Physical Layer Key Generation Methods for Arbitrary Fading Channels

Rajesh K. Sharma
School of Engineering and Science
Jacobs University Bremen
28759, Bremen, Germany
Email: ra.sharma@jacobs-university.de

Jon W. Wallace
School of Engineering and Science
Jacobs University Bremen
28759, Bremen, Germany
Email: wall@ieee.org

***Abstract*—Two methods are developed that can be applied to generate secret keys automatically from fading propagation channels that are reciprocal but have arbitrary (i.e. non Gaussian) statistics. Such methods may be necessary for physical-layer key generation in cases where the line-of-sight (LOS) component produces Rician channel statistics, not only because channel quantization based on Gaussian statistics will not provide equally probable symbols, but also because the symbol error rate (SER) and efficiency analysis based on Gaussian channels does not reflect true performance. An improved channel quantization method compared to [1], [2] is developed, where the empirical cumulative distribution function (cdf) of the channel is used directly to ensure equal probability of the key symbols. The results show that LOS channels can have slightly better SER performance than strictly Gaussian channels, especially at low SNR. Second, the idea of positional coding is developed, where a secret key can be transmitted by dividing empirical channel observations into multiple codewords and conveying a secret message from Alice to Bob in the sequence of channels fed forward from Alice to Bob. Analysis of the method illustrates that key mismatch rate can be made arbitrarily low by properly selecting the codeword length.**

I. Introduction

This work considers a wireless communications scenario identical to that in [1], [2], consisting of Alice and Bob that are legitimate nodes that wish to communicate securely, where Eve is a potential eavesdropper. A theoretical analysis on reciprocal channel key generation (RCKG) in a MIMO context has been considered in [3], [4], whereas [1] and [2] study the limits of RCKG from an experimental perspective, where information theoretic expressions and RCKG protocols are applied to three-node MIMO measurements. However, key generation schemes for non-Gaussian channels have not yet been considered.

The purpose of this paper is to develop methods for physical layer key generation that can be applied when the channel is non-Gaussian, which is important for practical channels that may have arbitrary fading statistics. Non-Gaussian fading may arise from such factors as the presence of a line-of-sight (LOS) component or the superposition of multipath and shadowing. The first part of the paper studies improved channel quantization that directly exploits empirical cumulative distribution functions (cdfs) of the channel snapshots to ensure equal probability of generated key symbols. The utility of the method is demonstrated by application to actual propagation data taken from three-node indoor measurements. In the second part of the paper, a new method for conveying a secret key from Alice to Bob based on positional coding is developed, which not only may be applied to channels with arbitrary fading statistics, but also allows the key mismatch rate to made arbitrarily low without the need for separate error control coding.

II. Empirical cdf-based Channel Quantization

In [1] and [2], the performance of key generation based on channel quantization is studied from an analytical and experimental perspective, where it is assumed that channels have Gaussian statistics, which may not be appropriate for real scenarios. To ensure maximum security of generated keys, the propagation channel should should have equal probability of being observed in different quantization sectors, requiring a method that can adapt to the current channel distribution.

We consider a straightforward solution to this problem, which discards the use of the Gaussian assumption for defining the quantization intervals, and instead chooses them based on the empirical cumulative distribution function (cdf) of measured channel data. The samples for each record of measurement data are divided into several blocks, where the fading statistics for a single block can be considered stationary. For each block the boundaries for equiprobable sectors in a single real dimension are determined for a desired number of quantization sectors (M_q). SER and efficiency graphs for the method can be computed using a Monte-Carlo analysis as is demonstrated below.

The performance of the new cdf-based method is now assessed in terms of SER and efficiency for CQG and CQA by application to the same propagation data as was presented in [2]. The data in a single measurement run is divided into 8 equal-length temporal segments (blocks). Since the cdfs for each block vary, the quantization intervals that are used are time-varying, and an example is shown in Fig. 1 for a single block assuming 8 quantization sectors for a single real dimension ($M_q = 8$). The data of two LOS measurements (scenarios 1-A and 1-C discussed in [2]) are considered and results shown reflect the average performance of the two measurements. The SNR in this work is defined as the ratio of the channel variance and the variance of estimation error as in

