Achievable Secrecy Rates in Physical Layer Secure Systems with a Helping Interferer

Arsenia Chorti[†,*], *Member, IEEE*, H. Vincent Poor[†], *Fellow, IEEE*
[†]Department of Electrical Engineering, Princeton University, Princeton, New Jersey 08544, US
[*] Institute of Computer Science (ICS) of the Foundation for Research and Technology - Hellas
N. Plastira 100, Vassilika Vouton, GR-700 13 Heraklion, Crete, Greece
{achorti, poor}@princeton.edu

***Abstract*—Various physical-layer techniques have so far been proposed to achieve perfect secrecy in wireless communication systems. In this framework, an approach is investigated to enhance secrecy using a helping interferer transmitted by a friendly node in the network, aiming at confusing a passive eavesdropper. Commonly, such physical layer security approaches rely on the injection of a noise-like signal to intentionally degrade the eavesdropper capacity. Instead, the use of a jamming signal with the same probability mass function as that of the actual data is proposed here. The gains of this approach are investigated via extensive symbol error rate measurements and evaluations of the achievable secrecy rates.**

I. Introduction

Recently, physical layer security approaches have gained renewed interest as promising candidates to enhance the secrecy of wireless communication systems. The pioneering works of Wyner [1] and Csiszár and Körner [2] have demonstrated that a noisy communication channel offers opportunities for non-zero rate secure communication when the eavesdropper's channel is on average a degraded version of the main channel. Analyses for the wireless fading channel [3] and Multiple-Input Multiple-Output (MIMO) systems [4] have established positive secrecy capacities for such systems even when on average the eavesdropper's channel can be better than that of the legitimate user.

In these approaches, the transmitter needs to know the Channel Impulse Response (CIR) at least between the transmitter and the legitimate receiver so that it can adapt the transmission rate accordingly, thus achieving a positive secrecy capacity. However, from a communication system point of view, the variable transmission rate might not be suitable for a number of applications, while the need for a feedback channel to provide the transmitter with the CIR is also disadvantegeous.

Alternatively, helping-interferer approaches [5], [6], [7], [8] have been proposed, making use of the idea of intentionally degrading the eavesdropper channel. In this paper, we investigate the design of the jamming signal in a helping interferer physical layer security approach. Unlike previous work, we argue that the interfering signal should not be drawn from a Gaussian distribution but rather should share the statistical properties of the data signal which is typically Binary Phase Shift Keying (BPSK) or M-ary Quadrature Amplitude Modulation (M-QAM) with a uniform probability mass function (pmf). We demonstrate the gains of this approach by evaluation of the actual secrecy rates in the investigated systems. Towards this end, we employ the gap approximation [9] in order to address the over/under-estimation of previous analyses based on the channel capacities.

II. Physical Layer Security

We assume a communication system in which length N observation vectors are obtained at the outputs of matched filters at the legitimate and eavesdropping receivers:

$$\mathbf{z}_{l/e} = \mathbf{D}_{l/e}\mathbf{d} + \mathbf{n}_{l/e}. \tag{1}$$

The indices l and e correspond to the legitimate receiver and the eavesdropper respectively, while the $N \times N$ matrices $\mathbf{D}_{l/e}$ denote the respective legitimate user and eavesdropper channel matrices; $\mathbf{d} = [d_1, \ldots, d_N]^T$ is a sequence of independent and identically distributed (i.i.d.) symbols d_i, typically BPSK or M-QAM transmitted symbols, and $\mathbf{n}_{l/e} = [n_{1,l/e}, \ldots, n_{N,l/e}]^T$ are length N noise vectors of i.i.d. Gaussian random variables with variances $\sigma^2_{n,l/e} = \frac{N_{0,l/e}}{2}$.

