knowing the eavesdropper channels creates more shared entropy between the two legitimate nodes. Since the communicating nodes do not know the eavesdropper channels, the rigorous definition of the number of safe key bits is $\min(I_{\mathrm{SK}}, I_{\mathrm{K}})$, although it should be noted that the condition $I_{\mathrm{SK}} > I_{\mathrm{K}}$ has not been observed in any of the simulations in this paper.

Assuming correlated zero-mean complex Gaussian random vectors for the links, it can be shown that

$$I_{\mathrm{K}} = \log_2 \frac{|\hat{\mathbf{R}}_{aa}||\hat{\mathbf{R}}_{a'a'}|}{|\hat{\mathbf{R}}_{AA'}|}, \tag{3}$$

where covariances of combined (stacked) random vectors are

$$\hat{\mathbf{R}}_{P_1 \dots P_M} = \mathrm{E}\left\{\mathbf{q}\mathbf{q}^H\right\}, \quad \mathbf{q} = [\mathbf{p}_1^T \mathbf{p}_2^T \dots \mathbf{p}_M^T]^T. \tag{4}$$

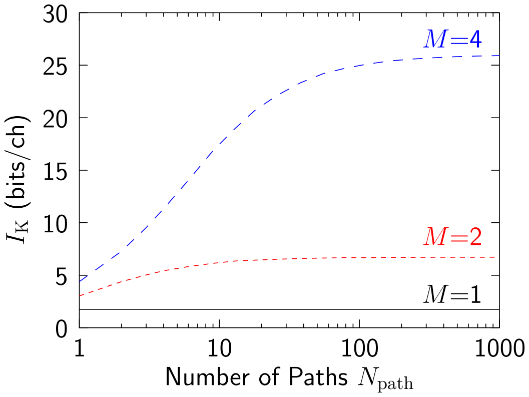

Fig. 2. Theoretical key bits that can be generated for M transmit and receive antennas and different levels of multipath for 10 dB SNR

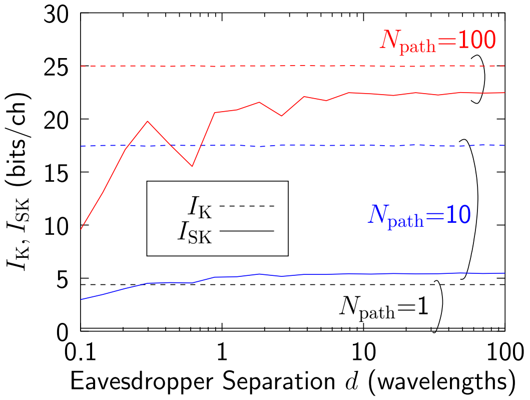

Fig. 3. Relative number of vulnerable key bits for $M = 4$ antennas for an eavesdropper at a distance d with varying levels of multipath and 10 dB SNR

Straightforward analysis reveals

$$I_{\mathrm{K}} = \log_2 |\mathbf{R}_{aa}\mathbf{R}_{\sigma}^{-1} + \mathbf{I}|, \tag{5}$$

where

$$\mathbf{R}_{\sigma} = (\sigma_1^2 + \sigma_2^2)\mathbf{I} + \sigma_1^2\sigma_2^2\mathbf{R}_{aa}^{-1}. \tag{6}$$

Evaluation of the secret key bits I_{SK} gives

$$I_{\mathrm{SK}} = \log_2 \frac{|\hat{\mathbf{R}}_{ABC}||\hat{\mathbf{R}}_{A'BC}|}{|\hat{\mathbf{R}}_{BC}||\hat{\mathbf{R}}_{AA'BC}|}, \tag{7}$$

where the covariance matrices are again the covariance of the stacked subscripted variables.

