Helping Interferer Physical Layer Security Strategies for M-QAM and M-PSK Systems

Arsenia Chorti[†,*] *Member, IEEE*
[†]Department of Electrical Engineering, Princeton University, Princeton, New Jersey 08544, USA
[*] 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@princeton.edu

***Abstract*—Physical layer security encompasses information theoretic approaches that could guarantee perfect secrecy in wireless communication systems. In this framework, helping interferer strategies rely on intentionally creating confusion at a potential eavesdropper by injecting a jamming signal. In cases where the information signal has a Gaussian probability density function (pdf) it has been demonstrated that the optimal jamming signal, under an overall power constraint, should also be Gaussian. However, in practical communication systems where data symbols are typically drawn from discrete uniform probability mass functions (pmf), commonly M-ary Quadrature Amplitude and M-ary Phase Shift Keying modulation schemes, the structure of the optimal jamming signal is still an open question. In the present work we aim at shedding light into this question. Our approach is based on formulating a secrecy capacity maximization problem by expressing the optimal arbitrary helping interferer pdf as a mixture of unknown Gaussians. The proposed approximation is well-suited for jamming signals of practical interest, i.e. Gaussian or M-QAM interferers and reveals that in certain scenarios it is advantageous to use jamming signals whose statistical structure resembles the data rather than the noise.**

I. Introduction

Security in the exchange of information has commonly been treated as an inherently applied subject, despite the theoretical formulation of perfect secrecy early on [1]. Notwithstanding decades of research, the gap between applied cryptography and information theoretic security has not yet been bridged. Shannon described encryption as a set of reversible transformations, such that the mutual information between the message and the enciphered text should be null. However, despite its conceptual beauty, the concept of perfect secrecy was abandoned as it proved difficult to develop practical codes along this line. On the contrary, cryptography mainly evolved as a part of computer science and relied on complexity, rather than information and communication theory. Commonly, such encryption protocols underpin the security of mobile telecommunications as well as e-business, e-commerce, e-government, banking networks, and are employed at upper layers of the network protocol stack.

Nevertheless, the aforementioned approaches share a common weakness; they assume ideal transmission and reception and do not account for the adverse characteristics of the communication medium. Specifically for wireless applications, there exists an experimentally established fundamental trade-off between security and throughput [2], [3]. In order to address this important issue in future wireless applications, information theoretic physical layer approaches on security have been gaining renewed interest. The breakthrough concept of physical layer security [4] is to exploit the characteristics of the wireless medium such as fading or noise to achieve secrecy in wireless transmissions.

The pioneering works of Wyner [4] and Csiszár and Körner [5] 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. Ensuring secrecy through equivocation, a single letter characterization of the secrecy capacity was obtained for Gaussian signals, as the difference between the capacities of the legitimate user and the eavesdropper [6]. Furthermore, analyses for the wireless fading channel [7] and Multiple-Input Multiple-Output (MIMO) systems [8] 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 *highly* 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 disadvantageous. In view of this, helping-interferer approaches [9], [10], [11] have been proposed, building on the idea of intentionally degrading the eavesdropper's channel. In this paper, we investigate the optimal design of the jamming signal in a helping interferer physical layer security approach.

In previous analyses, simplified secrecy capacity expressions were obtained assuming that the data have a Gaussian probability density function (pdf). On the contrary, in this investigation an analysis is presented for actual communication systems in which the data are drawn from multi-level/multiphase discrete uniform probability mass functions (pmf), typically M-ary Quadrature Amplitude Modulation (M-QAM) or M-ary Phase Shift Keying (M-PSK) constellations. Preliminary results presented in [12], suggested that in relation to the system Signal-to-Noise Ratio (SNR), using a Gaussian helping interferer might be a suboptimal choice for

This work was funded by the IOF "APLOE" (PIOF-GA-2010-274723) grant within the 7th Framework Program of the European Community.

978-1-4673-3140-1/12/$31.00 ©2012 IEEE

M-QAM and M-PSK systems. Motivated by these findings, in the present work a closed-form expression is derived for the secrecy capacity of M-QAM and M-PSK systems in the presence of an arbitrary interferer whose pdf is approximated as a mixture of Gaussian components. An extensive set of simulation results is presented for the scenario of asymmetric jamming, i.e. the helping interferer is located at the proximity of the eavesdropper and does not affect on the other hand the reception of the legitimate user. In this scenario it is established that in a large range of SNRs and Signal-to-Interference Ratios (SIRs) it is advantageous to use a jamming signal that shares the statistical properties of the data rather than the noise.