The idea of physical layer security is based on *a priori* knowledge of $\mathbf{D}_l$ and $\mathbf{D}_e$. If this information is available, we can establish a maximal rate of perfectly secure transmission of information, known as the secrecy capacity, simply using the difference of the capacities of the legitimate and eavesdropper channels, i.e [10]:

$$\begin{aligned} C_s &= (C_l - C_e)^+ \\ &= \left(\log_2 \det(\mathbf{I} + \gamma_l \mathbf{D}_l \mathbf{D}_l^H) - \log_2 \det(\mathbf{I} + \gamma_e \mathbf{D}_e \mathbf{D}_e^H)\right)^+ \\ &= \sum_{i=1}^{N} \left(\log_2 \frac{1+\gamma_l \lambda_i}{1+\gamma_e \xi_i}\right)^+, \end{aligned} \tag{2}$$

with γ_l and γ_e denoting the SNR of the forward and wiretap channels, respectively, and λ_i and ξ_i denoting the eigenvalues of $\mathbf{D}_l\mathbf{D}_l^H$ and $\mathbf{D}_e\mathbf{D}_e^H$, respectively. Finally, $(\cdot)^+ = \max(\cdot, 0)$.

Clearly, for those subchannels for which $\gamma_l\lambda_i > \gamma_e\xi_i$, we can transmit in perfect secrecy at a maximal rate of $\log_2 \frac{1+\gamma_l\lambda_i}{1+\gamma_e\xi_i}$ if the i-th data symbol d_i is drawn from a Gaussian distribution. Thus, knowledge of the legitimate and eavesdropper channels is necessary.

A principal disadvantage of the previous scenario is the fact that knowledge of the eavesdropper channel is a very stringent

This work was funded in part by the IOF "APLOE" (PIOF-GA-2010-274723) grant within the 7th Framework Program of the European Community and in part by the U. S. National Science Foundation Grant CNS-09-05398.

requirement. Alternatively, opportunistic approaches can be built based on estimates of the eavesdropper channel [11]. However, these may lead to unsatisfactorily low data rates.

Therefore, when trying to exploit the *true* randomness of the wireless channel, we are left with a number of open issues that cannot be resolved, unless we have an abundance of spectral resources and apply state of the art encoding, e.g. polar codes [12]. Unfortunately, such approaches again may limit substantially the overall throughput while even more importantly they can require a significant increase in the transceiver complexity. Two questions that naturally arise are: can we tune γ_l, γ_e, λ_is or ξ_is in an orderly, predefined manner? Can we achieve this goal with minimal (or *acceptable*) extra overhead and added complexity?

III. Helping Interferer Strategies

Helping interferer strategies rely on intentionally injecting - with the help of a friendly node in the network - a noise-like signal that degrades γ_e to a *greater* extent than the respective degradation of γ_l. From the eavesdropper's point of view, any such noise-like jammer is equivalent to having a random secret key superimposed on the transmitted data.

For simplicity, and without loss of generality, in the following let us assume a scenario in which a friendly jammer is located close to the eavesdropper but sufficiently far from the legitimate user. In an ideal Additive White Gaussian Noise (AWGN) channel the legitimate user and the eavesdropper observations[1] can be expressed as

$$z_l = d + \sigma_{n,l} n_l, \qquad (3)$$

$$z_e = d + \sigma_i i + \sigma_{n,e} n_e, \qquad (4)$$

where i denotes the projection of the helping interferer on the signal space[2] and $n_{l/e}$ are circularly Gaussian noise variables with variances $\sigma^2_{n,l/e}$.