For many practical scenarios, the eavesdropper will be far away from both nodes 1 and 2, in which case $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$ are independent of $\hat{\mathbf{h}}_a$ and $\hat{\mathbf{h}}_{a'}$ and analysis shows that $I_{\mathrm{SK}} = I_{\mathrm{K}}$, as expected. The worst case for security, however, is when the eavesdropper is near one of the nodes. When the eavesdropper is near node 1, for example, and only movement of node 2 or scatterers causes variation of $\mathbf{h}_c$ and $\mathbf{h}_a$, $\mathbf{h}_b$ is not random and contains no information, reducing (7) to

$$I_{\mathrm{SK}} = \log_2 \frac{|\hat{\mathbf{R}}_{AC}||\hat{\mathbf{R}}_{A'C}|}{|\hat{\mathbf{R}}_{C}||\hat{\mathbf{R}}_{AA'C}|}. \tag{8}$$

Figure 2 plots I_{K} versus the number of paths and the number of transmit and receive antennas M for a signal-to-noise ratio (SNR) of 10 dB (mean squared estimation error divided by mean squared channel gain) for 1000 random covariances generated with a simple path-based channel model where the paths for each realization have angles uniformly distributed on $[0, 2\pi]$ and equal power. For a fixed number of antennas, the shared information saturates with increasing paths, and there is a dramatic increase in the available number of key bits with additional antennas M.

Figure 3 plots the number of available bits I_{K} and safe bits I_{SK} for $M = 4$ transmit and receive antennas, where the eavesdropper is located a distance d (in wavelengths) from node 1. Although many more key bits can be generated than the single antenna case (Figure 2), far richer multipath and separation are required to keep all bits safe. This suggests that adding antennas to enhance the generation rate of key bits potentially leaks increasing information to the eavesdropper.

IV. Practical Key Generation Methods

A. Channel Quantization Methods

A simple method for generating a random key at nodes 1 and 2 is for the two nodes to perform channel quantization (CQ) simultaneously on $\hat{\mathbf{h}}_{a'}$ and $\hat{\mathbf{h}}_a$, respectively [2]. The total space of observable channels is divided into Q regions of equal probability, each with a unique assigned bit pattern. Due to estimation error at the two nodes, sometimes the key bits will not match, necessitating some kind of error correction over a public channel. This idea is extended to MIMO channels by performing CQ on each of the elements of the spatially whitened stacked channel matrix $\hat{\mathbf{h}}_{w,a}$, given by $\hat{\mathbf{h}}_{w,a} = \hat{\mathbf{R}}_{aa}^{-1/2}\hat{\mathbf{h}}_a$. The main drawback of simple CQ is that channels on the region boundaries cause frequent key mismatch difficult to correct using standard error control techniques.

To generalize the CQ idea and reduce key mismatch, channel quantization with guardband (CQG) has been considered that creates Q quantization regions with equal probability separated by a specified guardband. When the nodes observe channels within the guardband, a mismatch is likely to occur, and the nodes should not use that channel observation to generate a key symbol. This requires a guardband indicator bit (GIB) to be transferred between the two nodes indicating if the channel has been observed in the guardband. Note that the GIB provides no information to the eavesdropper about any key symbols. By properly adjusting the size of the guardband, the likelihood of the nodes making a mistake near quantization region edges can be made small. Note that when guardband is set to 0, CQG can be thought of as a generalized version of CQ [2] that exploits both amplitude and phase fluctuations.

In this work, we employ rectangular quantization regions that are symmetric about the origin, similar to quadrature amplitude modulation (QAM), allowing us to solve for the quantization intervals by only considering the in-phase (I) or quadrature (Q) dimension separately, each with $\sqrt{Q}$ intervals. Due to space limitations, we will only mention that an iterative algorithm has been developed for finding the required intervals. An example quantization map for $Q = 256$ quantization regions is depicted in Figure 4 assuming unit total channel variance and a guardband of 0.1.