This paper is organized as follows: in Section II the motivation behind this work is outlined, in Section III capacity expressions for M-QAM and M-PSK systems are reviewed and the respective secrecy capacities are evaluated. Furthermore, in Section IV the secrecy capacities are derived for the case of M-QAM and M-PSK systems in the presence of arbitrary jamming signals. Finally, simulation results for the case of asymmetric jamming are presented in Section V, while Section VI concludes the present work.

II. Motivation: Case Study of BPSK Systems

To illustrate the motivation behind this work, we begin by assuming a communication system in which length N observation vectors $\mathbf{z}_r$ are obtained at the outputs of matched filters at the legitimate ($r = l$) and eavesdropping receivers ($r = e$):

$$\mathbf{z}_r = \mathbf{H}_r \mathbf{d} + \mathbf{n}_r. \tag{1}$$

To allow for a compact notation, the generic index $r \in \{l, e\}$ corresponds to the legitimate receiver for $r = l$ and to the eavesdropper for $r = e$. The $N \times N$ matrices $\mathbf{H}_r$ denote the respective legitimate user's and eavesdropper's transformation matrices (typically channel or coding matrices) while $\mathbf{d} = [d_i], i = 1, \ldots, N$ is a sequence of independent and identically distributed (i.i.d.) data symbols. Finally, $\mathbf{n}_r = [n_{i,r}]^T, i = 1, \ldots, N$ are length N noise vectors of i.i.d. Gaussian random variables with variances $\sigma^2_{n,r} = \frac{N_{0,r}}{2}$.

Based on the findings in [13] and [14], the normalized, to the noise standard deviation, signal space minimum distances $\mathrm{d}_{\min r}, r \in \{l, e\}$ at the legitimate user and the eavesdropper respectively can be upper bounded by the Minkowski bound as:

$$\mathrm{d}_{\min l} \leq \sqrt{N} \det(\gamma_l \mathbf{H}_l \mathbf{H}_l^H)^{1/N} = \sqrt{N} \prod_{i=1}^{N} (\gamma_l \lambda_i)^{1/N} \tag{2}$$

$$\mathrm{d}_{\min e} \leq \sqrt{N} \det(\gamma_e \mathbf{H}_e \mathbf{H}_e^H)^{1/N} = \sqrt{N} \prod_{i=1}^{N} (\gamma_e \xi_i)^{1/N} \tag{3}$$

In (2) and (3), λ_i and ξ_i denote the eigenvalues of the legitimate user and the eavesdropper Gram matrices $\mathbf{H}_l \mathbf{H}_l^H$ and $\mathbf{H}_e \mathbf{H}_e^H$ respectively, while γ_l and γ_e denote the SNR of the forward and eavesdropper's channels, respectively. The above bounds infer that for typical digital communication systems, potential advantages - in terms of error rates - established at the legitimate user in respect to an eavesdropper are independent of the receivers' complexities.

Correspondingly, from a capacity point of view, for Gaussian data symbols $\mathbf{d}$ the secrecy capacity is simply evaluated as the difference between the capacities of the legitimate and eavesdropping channels, i.e [15]:

$$\begin{aligned} C_s &= (C_l - C_e)^+ \\ &= \left(\log\det(\mathbf{I}_N + \gamma_l \mathbf{H}_l \mathbf{H}_l^H) - \log\det(\mathbf{I}_N + \gamma_e \mathbf{H}_e \mathbf{H}_e^H) \right)^+ \\ &= \sum_{i=1}^{N} \left(\log \frac{1 + \gamma_l \lambda_i}{1 + \gamma_e \xi_i} \right)^+, \end{aligned} \tag{4}$$

with $(x)^+ = \max(x, 0)$ and $\mathbf{I}_N$ denoting the $N \times N$ identity matrix. 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 $\log \frac{1+\gamma_l \lambda_i}{1+\gamma_e \xi_i}$, with $\left(\frac{\gamma_l \lambda_i}{\gamma_l \xi_i}\right)^{1/N}$ being the corresponding ratios of the signal spaces minimum distances in the respective dimensions.

