Artificial-Noise-Aided Secure Transmission over Finite-Input Intersymbol Interference Channels

Serdar Hanoglu*,†, Sina Rezaei Aghdam*, and Tolga M. Duman*

*Dept. of Electrical and Electronics Engineering, Bilkent University, Ankara, Turkey, TR 06800
†Communication and Information Technologies Business Sector, ASELSAN Inc., Ankara, Turkey, TR 06370
Emails: {shanoglu, aghdam, duman}@ee.bilkent.edu.tr

***Abstract*—We propose an artificial noise (AN) injection strategy for securing communication over finite-input intersymbol interference (ISI) channels. The technique relies on injection of colored noise whose power spectral density has the least match with the spectrum of the main channel in a certain sense. By evaluation of an achievable secrecy rate, we demonstrate that the proposed AN injection based solution results in a considerable improvement over the existing approaches, especially when the eavesdropper works at high signal-to-noise ratios (SNRs).**

***Index Terms*—Physical layer security, finite-state wiretap channel, artificial noise, inter-symbol interference.**

I. Introduction

The wiretap channel was introduced by Wyner in 1975 where he defined the secrecy capacity as the maximum rate at which confidential messages can be reliably transmitted to a legitimate receiver while assuring that an eavesdropper does not acquire any information [2]. While there were only sporadic efforts on physical layer security until about a decade ago, with the proliferation of wireless networks, a considerable interest has been drawn towards exploring the capabilities of physical layer in securing communications in recent years.

Secrecy capacities of different classes of wiretap channels have been extensively investigated (see [3] for a survey). However, the important case of wiretap channels with memory in the form of intersymbol interference (ISI) has not received much attention until now. To the best of our knowledge, the only related work is reported in [4] where the authors employ a stochastic algorithm to evaluate a multi-letter form of the secrecy capacity expression. In addition, so as to increase the secrecy rates, the authors propose an iterative algorithm to optimize the transition probabilities of the Markov inputs for given main and eavesdropper's channels. This optimization leads to some improvements in the achievable secrecy rates when the receivers work at low signal-to-noise ratios (SNRs). However, at high SNRs, Markov inputs lose their advantages over uniform inputs, and no improvements are observed.

Injection of artificial noise (AN) has been one of the effective strategies for securing communication at the physical layer. The most widely studied technique is the one which uses the spatial degrees of freedom of multiple transmit antenna systems to inject AN in the null-space of the main channel (see, e.g., [5] and [6]). Other AN-aided transmission schemes have also been recently proposed for securing single-input single-output communications (see, e.g., [7]).

In this paper, we propose a novel AN-aided strategy for improving the achievable secrecy rates over finite-input ISI wiretap channels. More specifically, with the aid of the channel state information (CSI) of the main channel, we propose to inject colored noise whose power spectral density has the least match with the spectrum of the main channel. The idea is to affect the information rates at the legitimate receiver minimally while imposing considerable degradations in the eavesdropper's reception. This approach is inspired by the results of the several studies in the information theory literature in which transmission strategies rely on matching the spectrum of the input to that of the channel to increase information rates over ISI channels (see, e.g., [8] and the references therein). We introduce AN-aided secure transmission strategies for the scenarios where: a) only the CSI of the legitimate receiver is available at the transmitter, b) CSI of both the main and the eavesdropper's channel is known by the transmitter. We show through numerical examples that the proposed transmission schemes outperform the existing solutions in terms of performance and complexity.

The paper is organized as follows. Section II presents the system model, assumptions and the statement of the problem. The proposed AN injection method to increase the secrecy rates is described in Section III. In Section IV, we provide several numerical examples to demonstrate the efficacy of the proposed scheme and present our concluding remarks in Section V.

II. System Model and Problem Statement

We consider an ISI wiretap channel where a transmitter (Alice) communicates with a legitimate receiver (Bob) in the presence of an eavesdropper (Eve). The received vectors at Bob and Eve are expressed as

$$y_B(k) = \sum_{i=0}^{m_{AB}-1} g_{AB}(i)x(k-i) + n_{AB}(k), \qquad (1)$$

This work was supported by the Scientific and Technical Research Council of Turkey (TUBITAK) under the grant #113E223.
This work is primarily based on the M.S. Thesis of the first author [1].