A final CQ method, referred to as channel quantization alternating (CQA) is considered where alternating staggered quantization maps are used instead of guardband. Figure 5 depicts the modified procedure of specifying the quantization regions, where for $\sqrt{Q}$ desired regions per dimension,

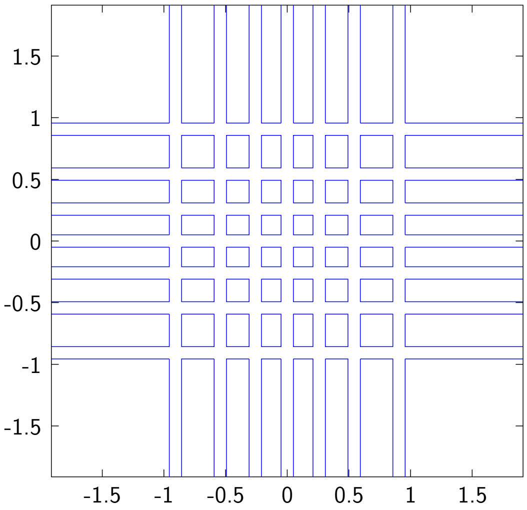

Fig. 4. Example map for 256 quantization regions having equal probability and a separating guardband of 0.1

$2\sqrt{Q}$ regions are first found having equal probability. At the node designated as the transmitter (TX), pairs of adjacent intervals are assigned ascending quantization values (QV) and alternating quantization maps (QM). When TX observes the channel in a given region, the QV symbol is added to its key and only the QM value is transmitted over the public channel to the receiver (RX). As can be seen, the TX chooses the quantization map where the observed channel is farthest from an edge, reducing the probability of mismatch. The RX observes the reciprocal channel, and depending on the received map indicated by the QM bit, assigns the corresponding QV symbol to the key. Like the GIB, the QM bit provides virtually no information to the eavesdropper.

B. Random Pre-Encryption

The random pre-encryption method generates the key at node 1 from the phases of a purposely constructed $M^2 \times 1$ vector $\mathbf{v}$. The elements of $\mathbf{v}$ are constructed as i.i.d. random variables with Rayleigh distributed amplitudes with variance $\sigma_{\mathbf{v}}^2$ and discrete phases uniformly distributed in the set $\{0, 2\pi/Q, \ldots, 2\pi(Q-1)/Q\}$, where Q is the phase quantization level. The discrete phases of the elements in $\mathbf{v}$ are mapped into binary bits using the mapping function $\mathrm{S} = f(\mathbf{v})$ using Gray codes, resulting in a key of length $M^2 \log_2 Q$.

Node 1 encrypts the vector $\mathbf{v}$ according to the operation $\mathbf{u} = \hat{\mathbf{h}}_{a'} + \mathbf{v}$ and sends $\mathbf{u}$ to node 2. Based on its knowledge of the channel, node 2 estimates the vector $\mathbf{v}$ using

$$\hat{\mathbf{v}} = \mathbf{u} - \hat{\mathbf{h}}_a = \mathbf{v} + \boldsymbol{\epsilon}_1 - \boldsymbol{\epsilon}_2. \tag{9}$$

If the value of $\mathbf{u}$ received at node 2 is corrupted by noise, another error term should be added in (9). Because our goal is to explore the possibilities of the approach, we assume that $\mathbf{u}$ is transmitted through an error-free channel. Finally, node 2 constructs the key from its estimate $\hat{\mathbf{v}}$ using the mapping function as $\widehat{\mathrm{S}} = f(\hat{\mathbf{v}})$.

One drawback of this method is the public transmission of $\mathbf{u}$ which potentially discloses information about $\mathbf{v}$ (or S) to the eavesdropper. The total information the eavesdropper obtains about S is