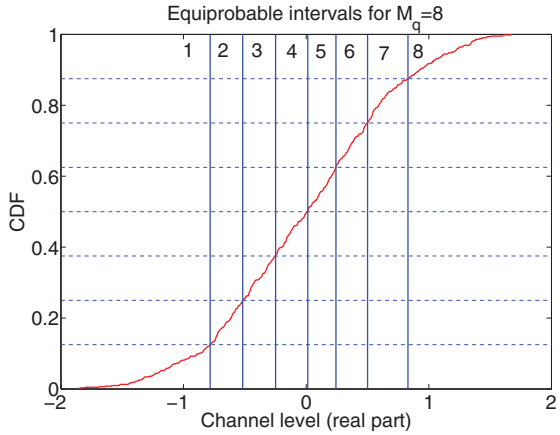

Fig. 1. Quantization intervals and boundaries for a single block of measurement data, assuming 8 quantization sectores

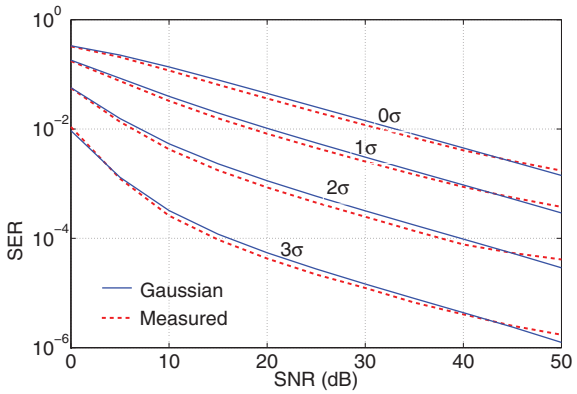

Fig. 2. SER performance (real dimension) of CQG for $M_q = 2$ and varying guardbands for the quantization intervals obtained from the distribution of measured data

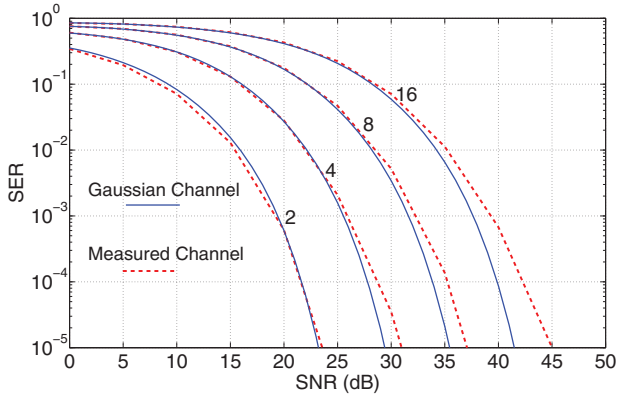

Fig. 3. SER performance of CQA for the quantization intervals obtained from the distribution of measured data

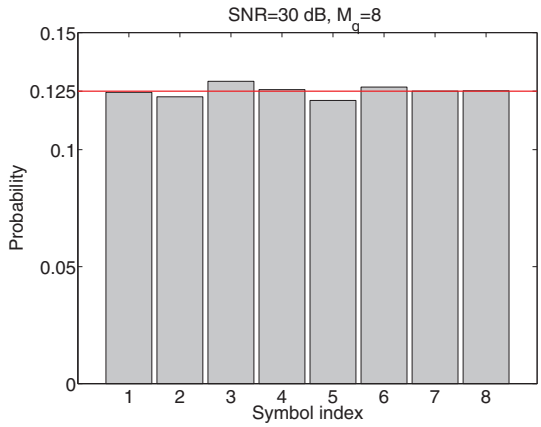

Fig. 4. Observed frequency of symbols for symbol indices 1-8 for a single block of measured data and 30 dB SNR

[2]. It is observed in Fig. 2 and 3 that the SER in the measured data is slightly lower than the Gaussian which is found for all values of guardbands g in CQG and low SNR and $M_q = 2$ in CQA. Although surprising, this effect appears to be due to the combination of the Rician channel statistics with the usual power normalization that does not remove the channel mean, and this has been verified by simple Monte-Carlo simulations of a Rician channel.

The efficiency of the CQG and CQA methods based on the cdf of measurement-based data is also compared with that obtained from Gaussian statistics which is plotted in Fig. 5 and 6. The results are close to each other except that for $M_q = 2$ the measurement-based result gives slightly better performance. However, for the higher M_q and large SNR the measurement-based efficiency is slightly smaller.