978-1-5386-2321-3/18/$31.00 ©2018 IEEE

$$y_E(k) = \sum_{i=0}^{m_{AE}-1} g_{AE}(i)x(k-i) + n_{AE}(k), \qquad (2)$$

respectively, where $x(k)$ denotes the transmitted message signal at time k. For simplicity, we assume that $g_{AB}(i)$ and $g_{AE}(i)$ are (real) Gaussian random variables with zero mean and their variances are determined according to the corresponding multipath delay profiles.[1] m_{AB} and m_{AE} are the number of propagation paths over the main and the eavesdropper's channels, respectively. The noise terms n_{AB} and n_{AE} are assumed to be Gaussian random variables with variances $N_{0,B}/2$ and $N_{0,E}/2$, respectively. We define the SNRs at the respective receivers as

$$SNR_{AB} = \frac{E_s\ \mathbb{E}\{\|g_{AB}\|^2\}}{N_{0,B}},\ SNR_{AE} = \frac{E_s\ \mathbb{E}\{[\|g_{AE}\|^2\}}{N_{0,E}}, \qquad (3)$$

where $\mathbb{E}$ denotes the expectation operator, $\|.\|$ denotes the Euclidean norm and E_s is the average energy per symbol.

We consider this setup with both channels experiencing (ergodic) block fading where the channel coefficients remain constant during each coherence interval and change independently from one block to the next. Furthermore, the fading coefficients corresponding to the main and the eavesdropper's channels are independent of each other. We also assume that the number of channel uses within each coherence interval is large enough to allow for random coding arguments [9].

For given realizations of channels, an achievable secrecy rate (conditioned on the channel gains) can be formulated for the finite state Gaussian wiretap channel as [4]

$$R_s = \left[\max_{P(x^n)} \lim_{n\to\infty} \frac{1}{n}\Big(I(X^n;Y_B^n) - I(X^n;Y_E^n) \Big) \right]^+, \qquad (4)$$

where $[a]^+ = \max\{a, 0\}$, $I(.;.)$ denotes the mutual information between channel input and output signals and $P(.)$ is probability density function. This expression is a lower-bound on the secrecy capacity as we skip the optimal selection of the auxiliary random variable for prefixing in [10, Theorem 3]. In order to evaluate the achievable ergodic secrecy rates, denoted by $\bar{R}_s$, the instantaneous secrecy rates in (4) should be averaged over different realizations of the channel coefficients, i.e.,

$$\bar{R}_s = \mathbb{E}_{g_{AB},g_{AE}}\{R_s\}, \qquad (5)$$

where $\mathbb{E}_{g_{AB},g_{AE}}\{.\}$ denotes the expectation over g_{AB} and g_{AE}. The system performance is quantified using the achievable ergodic secrecy rate given in (5), which is achievable via the variable rate coding scheme proposed in [9].

[1] In reality, for bandpass communication systems, these would be complex quantities. For simplicity, however, we take them as real throughout this article. The general methodology will work for the complex case in exactly the same way.

III. Methodology

In order to maximize R_s, we propose to allocate a fraction of the total power to inject AN along with the data transmission in contrast to the solution proposed in [4], which relies on iterative optimization of the transition probabilities of the Markov source. We employ uniformly distributed inputs and we inject colored AN with the least spectral match to the frequency response of the main channel. Therefore, the information rate over the main channel undergoes a minimal loss. On the other hand, this AN injection suppresses the reception at the eavesdropper (on average) leading to considerable improvements in the achievable secrecy rates. In the remainder of this section, we explain how such an AN can be generated and injected. Moreover, we will explain the required transformations to compute information rate terms using the existing algorithms in the literature.

A. Artificial Noise Injection

For the injection of the AN, we generate colored Gaussian noise by filtering a white Gaussian noise process as illustrated in Fig. 1. Under the AN-aided transmission, the signal transmitted by Alice, $x(k)$, takes the following form with the portion of power allocated to the AN denoted by α:

$$\begin{aligned} x(k) &= \sqrt{1-\alpha}s(k) + \sqrt{\alpha}w(k) \\ &= \sqrt{1-\alpha}s(k) + \sqrt{\alpha}\sum_{j=0}^{l} h(j)u(k-j), \end{aligned} \qquad (6)$$

for $k = 1, 2, \ldots$, where $s(k)$ is the transmitted signal for the desired message for Bob, and $w(k)$ is the colored noise injected by Alice at time k. We assume that $s(k)$ is drawn from a finite-alphabet set, specifically, from a binary phase shift keying (BPSK) constellation for the examples throughout the paper. $u(k)$ is zero mean and unit variance Gaussian noise and the filter h is assumed to be of length l where $\|h\|^2 = 1$.