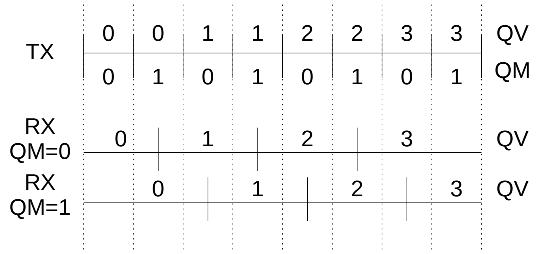

Fig. 5. Basic procedure for generating channel quantization alternating (CQA) maps for $\sqrt{Q} = 4$ quantization regions per dimension

$$\begin{aligned} I(\mathbf{v};\mathbf{u},\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c) &= I(\mathbf{v};\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c) + I(\mathbf{v};\mathbf{u}|\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c), \\ &= \log_2 \frac{|\hat{\mathbf{R}}_{UBC}||\hat{\mathbf{R}}_{VBC}|}{|\hat{\mathbf{R}}_{BC}||\hat{\mathbf{R}}_{UVBC}|}, \end{aligned} \tag{10}$$

where $I(\mathbf{v};\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c) = 0$ because $\mathbf{v}$ is independent of $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$ and, in the limit as $Q \to \infty$, $\mathbf{v}$ is normally distributed. If $\hat{\mathbf{h}}_{a'}$ and $\hat{\mathbf{h}}_a$ are independent of $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$ and $Q \to \infty$, then the information disclosed to the eavesdropper becomes

$$I(\mathbf{v};\mathbf{u}) = \log_2 \frac{|\hat{\mathbf{R}}_{\mathbf{vv}}||\hat{\mathbf{R}}_{\mathbf{uu}}|}{|\hat{\mathbf{R}}_{UV}|}. \tag{11}$$

Note that $I(\mathbf{v};\mathbf{u},\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c) \geq I(\mathbf{v};\mathbf{u})$, consistent with the intuition that more information about the key is revealed to the eavesdropper for correlated channels.

To increase the likelihood that $\widehat{\mathrm{S}} = \mathrm{S}$, the transmission of $\mathbf{u}$ uses LDPC coding with the message-passing decoding algorithm [6]. Also, the syndrome (set of parity bits) of the key is transmitted from node 1 to node 2, enabling node 2 to estimate the key with the help of $\widehat{\mathrm{S}}$, although this unfortunately discloses information about the key to the eavesdropper. Finally privacy amplification is applied to distill secret bits by hashing out the information revealed to the eavesdropper through the transmission of $\mathbf{u}$ and the syndrome [7]. The number of ultimate secret bits obtained per channel realization is $M^2 \log_2 Q$ less $I(\mathbf{v};\mathbf{u},\hat{\mathbf{h}}_b,\hat{\mathbf{h}}_c)$ (or $I(\mathbf{v};\mathbf{u})$), less the number of bits in the syndrome, less the value of the safety parameter [7] used in the privacy amplification.

V. Simulation Results

A. Simulation Model

We use the Saleh-Valenzuela Model with Angle (SVA) model to describe the physical propagation environment and use this information to synthesize the MIMO channel matrix [8]. In this model, each multipath cluster is described by a truncated Laplacian function with an angle spread of 26°. A narrowband implementation of the model is used which, as outlined in [8], requires specification of the normalized cluster arrival rate Λ and cluster decay rate Γ. Once a multipath model is created, a unique realization of the channel $\mathbf{h}^{(k)}$ is created for K different random node positions, $0 \leq k < K$. From this data, we define

$$\sigma_H^2 = \frac{\sum_{k=0}^{K-1} \|\mathbf{h}^{(k)}\|_F^2}{KM^2}, \tag{12}$$

where $\|\cdot\|_F$ denotes the Frobenius norm. The equivalent single-input single-output (SISO) SNR of the channel estimation is calculated as SISO SNR $= \sigma_H^2/\sigma^2$, where σ^2 is

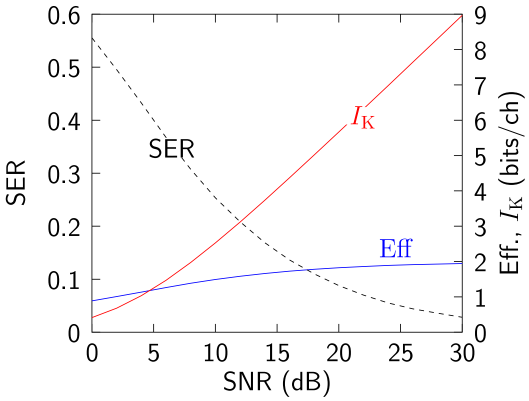

Fig. 6. Single-channel performance of channel quantization (CQ) with $Q = 4$ quantization regions

the variance of estimation error. In the simulation we assume $\sigma^2 = \sigma_1^2 = \sigma_2^2$.