The idea behind injecting noise-like Gaussian jamming signals in helping interferer strategies is to "tune" in a controlled manner the value of γ_l and γ_e. The underlying strategy is to degrade γ_e to a *greater* extent than γ_l. From the eavesdropper's point of view, any such noise-like jammer is equivalent to having a Gaussian random secret key superimposed on the transmitted data.

A simple example that illustrates the limitations of this approach in M-QAM and M-PSK systems is presented in [12]. Through a counterexample we show that Gaussian jamming is a sub-optimal strategy in M-QAM and M-PSK systems: Let us assume a Binary PSK (BPSK) broadcasting system in which a friendly jammer injects a signal $i(t)$ that affects the eavesdropper alone (e.g. the jammer is located close to the eavesdropper and sufficiently far from the legitimate user). In ideal Additive White Gaussian Noise (AWGN) channel conditions the legitimate user's and the eavesdropper's observations, reduced to scalars in the following for simplicity, are in this case expressed as:

$$z_l = d + \kappa_l i + \sigma_{n,l} n_l, \tag{5}$$

$$z_e = d + \kappa_e i + \sigma_{n,e} n_e, \tag{6}$$

where i denotes the projection of the helping interferer $i(t)$ on the signal space, $\kappa_l = 0$ and without loss of generality we have assumed that all variables involved are normalized to the data standard deviation, so that i has unit variance.

In a hypothetical noiseless scenario with $\kappa_e = 1$ and $\sigma^2_{n,e} = 0$, we examine the following two distinct approaches: (i) The jamming signal has a Gaussian pdf; in this approach the Bit-Error-Rate (BER) is evaluated at 0.1624. (ii) The jamming signal is a BPSK signal, with similar statistical properties to that of the *data* instead of the *noise*. In this approach, the eavesdropper is able to identify the transmitted symbol with certainty only in 50% of the cases, as illustrated in Table I, leading to BER of 0.25. This increase in the BER corresponds to a decrease in the signal space minimum distance as shown in [12], expressed as:

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

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

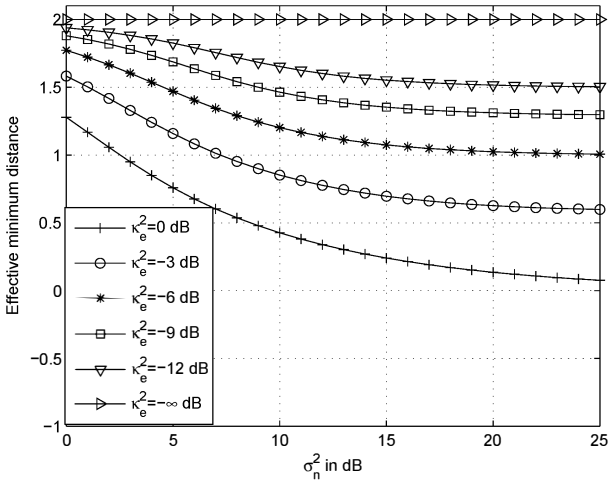

Fig. 1. Effective minimum distance in a BPSK constellation when using a BPSK jammer of normalized power κ_e^2.

with $P_{b,UI}$ denoting the probability of bit error at the eavesdropper when a BPSK jammer is employed, i.e. [14]

$$\begin{aligned} P_{b,UI} &= Pr(\hat{d} \neq d) \\ &= \frac{1}{4}\left[\mathrm{erfc}\left(\frac{\mathrm{d_{min}}/2-\kappa_e}{\sqrt{2}\sigma_{n,e}}\right)+\mathrm{erfc}\left(\frac{\mathrm{d_{min}}/2+\kappa_e}{\sqrt{2}\sigma_{n,e}}\right)\right]. \end{aligned} \tag{8}$$

The nominal minimum distance is $\mathrm{d_{min}} = 2$. There is a substantial decrease in the lattice effective minimum distance as depicted in Fig. 1. In effect, instead of increasing the denominator of the arguments of the complementary error functions, we are decreasing the numerators, in a sense decreasing the eavesdropper Gram matrices eigenvalues in (4).