The information rate terms in the secrecy rate expression of ISI channels in (4) can be computed by the forward recursion of the Bahl-Cocke-Jelinek-Raviv (BCJR) algorithm using simulated output data [11]. In this approach, information rates are accurately estimated by sampling both a long channel input and the resulting output sequence. This simulation-based computation is readily applicable if the Gaussian terms are independent and identically distributed (i.i.d.). Hence, we apply whitening to the received signals to obtain i.i.d. Gaussian noise terms before employing this simulation based information rate estimation. The mutual information terms of

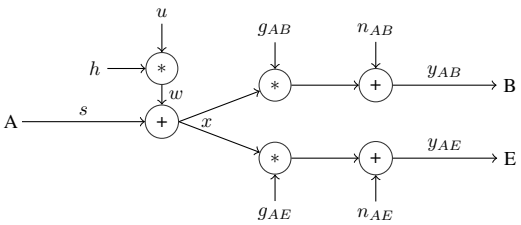

Fig. 1: The ISI fading wiretap channel with AN injection.

the whitened system are equivalent to the initial one as the whitening operation is invertible. Since the process is the same for both receivers, we only describe the whitening procedure for the legitimate receiver. In the presence of AN, the received vector at Bob is given by

$$\begin{aligned} y_B &= g_{AB} * (\sqrt{1-\alpha}s + \sqrt{\alpha}h * u) + n_{AB} \\ &= \sqrt{1-\alpha}g_{AB} * s + \underbrace{\sqrt{\alpha}g_{AB} * h * u + n_{AB}}_{e_{AB}} \end{aligned} \quad (7)$$

where $*$ is the convolution operator and e_{AB} represents the colored Gaussian noise received by Bob. We filter the received signal y_{AB} by the filter f_{AB} so that the equivalent channel representation becomes

$$\underbrace{f_{AB} * y_B}_{y_{B,eq}} = \underbrace{f_{AB} * \sqrt{1-\alpha}g_{AB}}_{g_{AB,eq}} * s + \underbrace{f_{AB} * e_{AB}}_{n_{AB,eq}}, \quad (8)$$

where the noise term $n_{AB,eq}$ is now i.i.d. Gaussian. After these transformations, we are able to employ the BCJR algorithm as in [11] directly. Since the computational complexity associated with the evaluation of information rates is determined by the length of the effective channels, i.e., $g_{AB,eq}$ and $g_{AE,eq}$, the whitening filters should be designed with the least number of taps possible.

B. Codebook-Based Filter Selection

Calculation of suitable filter coefficients for each channel realization is a computationally complex task. Thus, rather than proposing a systematic filter design according to the given main channel, we propose a simple codebook-based approach, which possesses a significantly lower complexity. We note that such codebook based schemes are commonly adopted in practice for different purposes such as reducing the amount of feedback overhead [12]. We create a codebook C with N FIR filters by randomly generating the filter coefficients. For each realization of g_{AB}, among the existing filters in the codebook C, we select the one that spectrally mismatches the main channel the most. Then, we inject AN by the use of this filter. As the dissimilarity measure of the main channel's frequency response and the filter, we propose the use of a simple metric given by

$$d_c = \sqrt{\int_{-0.5}^{0.5} \Big(|G_{AB}(f)|^2 - |H_c(f)|^2\Big)^2 df}, \quad (9)$$

where $c = 1, \ldots, N$. f denotes the normalized frequency and $|.|$ is the absolute value operator. $G_{AB}(f)$ and $H_c(f)$ are the frequency responses of the main channel and the c^{th} filter in the codebook C, respectively. After quantifying the similarity levels for all the filters in the codebook, we choose the one with the highest d_c value as our filter. In other words, the index of the filter to be used is determined as

$$\hat{c} = \arg \max_{c \in \{1,2,\ldots,N\}} d_c \quad (10)$$

One may note that other dissimilarity metrics, such as the Kullback–Leibler divergence, can also be considered, however, we adopt the metric in (9) since it is not computationally demanding.

C. Secure Transmission Strategies

We consider different AN injection strategies for the two different assumptions on the available CSI at the transmitter. First, we focus on the scenarios where the transmitter only knows the CSI of the main channel. We first create a fixed codebook C with a sufficiently large size. FIR filter coefficients in the codebook are generated independently from a standard normal distribution. For a given g_{AB}, we choose the filter that spectrally mismatches the main channel the most by choosing the filter with the highest d_c value. Once the filter is designed, the transmitter injects AN with a fixed ratio α.