B. Channel Quantization

To illustrate the performance of CQ methods, we begin by studying the single antenna Gaussian channel performance with varying SNR. The performance of realistic MIMO channels can then be conveniently found by characterizing the statistics of the SNR for prewhitened SVA channels. Here we assume that the eavesdropper channels are independent of the legitimate channels, so that only I_K needs to be considered.

Figure 6 shows the performance of key generation for simple CQ with a single channel, $Q = 4$ quantization regions, and varying SNR. Here, symbol error rate (SER) refers to the mismatch rate of symbols in the keys generated at the two nodes, and efficiency (Eff) is defined as the number of matching bits, or Eff $= (1 - \text{SER}) \log_2 Q$. We note that the theoretical maximum of 2 bits per channel is only acheived for very high SNR, exhibiting much lower efficiency than the theoretical maximum I_K. The crossing of the Eff and I_K curves at low SNR is due to the simple definition of efficiency, since at high SER, significant overhead is required to determine which symbols are actually correct.

The effect of adding guardband is depicted in Figure 7 for the CQG method with $Q = 4$ quantization regions and 15 dB SNR. Although guardband allows the SER to be reduced to a level that can be overcome with forward error correction, additional efficiency must be sacrificed. However, some of this efficiency can be regained by using the CQA method, since higher quantization levels are supported due to the lower likelihood of mismatch. Figure 8 depicts the performance for $Q = 4$ and 16 quantization regions and varying SNR, indicating efficiency much closer to the theoretical maximum.

To apply these characteristic single-channel results to realistic MIMO channels, the statistics of spatially pre-whitened SVA channels must be investigated. After prewhitening, the SNR of the ith pre-whitened channel is $\lambda_i \sigma_H^2 / \sigma^2$, where λ_i is the ith eigenvalue of $\hat{\mathbf{R}}_{aa}$. Figure 9 plots the cdfs for 1000 random realizations of the covariance eigenvalues for the narrowband SVA model with Laplacian clusters having an angular spread of 26°, $\Gamma = 2$, and $\Lambda = 1$ assuming uniform linear arrays with $M = 3$ antennas and $\lambda/2$ inter-element spacing. Combining this information with Figure 8, one can estimate the efficiency of a MIMO system with prewhitening. For example, assuming that an average (50% outage) uncoded SER of 0.1 is desired, quantization maps of size Q=16 and Q=4 require 18 dB and 12 dB SNR, respectively. For 20 dB SISO SNR, the required relative (eigenvalue to SISO) SNR is -2 dB and -8 dB, respectively. Figure 9 indicates that at the 50% level, 5 of the channels support Q=16 and 4 channels Q=4 for a total of 28 bits per channel.

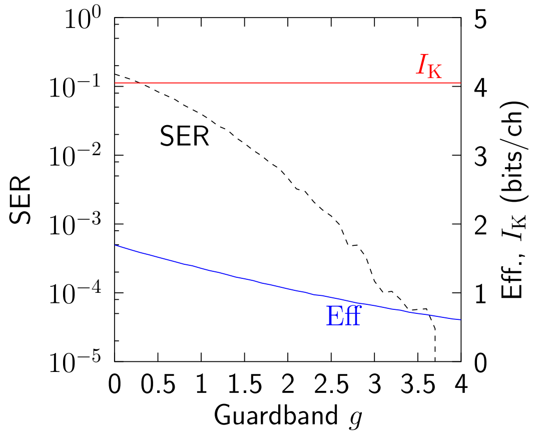

Fig. 7. Single-channel performance of channel quantization with guardband (CQG) with $Q = 4$ quantization regions, 15 dB SNR, and guardband g