In helping interferer physical layer security scenarios, it is typical to assume that i and $n_{l/e}$ are drawn from Gaussian probability density functions (pdfs). On the other hand d is typically drawn from a uniform probability mass function (pmf) with zero mean and variance σ_d^2, a scenario including M-ary Phase Shift Keying (M-PSK) and M-QAM. If the system employs BPSK modulation with unit energy per bit $E_b = \sigma_d^2 = 1$, the probability of the eavesdropper making an erroneous decision in the presence of a Gaussian Interferer (GI) is then simply:

$$P_{b,GI} = Pr(\hat{d} \neq d) = \frac{1}{2}\mathrm{erfc}\left(\frac{\mathrm{d}_{\min}/2}{\sqrt{2}(\sigma_i + \sigma_{n,e})}\right), \qquad (5)$$

where $\mathrm{erfc}(\cdot)$ denotes the complementary error function and $\mathrm{d}_{\min} = 2\sqrt{E_b}$ is the minimum distance in the BPSK constellation.

The outlined approach is practically equivalent to one-time pad encryption using a Gaussian key. In effect, we are decreasing γ_e in (2) to the value $\gamma_e = \frac{\sigma_d^2}{\sigma_i^2 + \sigma_{n,e}^2}$. The major advantage however when compared to a classical one-time pad is that the legitimate user does not need to share a secret key with the helping node as long as this secondary transmission does not degrade γ_l severely .

TABLE I
White BPSK Jammer

T_x	-1	-1	1	1
J_x	-1	1	-1	1
E_x	-2	0	0	2
$\hat{d}$	-1	?	?	1

Now, let us assume that the friendly node is instead using a jamming signal that has similar statistical properties to that of the *data* instead of the *noise*. The motivation behind following this approach is the following: The channel capacity is maximal when transmission occurs in the presence of white Gaussian noise. Therefore, if we want to intentionally decrease the eavesdropper channel capacity then the signals received at the eavesdropper end should deviate from Gaussianity. In effect, the minimization of the mutual information between the transmitter and the wiretapper suggests that the jammer should mimic the data pmf. A simple illustrative example follows assuming a BPSK system.

A. Case Study for a BPSK System

Let us revisit the scenario described in (3) and (4) with the jammer i being a BPSK signal with variance $\sigma_i^2 = 1$. Table I depicts the possible combinations in a hypothetical noiseless scenario ($\sigma^2_{n,e} = 0$) where the transmitter T_x and the jammer J_x transmit BPSK symbols $d = \pm 1$. The eavesdropper E_x is able to identify the transmitted symbol with certainty only in 50% of the cases. In this scenario, for the eavesdropper the probability of making an erroneous estimate is 25% so that the bit error rate (BER) is 0.25. On the other hand, if a GI of the same variance as the signal was used instead, then the eavesdropper's BER would be 0.1624.

Examining this scenario in greater detail, the eavesdropper observes a statistic z_e in the presence of a random variable $w = \sigma_i i + \sigma_{n,e} n_e$ whose pdf is a mixture of two Gaussians (scaled by $\frac{1}{2}$ and with the same variance as n_e) centered on the possible values of i, which for a BPSK Uniform Interferer (UI) will be $\pm\sigma_i$.

Due to symmetry, the decision regions of the Maximum Likelihood (ML) detector at the eavesdropper remain unchanged as the two half lines around the mid-distance point between the transmitted symbols. The probability of the eavesdropper making an erroneous decision is consequently expressed as

$$\begin{aligned} P_{b,UI} &= Pr(\hat{d} \neq d) \\ &= \frac{1}{4}\left[\mathrm{erfc}\left(\frac{\mathrm{d}_{\min}/2 - \sigma_i}{\sqrt{2}\sigma_{n,e}}\right) + \mathrm{erfc}\left(\frac{\mathrm{d}_{\min}/2 + \sigma_i}{\sqrt{2}\sigma_{n,e}}\right)\right]. \end{aligned} \qquad (6)$$

As long as (6) is larger than (5), a UI strategy is advantageous compared to a GI strategy. This effect is illustrated in the BER

[1] The observations are in general vectors, but here are reduced to scalars for simplicity.

[2] Without loss of generality we have assumed that all variables involved are normalized to the data standard deviation.