III. SECRECY CAPACITY OF M-QAM AND M-PSK SYSTEMS

We revisit the model described in (5) and (6) in absence of a jamming signal, i.e. $\kappa_r = 0, r \in \{l, e\}$. Furthermore, the data symbol d is drawn from a discrete uniform pmf of M-QAM or M-PSK constellations from the set $\mathfrak{D} = \{d^1, \ldots, d^M\}$. The system capacity $C_r(M)$ at the legitimate user ($r = l$) and the eavesdropper ($r = e$) can then be expressed as a function of the constellation size M as

$$\begin{aligned} C_r(M) &= \mathbb{E}_D\{D_{KL}(p_{Z_r|D}(z_r|d)\|p_{Z_r}(z_r))\} \\ &= -\frac{1}{M}\sum_{k=1}^{M}\int_{-\infty}^{\infty}\frac{1}{2\pi\sigma_{n,r}^2}e^{-\frac{|z_r|^2}{2\pi\sigma_{n,r}^2}} \\ &\times \log\left(\frac{1}{M}\sum_{m=1}^{M}e^{-\frac{|z_r|^2-|z_r+\Delta_r^{km}|^2}{2\sigma_{n,r}^2}}\right)dz_r, \end{aligned} \tag{9}$$

where $D_{KL}(\cdot,\cdot)$ denotes the Kullback−Leibler divergence and

$$\Delta_r^{km} = \frac{d^k - d^m}{\sqrt{2}\sigma_{n,r}} \tag{10}$$

is the normalized to the noise standard deviation distance between any two constellation points [16], [17].

A useful closed-form approximation of (9) was proposed in [17] so that in AWGN channel we have that

$$\begin{aligned} C_r(M) &\simeq -\frac{1}{M}\sum_{k=1}^{M}\log\left(\frac{1}{M}\sum_{m=1}^{M}e^{-|\Delta_r^{km}|^2}\right) \\ &- \frac{1}{M}\sum_{k=1}^{M}\sum_{m=1}^{M}\frac{e^{-|\Delta_r^{km}|^2\frac{1-\nu_r}{2-\nu_r}}-e^{-|\Delta_r^{km}|^2}}{\sum_{l=1}^{M}e^{-|\Delta_r^{kl}|^2(1-\nu_r)}}, \end{aligned} \tag{11}$$

where in (11) we denote

$$\nu_r = \frac{\gamma_r}{2(1+\gamma_r)}, r \in \{l, e\} \tag{12}$$

while γ_r denotes the SNR at the legitimate receiver ($r = l$) and the eavesdropper ($r = e$), respectively.

Measuring secrecy through the equivocation R_e, the secrecy capacity of M-QAM and M-PSK systems in AWGN is therefore expressed as:

$$\begin{aligned} C_s(M) = R_e &= (\mathcal{I}(Z_l;D) - \mathcal{I}(Z_e;D))^+ \\ &= (C_l(M) - C_e(M))^+ \end{aligned} \tag{13}$$

with C_l and C_e given in (11).

IV. SECRECY CAPACITY OF M-QAM AND M-PSK SYSTEMS WITH A HELPING INTERFERER

Now we revisit the model described in (5) and (6) in the presence of a jamming signal with an unknown pdf $p_I(i)$. Due to the independence of the random variables involved, the capacity of the legitimate receiver and the eavesdropper respectively can in this case be expressed as

$$\begin{aligned} C_r &= \mathbb{E}_D\{D_{KL}(p_{Z_r|D}(z_r|d)\|p_{Z_r}(z_r))\} \\ &= \mathbb{E}_D\Big\{D_{KL}\Big(p_I(i)\otimes p_{N_r|D}(n_r|d)\| \\ &\quad \sum_{k=1}^{M}\frac{1}{M}p_I(i)\otimes p_{N_r|D}(n_r|d^k)\Big)\Big\}, \end{aligned} \tag{14}$$

where $\otimes$ denotes convolution.