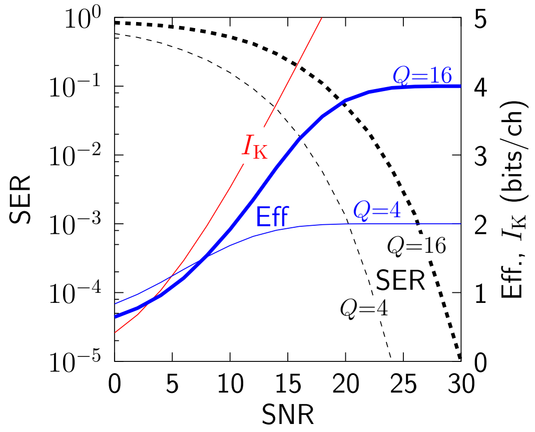

Fig. 8. Single-channel performance of channel quantization alternating (CQA) with $Q = 4$ and 16 quantization regions

C. Random Pre-Encryption

We limit our analysis to the case where $\hat{\mathbf{h}}_{a'}$ and $\hat{\mathbf{h}}_a$ are independent of $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$ since the application of the method is identical when $\hat{\mathbf{h}}_{a'}$ and $\hat{\mathbf{h}}_a$ are correlated with $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$ except that we hash out $I(\mathbf{v}; \mathbf{u}, \hat{\mathbf{h}}_b, \hat{\mathbf{h}}_c)$ bits rather than $I(\mathbf{v}; \mathbf{u})$ bits. This means that $\mathbf{h}_b$ and $\mathbf{h}_c$ are constructed from independent realizations of the SVA model. For each simulation, 200,000 unique SVA model realizations with $\Gamma = \Lambda = 1$ are used, with the results shown representing averages over the ensemble of channels. A rate 1/2 LDPC code with code length 816 is used with 100 decoding iterations. The safety parameter in the privacy amplification is set to be 10.

Fig. 10 plots the bit-error-rate (BER) performance of the generated binary bits versus SNR for $r = \sigma_{\mathbf{v}}^2 / \sigma_H^2 = 0.5$ and 1 when $M = 3$ and $Q = 2^2$. Only the curve marked with ‘LDPC’ uses the LDPC coding. These results show that a larger value of r, which corresponds to increased transmission power, creates a slight performance improvement, highlighting the trade-off between transmit power and

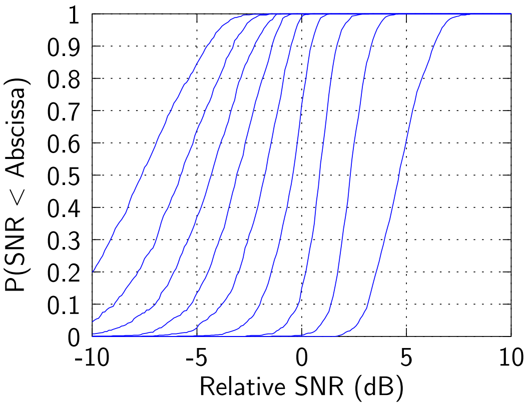

Fig. 9. Channel covariance eigenvalue distributions of the SVA model with $M = 3$ antennas. Relative SNR is the eigenvalue SNR for a SISO SNR of 0 dB.

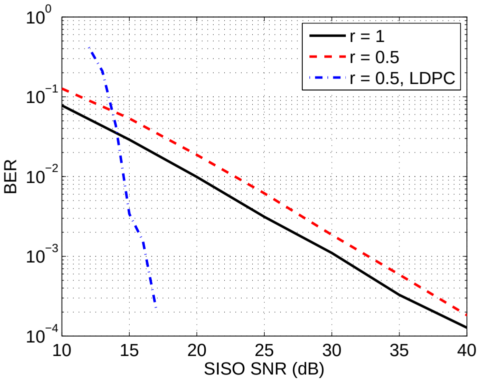

Fig. 10. Comparisons of BER performance of the generated binary bits with different values of r for $M = 3$ and $Q = 2^2$ with and without LDPC coding.