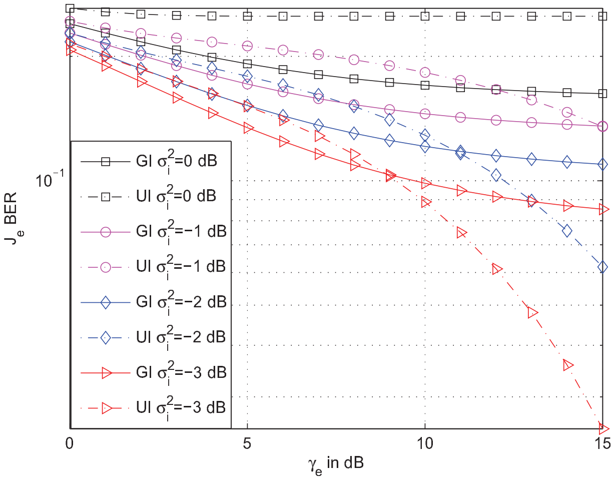

Fig. 1. BER at the eavesdropper for a UI and GI helping interferer strategies in a BPSK system. $E_b = 1$ and $\gamma_e = \sigma_{n,e}^{-2}$.

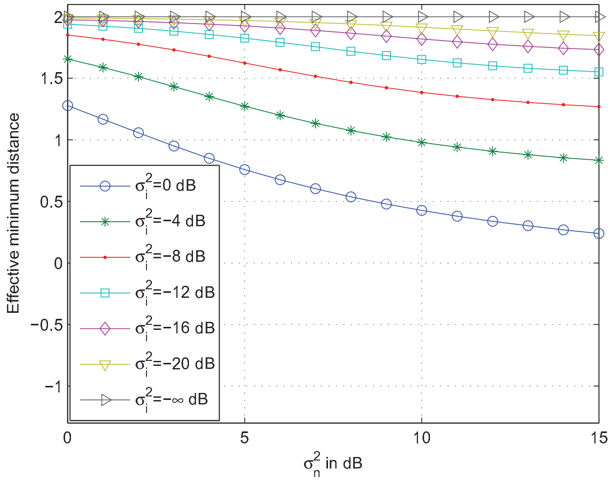

Fig. 2. Effective minimum distance in a BPSK constellation when using a UI jammer of normalized power σ_i^2.

curves depicted in Fig. 1. In the low and medium SNR regions there is a clear gain in pursuing a UI strategy.

The deterioration of the eavesdropper's error performance can be quantified by estimating the corresponding decrease in the effective minimum distance in the constellation lattice due to the use of the UI, evaluated in (7):

$$\mathrm{d}_{\mathrm{eff}} = 2\sqrt{2}\sigma_{n,e}\mathrm{erfc}^{-1}(2P_{b,UI}(\sigma_i, \sigma_{n,e})). \tag{7}$$

The nominal minimum distance in this case study is $\mathrm{d}_{\min} = 2\sqrt{E_b} = 2$. There is a substantial decrease in the lattice effective minimum distance as depicted in Fig. 2. In effect, instead of increasing the denominator of the argument of the complementary error function, we are decreasing the numerator, in a sense decreasing the eavesdropper eigenvalues in (2).

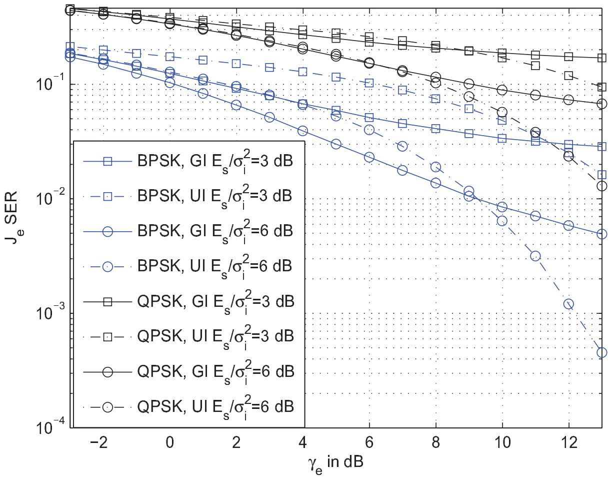

Fig. 3. Eavesdropper SER in the presence of a UI interferer of normalized power σ_i^2 in BPSK and 4-QAM systems.