In order to simplify calculations, in the following we assume that $p_I(i)$ can be approximated by a mixture of L complex (two-dimensional) Gaussians centered on μ_λ and with variances σ_λ^2, $\lambda = 1, \ldots, L$, i.e,

$$p_I(i) \simeq \sum_{\lambda=1}^{L}\frac{1}{L2\pi\sigma_\lambda^2}e^{-\frac{|i-\mu_\lambda|^2}{2\sigma_\lambda^2}}. \tag{15}$$

Justification of the above choice is twofold. Firstly, evaluations of the convolutions in (14) can be simplified and secondly, the approximation in (15) becomes equality for a list of practically

important functions $p_I(i)$ including the case of Gaussian pdf and discrete multilevel/multiphase pmf interferers. In particular, based on a weak convergence argument [18], a discrete uniform M-QAM or M-PSK pmf with alphabet $\mathfrak{D}$ may be approximated as:

$$\begin{aligned} p_I(i) &= \sum_{m=1}^{M} \frac{1}{M}\delta(i-d^m) \\ &\simeq \lim_{\alpha\to 0}\sum_{m=1}^{M}\frac{1}{M}\delta_\alpha(i-d^m) \end{aligned} \tag{16}$$

with

$$\delta_\alpha(x) = \frac{1}{2\pi\alpha^2}e^{-\frac{x^2}{2\alpha^2}} \tag{17}$$

and $\delta(x)$ denoting the delta function.

Using the model in (15), the pdfs of the random variables $w_r = \kappa_r i + \sigma_{n,r} n_r$ are simply

$$p_{W_r}(w_r) = \sum_{\lambda=1}^{L}\frac{1}{L2\pi\rho_{\lambda,r}^2}e^{-\frac{|w_r-\mu_\lambda|^2}{2\rho_{\lambda,r}^2}}, \tag{18}$$

where $\rho_{\lambda,r}^2 = \sigma_\lambda^2 + \sigma_{n,r}^2$. The capacity C_r^* of the legitimate receiver and the eavesdropper in AWGN in the presence of an arbitrary interferer $i(t)$ can then be respectively expressed as

$$\begin{aligned} C_r^*(M,p_I(i)) &= -\frac{1}{M}\sum_{k=1}^{M}\sum_{\lambda=1}^{L}\int_{-\infty}^{\infty}\frac{1}{L2\pi\rho_{\lambda,r}^2}e^{-\frac{|z_r|^2}{2\pi\rho_{\lambda,r}^2}} \\ &\times \log\frac{1}{M}\sum_{m=1}^{M}\sum_{l=1}^{L}e^{-\frac{|z_r|^2-|z_r+(\zeta_r^{k\lambda}-\zeta_r^{ml})|^2}{2\rho_{\lambda,r}^2}}dz_r \end{aligned} \tag{19}$$

where

$$\zeta_r^{xy} = \frac{d^x-\mu_y}{\sqrt{2}\rho_{\lambda,r}} \tag{20}$$

are the normalized to the combined standard deviation distances between the constellation points and the mean values of the Gaussian components.

After some algebraic manipulations, we conclude that

$$C_r^*(M,p_I(i)) = \frac{C_r(M\cdot L) - \log M + \log L}{2}. \tag{21}$$

Denoting the set $\mathcal{Q}$ as the product of the sets $\mathcal{M} = \{1,\dots,M\}$ and $\mathcal{L} = \{1,\dots,L\}$ and setting

$$Q = |\mathcal{Q}|, \tag{22}$$

$$\tau_r^{\xi\beta} = \zeta_r^{k\lambda} - \zeta_r^{ml}, \xi,\beta\in\mathcal{Q}, k,m\in\mathcal{M}, \lambda,l\in\mathcal{L} \tag{23}$$

we may approximate the capacity in the main and eavesdropper's channels by

$$\begin{aligned} C_r^* &= -\frac{1}{Q}\sum_{\xi\in\mathcal{Q}}\int_{-\infty}^{\infty}\frac{1}{2\pi\rho_{\lambda_r}^2}e^{-\frac{|z_r|^2}{2\rho_{\lambda,r}^2}} \\ &\times \log\left(\frac{1}{Q}\sum_{\beta\in\mathcal{Q}}e^{-\frac{|z_r|^2-|z_r+\tau_r^{\xi\beta}|^2}{2\rho_{\lambda,r}^2}}\right) \\ &- \frac{\log M-\log L}{2} \end{aligned} \tag{24}$$

$$\begin{aligned} &\simeq -\frac{1}{Q}\sum_{\xi\in\mathcal{Q}}\log\left(\frac{1}{Q}\sum_{\beta\in\mathcal{Q}}e^{-|\tau_r^{\xi\beta}|^2}\right) \\ &- \frac{1}{Q}\sum_{\xi\in\mathcal{Q}}\sum_{\beta\in\mathcal{Q}}\frac{e^{-|\tau_r^{\xi\beta}|^2\frac{1-\nu_r}{2-\nu_r}} - e^{-|\tau_r^{\xi\beta}|^2}}{\sum_{n\in\mathcal{Q}}e^{-|\tau_r^{\xi n}|^2(1-\nu_r)}} \\ &- \frac{\log M-\log L}{2}. \end{aligned} \tag{25}$$