Fig. 4 shows the observed probability of the key symbol indices generated by Alice for CQA with $M_q = 8$ and SNR of 30 dB. It is seen that all the symbols are almost equally probable making the key generation secure and efficient.

III. Positional Coding of Fading Channels

Although the quantization method developed in the previous section overcomes the difficulty of non-Gaussian statistics causing non-uniform coverage of the key symbols, it does not solve the problem of key mismatch. Quantization methods like this and those presented in [2] that encode individual channel observations separately require separate error control coding in addition to the quantization to achieve keys that are robust to mismatch. Error control coding complicates the key generation procedure and transmitted error control bits reveal information about the key that diminish the effective key length.

An interesting alternative to channel-by-channel key quantization and separate error control coding is to encode multiple channel observations jointly. By assigning key symbols to different *sequences* of channel observations, the probability of mistaking one symbol for another (or one sequence for another) can be made arbitrarily low, as is known from basic coding theory. However, an important question is how to create a codebook for a given set of measured channels having arbitrary fading statistics.

This section considers a novel way of using observations

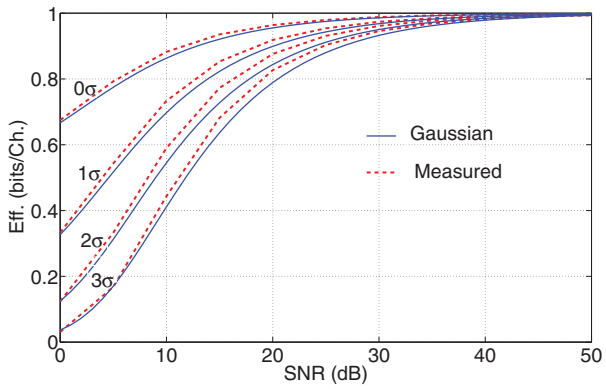

Fig. 5. Efficiency of CQG for the measurement-based distribution

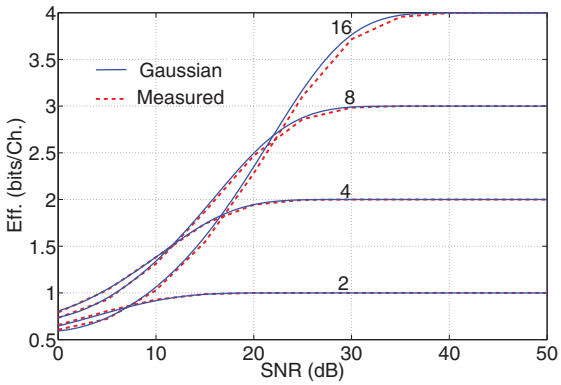

Fig. 6. Efficiency of CQA for the measurement-based distribution

of the propagation channel to convey secret information from Alice to Bob that exploits the *order* of the observed channels. As will be demonstrated, by choosing the length of each keyword to be long enough, the probability of a mismatch in the transmitted information (key) can be made arbitrarily low.

A. Principle of Channel Positional Coding

First we give a simple analogy that demonstrates the idea of positional coding and then we explain precisely how this can be accomplished with a fading reciprocal propagation channel. Consider Alice and Bob as having two copies of a photograph that cannot be seen by Eve. Alice cuts her copy of the photo horizontally into M pieces and numbers them logically from 1 to M going from left to right. Alice creates a table of all possible sequences of the M pieces and numbers these 1 through $M!$, and this sequence enumeration table is given to Bob and Eve. Alice picks a number between 1 and $M!$ (the message) and using the table puts the M pieces in that sequence before handing them to Bob. Finally, Bob can match the received pieces with his photo to determine the indices of the pieces and which sequence (or message) was sent. Note that even if Eve observes the pieces transmitted from Alice to Bob, the order to her is random, and since she does not

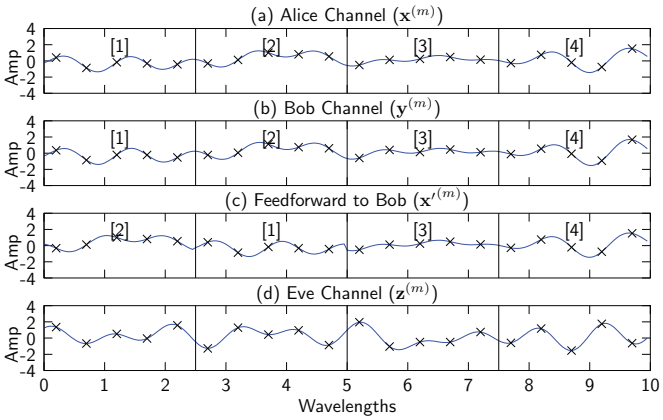

Fig. 7. Example demonstrating positional coding using a Rayleigh propagation channel

have access to the original photo, she can only determine the order by matching the pieces at the edges (much like a jigsaw puzzle with no reference picture!). However, if the photo is sufficiently random, matching at the edges will not be possible.