IV. Generalization to M-PAM and M-QAM UI

The generalization of using a jammer that shares the statistical properties of the data symbol (denoted as the UI strategy in the following) in the case of M-ray Pulse Amplitude Modulation (M-PAM) is straightforward. Assuming the case of an M-PAM data symbol, an M-PAM jammer of relative power σ_i^2 results in the reception of an observation z_e whose pdf is a mixture of M Gaussians, scaled by a factor of $\frac{1}{M}$, centered on $\pm\sigma_i(2m-1-M), m = 1, \ldots, M$. As a result, the eavesdropper's Symbol Error Rate (SER) can be expressed in closed form as

$$P_M = \frac{2(M-1)}{M^2}\sum_{m=1}^{M} Q\left(\frac{d_{\min}/2 + \sigma_i(2m-1-M)}{\sigma_{n,e}}\right). \tag{8}$$

Correspondingly, the SER of a rectangular M-QAM signal on which acts an M-QAM jammer is derived by perceiving this two-dimensional modulation as two orthogonal $\sqrt{M}$-PAMs and evaluating the SER as [13]

$$P_M = 1 - (1 - P_{\sqrt{M}})^2 \tag{9}$$

where $P_{\sqrt{M}}$ is given in (8). In Figs. 3 and 4 we provide a comparison of the eavesdropper SER for varying σ_i^2 and $\gamma_e = \frac{\sigma_d^2}{\sigma_{n,e}^2}$ in BPSK, 4-QAM, 16-QAM and 64-QAM systems. A substantial deterioration of the eavesdropper SER can be achieved for low and medium SNRs in all cases examined.

V. Evaluation of Secrecy Rates Using the Gap Approximation

The increase in the eavesdropper probability of symbol error is an important indication of the potential advantages in designing jamming signals tailored to the specifications of the communication system. However, the true figure of merit to judge whether this customization is worth undertaking is the actual achievable rate and the secrecy rate in particular. Currently, such evaluations rely on the theoretical bound of the system secrecy capacity. Although the secrecy capacity offers

TABLE II
ACHIEVABLE RATES OF UNCODED MODULATION SCHEMES AS A FUNCTION OF THE SNR GAP

BPSK	$R_b = \frac{\text{SNR}}{\Gamma(P_M)} \simeq \log_2\left(1 + \frac{\text{SNR}}{\Gamma(P_M)/(\ln(2)}\right)$	$\Gamma(P_M) = \left[Q^{-1}(P_M)\right]^2/2$
M-PAM, $M > 2$	$R_b = \frac{1}{2}\log_2\left(1 + \frac{\text{SNR}}{\Gamma(P_M,M)}\right)$	$\Gamma(P_M, M) = \left[Q^{-1}\left(\frac{MP_M}{2(M-1)}\right)\right]^2/6$
M-PSK , $M > 2$	$R_b = \frac{1}{2}\log_2\left(\frac{\text{SNR}}{\Gamma(P_M,M)}\right)$	$\Gamma(P_M, M) = \left[\frac{Q^{-1}(P_M/2)}{\sqrt{2}\pi}\right]^2$
M-QAM	$R_b = \log_2\left(1 + \frac{\text{SNR}}{\Gamma(P_M)}\right)$	$\Gamma(P_M) = \Big[Q^{-1}\big((P_M/4\big)\big]^2/3$