For the scenarios where the CSI of the eavesdropper's channel is also available at the transmitter[2], we propose to perform an optimization over the portion of the power allocated to AN. In this case, once the filter with the highest d_c is selected from the codebook, the ergodic secrecy rate is computed for a number of α values. The α value which corresponds to the highest R_s is taken as the power portion allocated to the AN. As a result, the algorithm returns the chosen filter and the power allocation parameter for AN-aided secure transmission over finite-input ISI channels for a specific channel realization. These steps are summarized in Algorithm 1. For ergodic fading ISI channels, this procedure is repeated for all channel realizations.

Algorithm 1 The proposed algorithm for AN-aided transmission

procedure AN(g_{AB}, g_{AE}, SNR_{AB}, SNR_{AE}, C)
  Obtain the index $\hat{c}$ of the best filter in the codebook according to (10).
  for various α values **do**
    Pick a large value of N
    Generate colored noise w using filter $h_{\hat{c}}$
    Generate a realization of s, y_B and y_E
    Calculate the corresponding R_s
  end for
  Obtain the value of α which results in the highest R_s
  Output optimal $(h_{\hat{c}}, \alpha)$
end procedure

IV. Numerical Results

In this section, we provide numerical examples to show the efficacy of the proposed AN-aided transmission technique over finite-input ISI channels. First, we consider a scenario in which the channel coefficients are fixed. Then, we provide examples for (ergodic) fading ISI channels.

A. Fixed Channels Scenario

Before investigating ergodic fading ISI channels, let us consider two examples to demonstrate the simple idea behind the AN-aided strategy. In these examples, channel coefficients are fixed as $g_{AB} = [0.6320 \quad 0.7750]$ and $g_{AE} = [-0.6803 \quad 0.7330]$. Fig. 2 shows the frequency responses of

[2]This is a valid assumption for the scenarios where the eavesdropper is a registered user of the network.

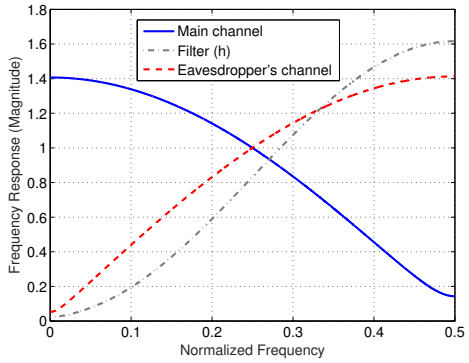

Fig. 2: An example of a suitable AN filter for a given main channel frequency response.

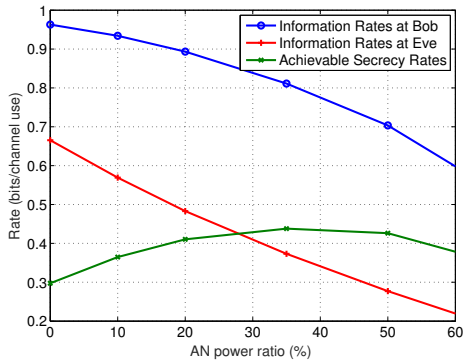

Fig. 3: Information rates and achievable secrecy rates for the example given in Fig. 2 for different AN power ratios with $SNR_{AE} = 0\ dB$ and $SNR_{AB} = 5\ dB$.

these channels along with that of a suitable AN filter with $h = [-0.4082 \quad 0.8165 \quad -0.4082]$.

In the first example, we fix the SNR values at the legitimate receiver and the eavesdropper as $0\ dB$ and $5\ dB$, respectively. Then, we evaluate the information rates over the legitimate receiver and the eavesdropper for different portions of power allocated to AN. It is observed that injecting AN in the proposed manner results in a relatively small degradation in the information rates of the legitimate receiver whereas it considerably disrupts the reception at the eavesdropper and, as a result, improved secrecy rates are attained as verified in Fig. 3, which shows that achievable secrecy rate is a function of the AN power ratio and it has a maximum for a certain value of α. Therefore, it is possible to maximize the achievable secrecy rates by optimizing the AN power ratio.