BER performance. Furthermore, this plot shows the dramatic improvement obtained when LDPC coding is applied to the transmission. Fig. 11 plots the number of the secret bits per channel using LDPC codes with $M = 3$ for different values of r as well as the performance bound computed using (5). These curves clearly reveal how additional transmit power (and therefore effective SNR) increases the length of the secret key. Unfortunately, Fig. 11 also demonstrates that the slope of the curves for the random pre-encryption method are smaller than that for the bound. Finally, Fig. 12 compares the secret bits per channel for different numbers of antennas with $r = 0.5$, showing that a longer secret key is generated as the array size increases. The increasing slope of the curves with additional antennas also demonstrates that larger array sizes improve the efficiency of the key generation method.

VI. Conclusions

This paper has discussed the establishment of secret encryption keys for nodes operating in wireless channels by exploiting the common randomness associated with MIMO channel coefficients. After providing a discussion of the theoretical performance bounds, the paper proposes two practical methods for key generation and demonstrates their performance using simulations based on physically representative channel models. These simulations show that while the methods fall short of realizing the upper performance bounds, they do offer increased efficiency in key generation as the number of antennas increases.

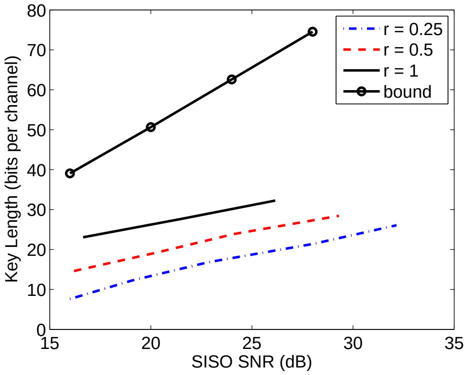

Fig. 11. Secret bits per channel for different values of r with LDPC codes, $M = 3$ and BER $= 10^{-3}$.

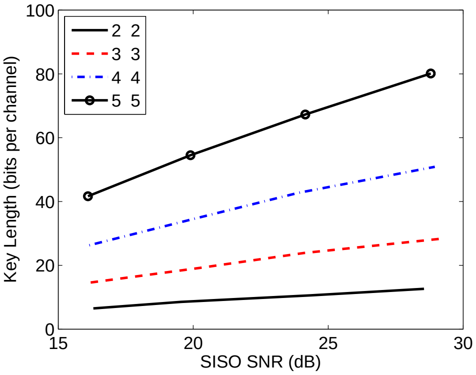

Fig. 12. Secret bits per channel for different numbers of antennas, $r = 0.5$ and BER $= 10^{-3}$.

Acknowledgment

This work was supported in part by the US Army Research Office under the Multi-University Research Initiative (MURI) Grants # W911NF-04-1-0224 and # W911NF-07-1-0318.

References

[1] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, pp. 3776–3784, Nov. 2005.

[2] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. Int. Conf. Acoustics, Speech and Signal Processing*, Las Vegas, Nevada, Mar. 31-Apr. 4 2008, pp. 3013–3016.

[3] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, pp. 3–6, Jan. 1995.

[4] A. O. Hero, III, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, pp. 3235–3249, Dec. 2003.

[5] M. Bloch, J. Barros, M. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[6] A. D. Liveris, Z. Xiong, and C. N. Georghiades, "Compression of binary sources with side information at the decoder using LDPC codes," *IEEE Commun. Lett.*, vol. 6, no. 10, pp. 440–442, Oct. 2002.

[7] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[8] J. W. Wallace and M. A. Jensen, "Modeling the indoor MIMO wireless channel," *IEEE Trans. Antennas Propag.*, vol. 50, pp. 591–599, May 2002.