This same principle can be applied to send a secret message using a reciprocal propagation channel. Fig. 7 shows a simple example of a Rayleigh fading channel at Alice, Bob, and Eve. Alice and Bob observe the channels in Fig. 7(a) and (b), respectively, which are reciprocal and highly correlated. The observed block of channels is decimated into samples that are nearly uncorrelated in time ($\times$'s in the figure) and divided into $M = 4$ codewords of $N = 5$ samples each, where $x_n^{(m)}$ is the nth uncorrelated sample of the mth codeword. Next, Alice picks the sequence $[2], [1], [3], [4]$ to send to Bob, and transmits her observed channels to Bob in this order as shown in Fig. 7(c). Bob can then match the codewords $\mathbf{x}'^{(m)}$ received with his own estimated channels $\mathbf{y}^{(m)}$ to determine the numbering of the codewords and obtain the message. In Fig. 7(d), Eve's channel is shown that is weakly correlated with that of Alice and Bob, but it should be clear that similarities are insufficient to perform the match, and the decimation procedure has removed the possibility of edge matching.

For M codewords, the length of the generated key is $L_M = \log_2(M!)$. Thus, the efficiency of the positional coding strategy is given by

$$\eta = \log_2(M!)/(MN) \quad \text{(bits/channel)}, \tag{1}$$

which is somewhat less efficient than normal channel coding that would have an efficiency of $\log_2(M)/N$ bits per channel use. Note also that the N samples do not need to represent temporal samples, but could be from N different OFDM bins or N different antennas in a MIMO system.

B. Decoding Strategies for Positional Coding

In our work, we have considered three possible strategies for decoding positionally coded messages. All of the methods are based on the Euclidean distance of two channel codewords

$$d(\mathbf{x}, \mathbf{y}) = ||\mathbf{x} - \mathbf{y}||^2. \tag{2}$$

1) Parallel Decoding: In this case, Bob computes the distance matrix elements $d_{m_1,m_2} = d(\mathbf{x}'^{(m_1)}, \mathbf{y}^{(m_2)})$ and declares the mth received codeword to have index

$$\mathrm{idx}_m = \arg\min_{m_2} d_{m,m_2}. \tag{3}$$

Note that this operation can be performed fully in parallel for all codewords.

2) Min Distance Ordered Decoding: Here, Bob uses the fact that he is more certain about some codewords than others and chooses the decoding order according to this confidence. Bob decodes the M codewords sequentially, by letting $\mathcal{M}_1 \leftarrow \{\}$ and $\mathcal{M}_2 \leftarrow \{\}$ be empty sets and at step k he declares

$$\mathrm{idx}_{m_k} = \arg \min_{\substack{m_2 \\ m_2 \notin \mathcal{M}_2}} d_{m_k,m_2}, \tag{4}$$

$$m_k = \arg \min_{\substack{m_1 \\ m_1 \notin \mathcal{M}_1}} \min_{\substack{m_2 \\ m_2 \notin \mathcal{M}_2}} d_{m_1,m_2}, \tag{5}$$

and lets $\mathcal{M}_1 \leftarrow \mathcal{M}_1 \cup m_k$ and $\mathcal{M}_2 \leftarrow \mathcal{M}_2 \cup \mathrm{idx}_{m_k}$.

3) Min-Max Distance Ordered Decoding: Instead of only considering the codeword that is closest to one of his own channels, Bob can base his confidence on minimizing the distance of the best match and simultaneously maximizing distance to the second closest match. This potentially avoids mismatches where codewords are not strongly separated and saves decoding these codewords until the end. This is similar to the Min distance decoding, except the chosen index is

$$m_k = \arg \max_{\substack{m_1 \\ m_1 \notin \mathcal{M}_1}} \Big[\min_{\substack{m_2 \\ m_2 \notin \mathcal{M}_2}}{}^{(2)} d_{m_1,m_2} - \min_{\substack{m_2 \\ m_2 \notin \mathcal{M}_2}}{}^{(1)} d_{m_1,m_2} \Big], \tag{6}$$

where $\min^{(i)}$ means the ith smallest value.