An approximation for the secrecy capacity can be obtained by noticing that the second sum in (25) is negligible compared to the first sum, so that

$$C_s \simeq \left(-\frac{1}{Q}\sum_{\xi\in\mathcal{Q}}\log\left(\frac{\sum_{\beta\in\mathcal{Q}}e^{-|\tau_l^{\xi\beta}|^2}}{\sum_{\beta\in\mathcal{Q}}e^{-|\tau_e^{\xi\beta}|^2}}\right)\right)^+. \tag{26}$$

The optimal jamming signal maximizes (26) subject to an overall power constraint at the legitimate receiver,

$$\sigma_d^2 + \kappa_l^2 \le P. \tag{27}$$

The maximization of (26) s.t. (27) is an integer mutlivariate and multiparametric optimization problem. In the following we present simulation results in asymmetric interferer scenarios, evaluating the respective secrecy capacities in the case of Gaussian and M-QAM jamming signals.

V. Asymmetric Interferer, Non-degraded Eavesdropper Channel

In this scenario the injection of the noise is performed by a helping node in the vicinity of the eavesdropper, located sufficiently far from the legitimate receiver so that

$$\kappa_l \simeq 0. \tag{28}$$

Furthermore, we assume that the legitimate user and the eavesdropper experience similar degradation due to white noise, i.e.

$$\sigma_{n,l} = \sigma_{n,e} = \sigma_n, \tag{29}$$

so that the SNR in the main and the eavesdropper's channel is equal to γ_0. We will examine two distinct strategies. According to the first strategy, the interferer is a zero-mean Gaussian signal while according to the second it is a discrete multilevel/multiphase signal (M-QAM or M-PSK), mimicking the statistical properties of the data.

In the Gaussian interferer strategy, denoted as the GI approach in the following, we have

$$L = 1, \mu_1 = 0, \sigma_1 = \kappa_e. \tag{30}$$

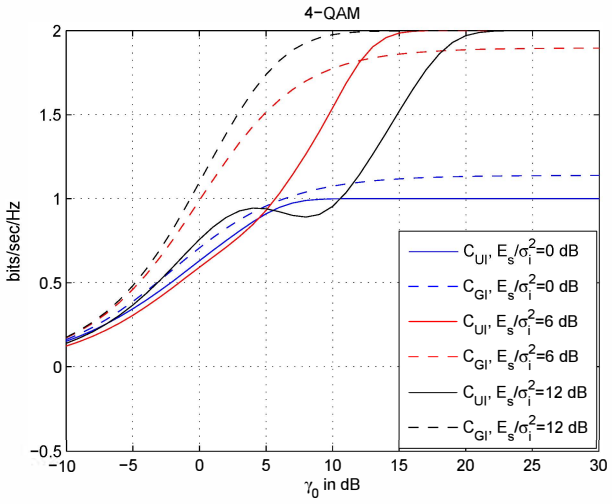

Fig. 2. Capacity of 4-QAM systems in the presence of a jamming signal.

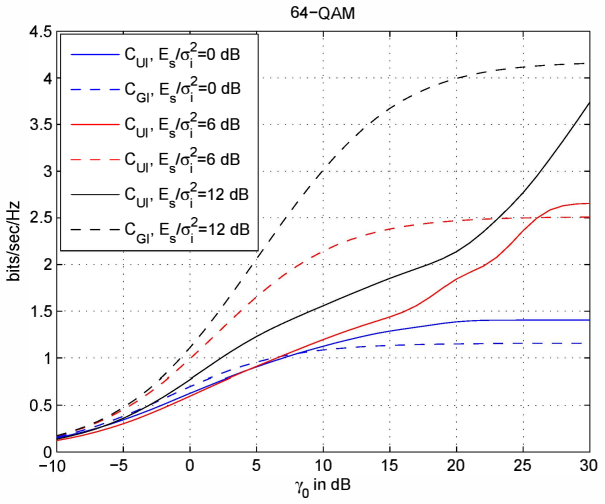

Fig. 4. Capacity of 64-QAM systems in the presence of a jamming signal.