In the second example, for the same channel and filter coefficients and with fixed SNR at the legitimate receiver, we evaluate achievable secrecy rates by considering different SNR values at the eavesdropper. Fig. 4 clearly demonstrates the dependence of the optimal AN power ratio α on the SNR value at the eavesdropper. More specifically, it is shown that the optimal AN power increases for the eavesdroppers with

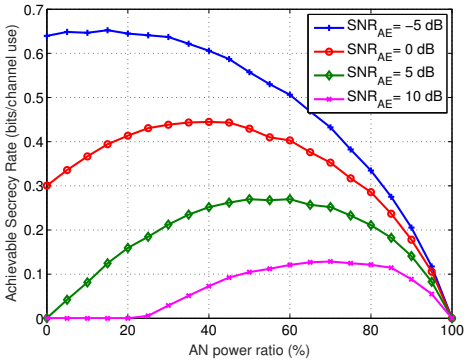

Fig. 4: Achievable secrecy rate results for the example given in Fig. 2 for different AN power ratios with different SNR_{AE} values when $SNR_{AB} = 5\ dB$.

higher SNRs. This observation is consistent with the results in [13]-[14], which demonstrate that for wiretap channels driven by finite-alphabet inputs, the higher the SNR, the higher is the optimal fraction of power allocated to the artificial noise. Moreover, this observation underlines the necessity for optimization of the portion of power allocated to AN, as is addressed by Algorithm 1. One may note this behavior is different for the cases of Gaussian channel inputs where secrecy rate is a concave function of the SNR (see, e.g., Fig. 2 in [7]).

B. Ergodic Fading ISI Channels

In the previous examples, for illustrative purposes, we considered a scenario in which the channel coefficients are fixed and their spectra are considerably different from each other. We now provide examples for ergodic fading ISI channels by averaging the secrecy rates over many realizations of the channels. These include various pairs where the spectral difference between the channels are small (dissimilar to the extreme case in Fig. 3).

We consider two examples with different SNRs, and we evaluate the average $\bar{R}_s$ by considering the instantaneous R_s values over 500 realizations of the channels. We set the sequence length to $n = 10^5$. The channel coefficients for the main and eavesdropper's channels are generated with respect to the multi-path delay profiles $p_{AB} = [0.7311 \quad 0.2689]$ and $p_{AE} = [0.2689 \quad 0.7311]$. In order to inject colored AN, we employ a filter of length $l = 3$. For this example, we find that 6-tap FIR filters possess sufficient accuracy to whiten the channels, resulting in equivalent 7-tap channels. One should note that, in this case, computational complexity increases as we need to employ the sum-product algorithm for the equivalent 7-tap channels instead of 2-tap channels. However, the overall computational complexity is still very manageable (e.g., compared to [4]) as only a few evaluations of the information rates are required for implementation of Algorithm 1.

In the first example, we set $\text{SNR}_{AE} = 0\ dB$ and sweep the main channel SNR value from $-5\ dB$ to $15\ dB$. The optimal

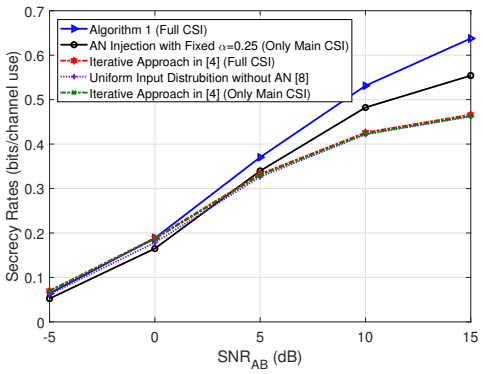

Fig. 5: Ergodic secrecy rates under different CSI assumptions and transmission schemes for $\text{SNR}_{AE} = 0\ dB$.

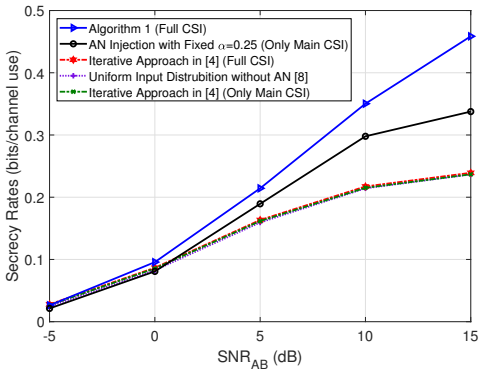

Fig. 6: Ergodic secrecy rates under different CSI assumptions and transmission schemes for $\text{SNR}_{AE} = 5\ dB$.