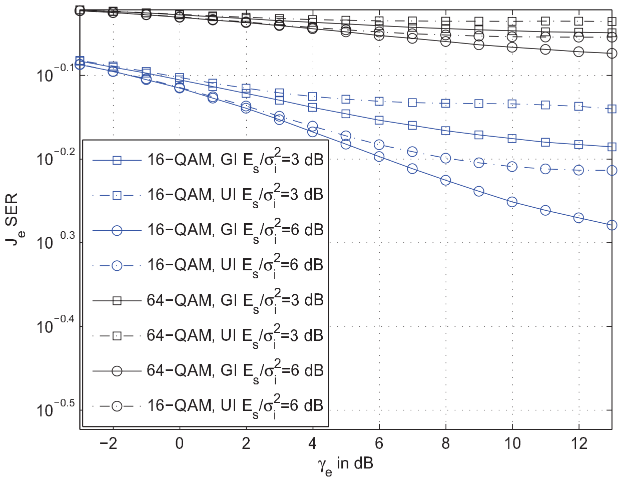

Fig. 4. Eavesdropper SER in the presence of a UI interferer of normalized power σ_i^2 in 16-QAM and 64-QAM systems.

invaluable insight in terms of upper bounds, it not readily applicable in the case of systems employing BPSK or M-QAM modulation. To overcome this obstacle, we propose here the use of the gap approximation in order to estimate the actual achievable secrecy rates.

The gap [9] corresponds to the effective penalty in SNR (and therefore in the achievable rate) due to the use of a suboptimal input signal with a uniform pmf and is extensively used in bit-loading algorithms. Closed form expressions have been presented for M-QAM [14] and M-PSK signals with $M > 2$ [15]. To complement these results, we present a derivation of the gap in the case of BPSK. The expressions are summarized in Table II for convenience.

To evaluate the achievable rate for BPSK signals, we start with the expression for the probability of bit error (which here coincides with the probability of symbol error), $P_b = P_M$, noting that in all modulations $\frac{E_b}{N_0} = \frac{1}{\log_2 M}\frac{E_s}{N_0}$:

$$\begin{aligned} P_M &= Q\left(\sqrt{\frac{2E_b}{N_0}}\right) = Q\left(\sqrt{\frac{2E_s}{\log_2 MN_0}}\right) \Rightarrow \\ R_b &= \frac{\text{SNR}}{\Gamma(P_M)} \simeq \log_2\left(1 + \frac{\text{SNR}}{\Gamma(P_M)/\ln(2)}\right), \end{aligned} \tag{10}$$

where $R_b = \log_2 M$ is the bit-rate in bits/sec/Hz and the gap is expressed as $\Gamma(P_M) = \left[Q^{-1}(P_M)\right]^2/2$ with $Q(x) = \frac{1}{2}\text{erfc}\left(\frac{x}{\sqrt{2}}\right)$. Unlike other modulation schemes, the rate is linear in the SNR and inversely proportional to the gap, while it is possible to obtain an approximation for $\frac{\text{SNR}}{\Gamma(P_M)/\ln(2)} \ll 1$.

Based on the previous analysis, the *achievable secrecy rate* of a BPSK or M-QAM scheme is then expressed as

$$R_s = (R_l - R_e)^+. \tag{11}$$

In the case of GI, the expressions in Table II can be directly applied to evaluate the secrecy rate R_s. However, in the case of the UI, a further manipulation is necessary in order to determine the effective system SNR. Towards this end we will rely on a union bound approximation for a baseline M-PAM constellation in a relatively high SNR regime. This approximation will then be directly applicable to BPSK and M-QAM.