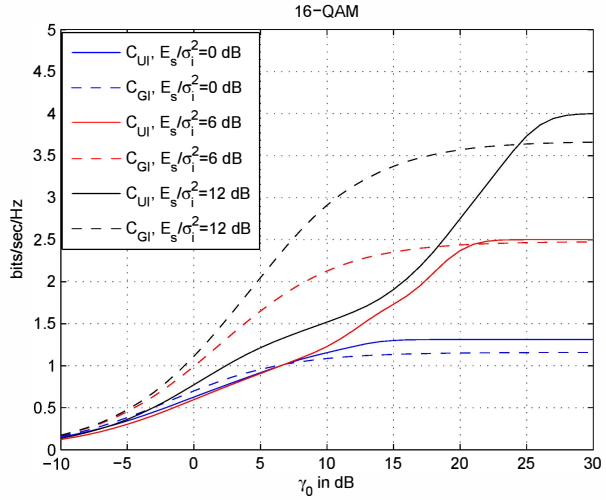

Fig. 3. Capacity of 16-QAM systems in the presence of a jamming signal.

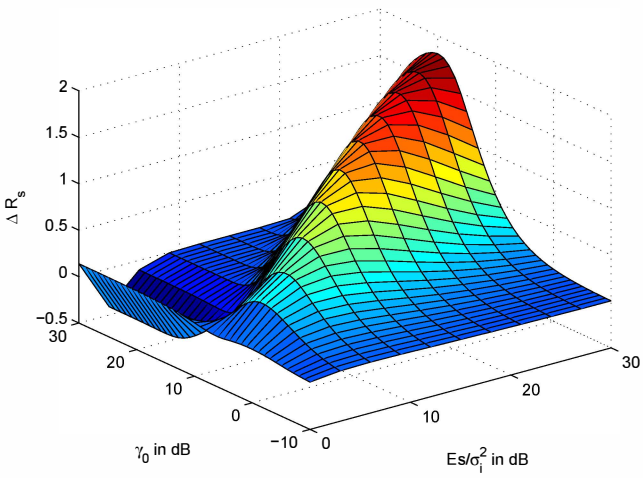

Fig. 5. Difference in secrecy rates for 4-QAM systems.

The second strategy, denoted as Uniform Interferer (UI) approach in the following, is summarized as

$$L = M,\ \mu_\lambda = \kappa_e d,\ \sigma_\lambda = 0,\ \lambda = 1, \ldots, L. \quad (31)$$

The capacities C_{GI} and C_{UI} in the GI and UI strategies respectively are evaluated in Figs 2, 3 and 4 for 4-QAM, 16-QAM and 64-QAM systems. The achievable rates in the GI and UI strategies follow distinctly different trends. Increasing the SNR increases the achievable rate in the case of the GI strategy. On the other hand, the effect is more complex in the UI strategy and further depends on the SIR.

Based on the above results, we expect that depending on the SNR and the SIR either the GI or the UI approach may be advantageous in terms of achievable secrecy rates. The difference in secrecy rates can be quantified in bits/symbol/Hz as

$$\Delta R_s = R_{s,UI} - R_{s,GI}. \quad (32)$$

In Figs 5, 6 and 7 ΔR_s is depicted for 4-QAM, 16-QAM and 64-QAM systems. In the high SNR and high SIR region an advantage of more than $\log_2 M - 1$ bits/symbol/Hz in the achievable secrecy rate can be established when the UI strategy is used.