filter is selected from a codebook of size $N = 100$ where the value of N is chosen large enough not to reduce filter diversity but not too large so as to preserve the low complexity nature of the algorithm. In the implementation of Algorithm 1, after obtaining the AN filter that spectrally mismatches the main channel the most, we evaluate R_s with five different values of α and select the one resulting in the highest R_s value. We also implement the proposed AN injection scheme in the scenarios with the main channel CSI only. In this case, once a suitable AN injection filter is obtained, the AN is injected with a fixed and predetermined power allocation ratio. We take $\alpha = 0.25$ for all channel realizations and all the SNR values in this case. Furthermore, so as to evaluate the achievable secrecy rates with the iterative approach of [4], we consider Markov inputs of order 1.

Fig. 5 compares the achievable secrecy rates by the proposed AN-aided scheme with those of the iterative approach in [4]. These results reveal that, while the iterative approach only slightly improves the achievable secrecy rates, the AN-aided transmission schemes provide significant enhancements. We also observe that the transmitter's knowledge on the Eve's CSI results in considerably higher secrecy rates since the transmitter can optimize the portion of power allocated to the AN with this knowledge. In contrast, there are no significant benefits of availability of Eve's CSI for the iterative approach.

In the second example, we increase the eavesdropper's SNR to $5\ dB$ in Fig. 6. We observe that the same conclusions are valid for this case, as well. In addition, we observe that AN injection is more effective when compared to the previous case as it plays a more vital role in suppressing the information rates at the eavesdropper operating at a higher SNR. In this example, the CPU times needed to evaluate d_c and obtain a suitable filter from a codebook of size 100 is about 0.3 seconds on an Intel Core-i7-4770, 3.4 GHz processor which clearly shows that the newly proposed scheme is computationally inexpensive.

V. Conclusion

In this paper, we have proposed a secure transmission scheme over ISI wiretap channels which relies on injection of colored artificial noise whose spectrum has the least match with the frequency response of the main channel. The method is inspired by the information theoretic results on signaling over ISI channels, and it has a very low complexity. Our numerical results demonstrate its efficacy in improving the secrecy rates over both fixed and fading ISI channels.

References

[1] S. Hanoglu, "Secrecy rates of finite-input intersymbol interference channels," M.S. thesis, Dept. Elec. and Electron. Eng., Bilkent Univ., Ankara, Turkey, 2016.

[2] A. D. Wyner, "The wire-tap channel," *The Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[3] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*, Delft, The Netherlands: Now Publishers, 2009.

[4] Y. Sankarasubramaniam, A. Thangaraj, and K. Viswanathan, "Finite-state wiretap channels: Secrecy under memory constraints," in *IEEE Inform. Theory Workshop*, Volos, Greece, Oct. 2009, pp. 115-119.

[5] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise, "*IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, June 2008.

[6] S. Rezaei Aghdam and T. M. Duman, "Low complexity precoding for MIMOME wiretap channels based on cut-off rate," *IEEE Int. Symp. Inf. Theory (ISIT)*, Barcelona, 2016, pp. 2988-2992.

[7] H. Qin, Y. Sun, T. H. Chang, X. Chen, C. Y. Chi, M. Zhao, and J. Wang, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2717-2729, June 2013.

[8] D. N. Doan and K. R. Narayanan, "Design of good low-rate coding schemes for ISI channels based on spectral shaping," *IEEE Trans. on Wireless Commun.*, vol. 4, no. 5, pp. 2309-2317, Sep. 2005.

[9] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.

[10] M. Bloch and J. N. Laneman, "On the secrecy capacity of arbitrary wiretap channels," in *Proc. 46th Allerton Conf. Commun., Control, Comput.*, Monticello, IL, Sep. 2008, pp. 818-825.

[11] D. Arnold and H. A. Loeliger, "On the information rate of binary-input channels with memory," in *IEEE Int. Conf. Commun.*, Helsinki, Finland, vol. 9, 2001, pp. 2692-2695.

[12] 3GPP TS 36.211, V0.3.1; "Physical Channels and Modulation (Release 8)" (2007-02).

[13] S. Bashar, Z. Ding, and C. Xiao, "On the secrecy rate of multi-antenna wiretap channel under finite-alphabet input," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 527-529, May 2011.

[14] S. Rezaei Aghdam and T. M. Duman, "Joint precoder and artificial noise design for MIMO wiretap channels with finite-alphabet inputs based on the cut-off rate," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3913-3923, Jun. 2017.