Performance Analysis of Transmission Over AWGN Wiretap Channels With Practical Codes

Marco Baldi[1], Nicola Maturo[1], Stefano Tomasin[2]

[1]Università Politecnica delle Marche, Ancona, Italy, {m.baldi; n.maturo}@univpm.it

[2]University of Padua, Padua, Italy, tomasin@dei.unipd.it

I. Introduction and Problem Statement

The achievable secure information rate is known for several wiretap channel models. However, only a few practical code constructions are available up to now. Moreover, these few proposals are focused on discrete channels [1], while no solution is available for continuous-output channels. We propose a pragmatic solution to assess and optimize the performance achievable by practical coding and modulation schemes over additive white Gaussian noise (AWGN) wiretap channels.

II. Proposed Solution Outline

We consider a system where Alice encodes a message $\mathcal{M}$ of k bits scrambled with random bits [3] and encoded with an error correcting code with finite codeword length. The encoded bits are then QAM modulated before transmission. The message must be reliably decoded by Bob, while remaining secret to the eavesdropper agent Eve. Channels between Alice and Bob, and Alice and Eve are AWGN with independent noise samples.

In order to study the performance of this scheme, we consider the equivocation rate measured at the eavesdropper, as derived in [2], i.e.,

$$\rho_e = \frac{1}{n}\left[\mathrm{H}(X^n) - \mathrm{I}(X^n; Z^n) + \mathrm{H}(\mathcal{M}|Z^n, X^n) - \mathrm{H}(X^n|\mathcal{M}, Z^n)\right] , \tag{1}$$

where X^n is the n-bit transmitted codeword, Z^n is the vector of n real-valued samples received by Eve from the channel, $\mathrm{H}(\cdot)$ denotes the entropy function, and $\mathrm{I}(\cdot,\cdot)$ denotes the mutual information. We suppose to use a code with dimension l, $k \le l < n$, therefore the code rate is $\rho_c = l/n$ and the secret rate is $\rho_s = k/n \le \rho_c$. The remaining $l-k$ information bits are padded with the random bits, and scrambled in order to avoid systematic transmission. Then we have $\mathrm{H}(X^n) = \ell$, $\mathrm{H}(M|Z^n, X^n) \le \mathrm{H}(\mathcal{M}|X^n) = 0$.

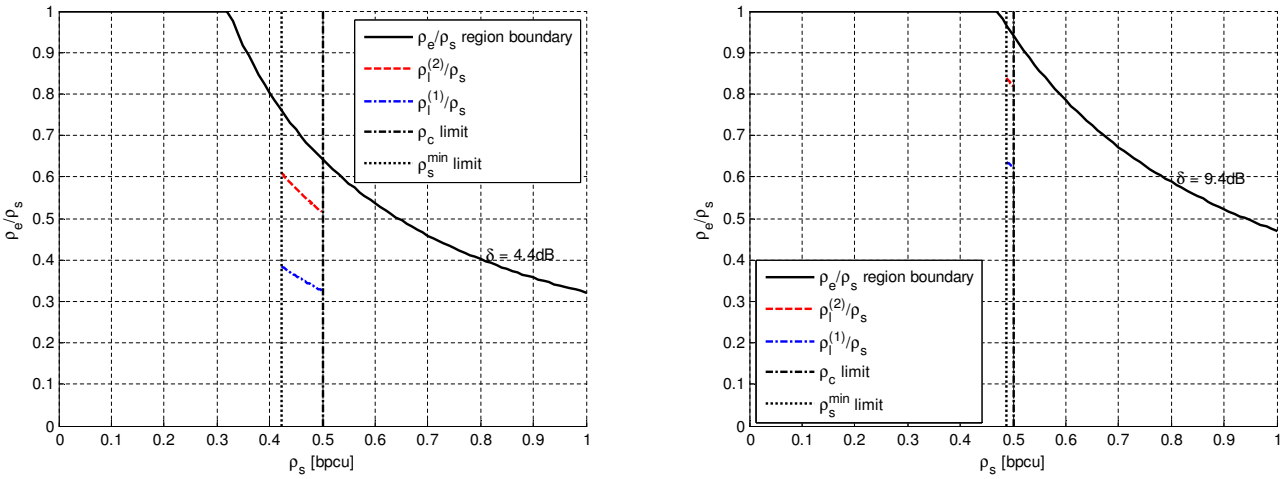
Let $\eta(\rho_s)$ be the codeword error rate (CER) experienced by a fictitious receiver at the wiretapper position trying to decode for X^n from observing Z^n and $\mathcal{M}$. By Fano inequality we have $\mathrm{H}(X^n|\mathcal{M}, Z^n) \le 1 + (\ell - k)\eta(\rho_s)$. In [2] $\mathrm{I}(X^n; Z^n)$ is upper bounded by nC_E, where C_E is the input-constrained Eve's channel capacity, and a (indeed rather loose) lower bound on ρ_e is obtained, i.e.,

$$\rho_e \ge \rho_c - C_E - (\rho_c - \rho_s)\eta(\rho_s) - \frac{1}{n} = \rho_l^{(1)} . \tag{2}$$