C. Performance Analysis

To see the performance of positional coding based on a shared reciprocal channel, simulations were performed using independent complex Gaussian channels with SNR=10 dB at Alice and Bob, where SNR is the ratio of channel variance to channel estimation error as defined in [2]. Monte Carlo simulations were run for various values of M and N for the different decoding methods, where the number of realizations was varied from 100 to 10^7 in order to obtain enough error events for smooth curves. Fig. 8 depicts the resulting probability of key error P_{err}, which occurs if there is a mismatch in the position of any of the estimated codewords.

As can be seen, the probability of having a mismatch of the sent message (or key) can be made arbitrarily small by either increasing the number of samples per codeword N or by reducing the number of codewords M (which also would mean a shorter key). If K keys are to be concatenated to form a longer key, the probability of having the total key be correct is $1-[1-P_{\mathrm{err}}(M,N)]^K$. As an example, using the best decoding strategy a key mismatch rate of $P_{\mathrm{err}} = 0.1$ can be obtained with $N = 3, M = 10$ ($L_M = 22$ bits), $N = 4, M = 30$ ($L_M = 108$ bits), or $N = 5, M = 60$ ($L_M = 272$ bits).

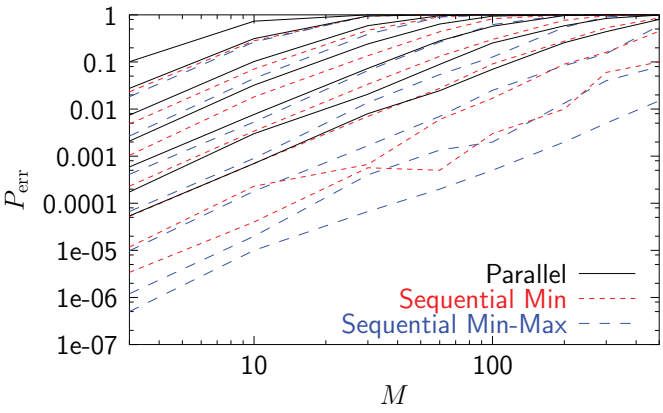

Fig. 8. Performance of positional coding for the three decoding methods versus the number of codewords M. Multiple curves for each decoding method are for $N = 2, 3, \ldots, 8$ moving from top to bottom.

IV. Conclusion

In this paper we have considered methods for physical layer key generation that can exploit common random fading of reciprocal wireless channels, with a focus on methods for channels having arbitrary (possibly non-Gaussian) fading statistics. First, the quantization methods in [2] were extended to arbitrary fading channels by generating quantization maps based on empirical cumulative distribution functions cdfs of the data at hand, ensuring equal probability coverage of the generated key symbols. Application of the method to measured indoor channels indicated that symbol error performance similar to the quantization of Gaussian channels is obtained, even in indoor LOS environments.

Second, the idea of positional coding, where a secret key can be transmitted from Alice to Bob in the *sequence* of channels fed forward from Alice to Bob was explored. The method is not only applicable to arbitrary fading channels, but also can provide robustness of the generated keys to mismatch. Analysis of the performance of the method for Gaussian channels indicated that low key mismatch rate can be obtained for useful key lengths and moderate complexity.

Acknowledgment

This work was supported by a grant from the German Research Foundation (DFG) under the COIN Focus Program.

References

[1] J. W. Wallace and R. K. Sharma, "Experimental investigation of MIMO reciprocal channel key generation," in *Proc. 2010 IEEE Intl. Conf. Commun.*, May 2010, pp. 1–5.

[2] 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, no. 3, pp. 381–392, Sept. 2010.

[3] J. Wallace, C. Chen, and M. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *Proc. 2009 European Antennas Propag. Conf. (EuCAP '09)*, Berlin, Germany, Mar. 23-27, 2009, pp. 1499 – 1503.

[4] J. Wallace, "Secure physical layer key generation schemes: Performance and information theoretic limits," in *Proc. 2009 IEEE Intl. Conf. Commun.*, Dresden, Germany, June 14-18, 2009, pp. 1–5.