In M-PAM systems, the SNR can be expressed as

$$\frac{E_s}{N_0} = \frac{\text{d}^2 E_g(M^2-1)}{6N_0}, \tag{12}$$

where E_g is the carrier waveform power, here taken to be $E_g = 0.5$ Watts for a sinusoidal carrier, and d denotes the distance between the constellation points. When the SNR is high, in (12) we can disregard all but the closest neighboring points (which are now effectively located at $\text{d}_{\min} \pm \sigma_i$). As a result, we may approximate the effective SNR as

$$\frac{E_s}{N_0}eff \simeq \frac{E_s - \sigma_i^2}{4N_0}. \tag{13}$$

We employ (13) in the evaluation of the achievable rate in the eavesdropper in the presence of a UI jammer. The gain or loss in using a UI instead of a GI in terms of secrecy rates is then straightforwardly given as

$$\Delta R_s = R_{e,UI} - R_{e,GI}, \tag{14}$$

where $R_{e,UI}$ and $R_{e,GI}$ denote the achievable rates at the eavesdropper in the presence of a UI and GI jammer respectively.

In Figs. 5, 6, 7 and 8 we present the achievable secrecy rates for BPSK, 4-QAM, 16-QAM and 64-QAM systems. The achievable secrecy rates are higher when a UI strategy is applied instead of a GI strategy at low and medium SNRs.

VI. CONCLUSIONS AND FUTURE WORK

In this paper we have investigated an alternative approach in the framework of physical layer security using a helping interferer. We have examined the possibility of using - with the aid of a helping node in the network - a jammer with similar statistical properties to that of the actual data signal instead of a noise-like jammer as is commonly considered in the literature. We have demonstrated that for low and medium SNRs there is a clear gain in terms of the invoked SER at

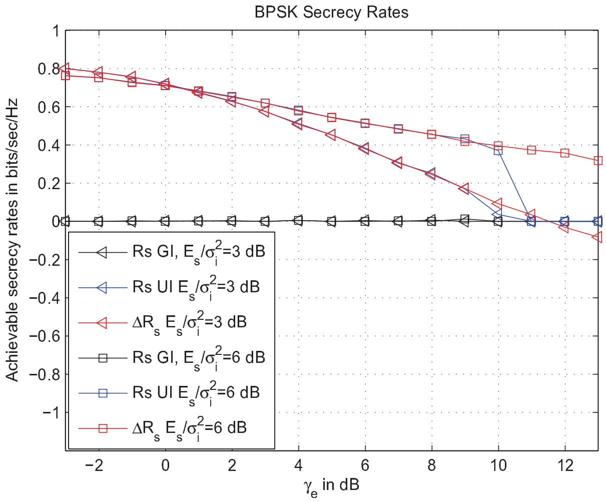

Fig. 5. Achievable secrecy rates R_s for a BPSK system.

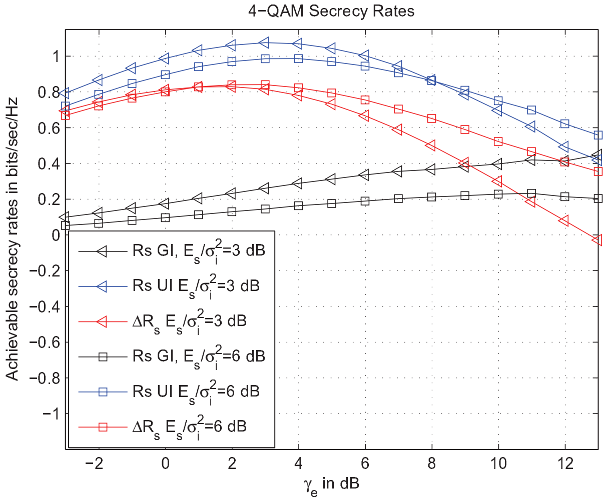

Fig. 6. Achievable secrecy rates R_s for a 4-QAM system.