In order to obtain a more realistic bound, we observe that the finite length coding is also a drawback for Eve, as it conveys a reduced mutual information on the secret message bits with respect to capacity-achieving coding. We can take this fact into account by modeling the concatenation of the AWGN channel and Eve's decoder as a binary symmetric channel (BSC) with bit error rate (BER) equal to that experienced by Eve after decoding. In this case, instead of C_E, we consider the mutual information between the transmitted codeword X^n and the n-bit vector $\hat{Z}^n$ obtained at the output of Eve's practical decoder (belief propagation decoder for low-density parity-check (LDPC) codes). The corresponding bound on the fractional equivocation rate is:

$$\rho_e \ge \rho_c - \mathrm{I}(X^n; \hat{Z}^n) - (\rho_c - \rho_s)\eta(\rho_s) - \frac{1}{n} = \rho_l^{(2)} \ge \rho_l^{(1)} . \tag{3}$$

For estimating $\mathrm{I}(X^n; \hat{Z}^n)$ we use semi-analytical methods (details in the presentation).



(a) (b)

Fig. 1. Fractional equivocation rate (ρ_e/ρ_s) bounds for (a) a rate-0.5 LDPC code with BPSK modulation and (b) a rate-0.5 LDPC code with 16-QAM modulation.

III. Preliminary Numerical Results and Conclusions

We consider LDPC codes as error correcting codes. In order to be sure that Eve's uncertainty is concentrated on the secret message, we require that $\eta(\rho_s)$ is small. By setting $\eta(\rho_s) \leq 10^{-3}$, and using codes with $n > 10^3$, the two last terms in the expressions of $\rho_l^{(1)}$ and $\rho_l^{(2)}$ become negligible.

The parameters of the considered coded modulation schemes are summarized in Table I. The value of $\rho_s^{\min}$ has been found by imposing that $\eta(\rho_s^{\min}) = 10^{-3}$ at Eve's signal-to-noise ratio (SNR) per bit $\frac{E_b^{(E)}}{N_0}$. Obviously, for any secret rate value $\rho_s : \rho_s^{\min} \leq \rho_s \leq \rho_c$, this condition remains valid. Bob's SNR per bit $\left(\frac{E_b^{(B)}}{N_0}\right)$ has been fixed such that his CER is $\leq 10^{-4}$, which is a reasonable reliability target.

TABLE I
Parameters of the considered LDPC coded modulation schemes.

Scheme	n	ρ_c	$\rho_s^{\min}$	Mod.	$\frac{E_b^{(B)}}{N_0}$	$\frac{E_b^{(E)}}{N_0}$
1	2364	0.5	0.423	BPSK	2.2 dB	-2.2 dB
2	4096	0.5	0.488	16-QAM	4.8 dB	-4.6 dB

Fig. 1 shows the fractional equivocation rate (ρ_e/ρ_s), where δ denotes the SNR ratio between Bob and Eve, and the fractional equivocation rate region boundary has been computed as $\min\{1, C_b/\rho_s\}$, with C_b being the input-constrained secrecy capacity. As we observe from the figure, both the considered LDPC coded modulation schemes are able to transmit secret messages at a rate which is not far from the equivocation rate at Eve's. In particular, the longest LDPC code, together with 16-QAM modulation, is able to achieve a fractional equivocation rate > 0.8, which is a good result from the security standpoint. These preliminary results suggest that using long LDPC codes together with high order modulation schemes should allow to approach the ultimate performance achievable by practical finite length coding schemes in terms of security at the physical layer.

References

[1] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," in *Proc. IEEE International Symposium on Information Theory (ISIT 2010)*, Austin, TX, Jun. 2010, pp. 913–917.

[2] C. W. Wong, T. F. Wong, and J. M. Shea, "Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel," 2011, to appear in the *IEEE Trans. Inf. Forensics Security*.

[3] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 883–894, Jun. 2012.