VI. Conclusions

Unlike previous helping interferer approaches in the framework of physical layer security, the present work does not assume Gaussianity of the interferer as the optimal jamming strategy. On the contrary, we have shown through a counterexample that for practical communication systems that employ M-QAM or M-PSK modulations this is a sub-optimal choice. We have derived a closed-form approximate expression for the secrecy capacity in such systems by approximating an arbitrary helping interferer pdf as a mixture of Gaussian components. Through simulation, we have demonstrated that in the high SNR and high SIR region there is a clear gain in terms of secrecy rates in asymmetric helping interferer scenarios when the jamming signal shares the statistical properties of the data rather than the noise. Future work will quantify

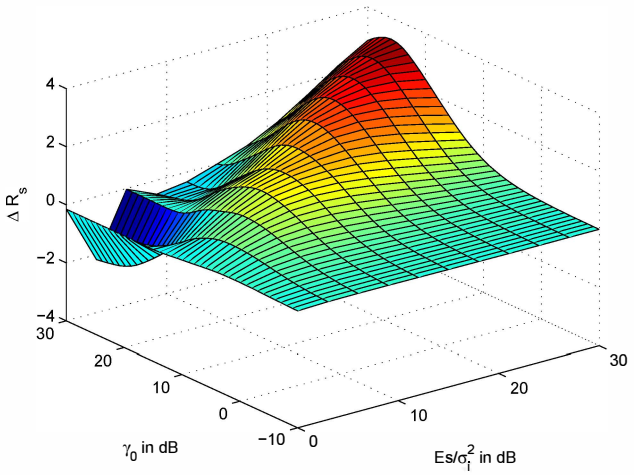

Fig. 6. Difference in secrecy rates for 16-QAM systems.

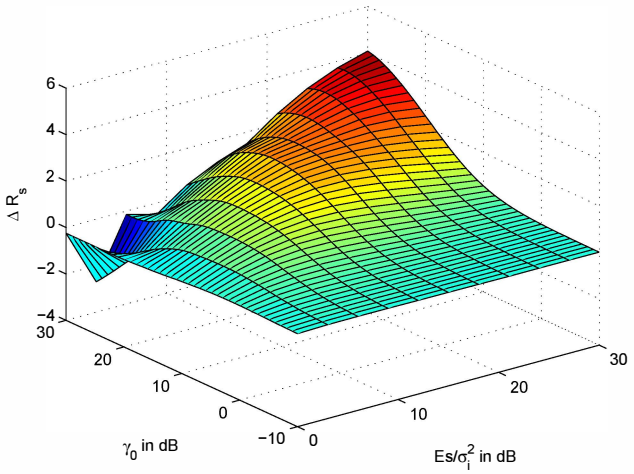

Fig. 7. Difference in secrecy rates for 64-QAM systems.

the corresponding reduction in the mutual information of the strategies examined making use of the Hirschman entropy.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," Bell Labs, Confidential report, 1946.

[2] E. Barka and M. Boulmalf, "Impact of encryption on the throughput of infrastructure WLAN IEEE 802.11g," in *Proc. IEEE Wireless Communications and Networking Conference*, Hong Kong, 11-15 Mar. 2007, pp. 2691 – 2697.

[3] S. Siwamogsatham, K. Hiranpruek, C. Luangingkasut, and S. Srilasak, "Revisiting the impact of encryption on performance of the IEEE 802.11 WLAN," in *Proc. Int. Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*, Krabi, Thailand, 14-17 May 2008, pp. 381 – 384.

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

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

[6] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[7] 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.

[8] 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.

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

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

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

[12] A. Chorti and H. V. Poor, "Achievable secrecy rates in physical layer secure systems with a helping interferer," in *IEEE Int. Conference on Computing, Networking and Communications*, Maui, HI, 30 Jan. - 2 Feb. 2012.

[13] V. Lyubashevsky and D. Micciancio, "On bounded distance decoding, unique shortest vectors, and the minimum distance problem," in *Proc. Advances in cryptology - Crypto 2009*. Santa Barbara, CA: Springer, Aug. 2009, pp. 577–594.

[14] A. Chorti and H. V. Poor, "Faster than Nyquist interference assisted secret communication for OFDM systems," in *in Proc. IEEE Asilomar Conference*, Monterey, CA, 4-7 Nov. 2011.

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

[16] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. Information Theory*, vol. 28, no. 1, pp. 55–65, Jan. 1982.

[17] S. B. Slimane, "Approximation to the symmetric capacity of Raylleigh fading channels with multi-level signals," *IEEE Communications Letters*, vol. 10, no. 3, pp. 129–131, Mar. 2006.

[18] H. Brézis, *Functional Analysis, Sobolev Spaces and Partial Differential Equations*. New York; London: Springer, 2011.