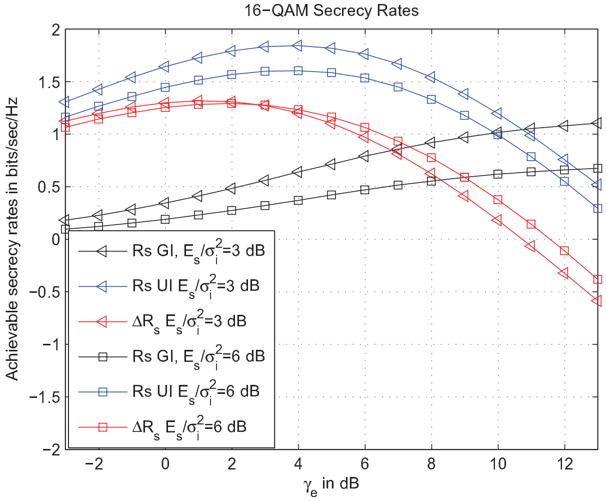

Fig. 7. Achievable secrecy rates R_s for a 16-QAM system.

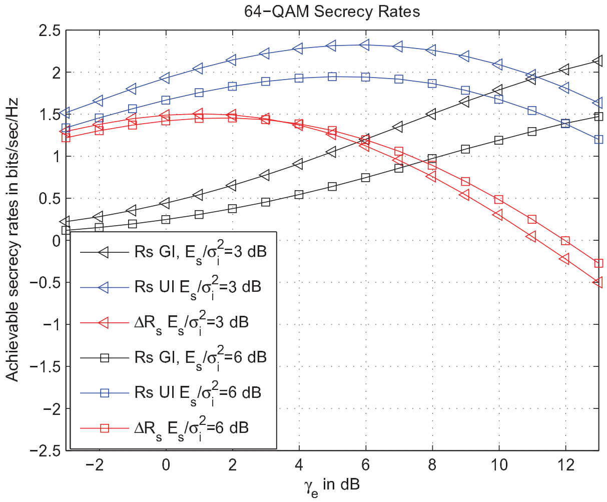

Fig. 8. Achievable secrecy rates R_s for a 64-QAM system.

the potential eavesdropper. Furthermore, we have evaluated the gain in secrecy rates based on the gap and union bound approximations. Future work will quantify the corresponding reduction in the mutual information of the strategies examined making use of the Hirschman entropy.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1385–1357, Oct. 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Information Theory*, vol. 54, no. 10, pp. 4687–5403, Oct. 2008.

[4] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple antenna wiretap channel," *IEEE Trans. Information Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[5] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The Gaussian wiretap channel with a helping interferer," in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, Jul. 2008, pp. 389–393.

[6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[7] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. New York: Springer, 2010.

[8] N. Marina, H. Yagi, and H. V. Poor, "Improved rate-equivocation regions for secure cooperative communication," in *Information Theory Proceedings (ISIT)*, St Petersbourg, Russia, Jul. 2011, pp. 2871 – 2875.

[9] G. D. Forney and M. V. Eyuboglu, "Combined equalization and coding using precoding," *IEEE Communications Magazine*, vol. 29, no. 12, pp. 25 – 34, Dec. 1991.

[10] A. M. Tulino and S. Verdú, *Random Matrix Theory and Wireless Communications*. Hanover MA: Now Publishers Inc., 2004.

[11] M. A. Haleem, C. N. Mathur, R. Chandramouli, and K. P. Subbalakshmi, "Opportunistic encryption: A trade-off between security and throughput in wireless networks," *IEEE Trans. on Dependable and Secure Computing*, vol. 4, no. 4, pp. 313 – 324, 2007.

[12] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *arXiv:1007.3568v1*, vol. cs.IT, pp. 1–14, Jul. 2010.

[13] J. G. Proakis, *Digital Communications*, 4th ed. New York: McGraw Hill, 2001.

[14] J. M. Cioffi, G. P. Dudevoir, M. V. Eyuboglu, and G. D. Forney, "MMSE decision-feedback equalizers and coding: II coding results," *IEEE Trans. Communications*, vol. 43, no. 10, pp. 2595–2604, Oct. 1995.

[15] A. Garcia-Armada, "SNR gap approximation for M-PSK-based bit loading," *IEEE Trans. Wireless Communications*, vol. 5, no. 1, pp. 57–60, Jan. 2006.