Optimal Jamming Strategies in Digital Communications – Impact of Modulation

SaiDhiraj Amuru and R. Michael Buehrer
Bradley Department of Electrical and Computer Engineering
Virginia Tech, Blacksburg, VA USA
Email: {adhiraj, rbuehrer}@vt.edu

***Abstract*—Jamming attacks can significantly impact the performance of wireless communication systems, and can lead to significant overhead in terms of re-transmissions and increased power consumption. This paper considers the problem of optimal jamming over an additive white Gaussian noise channel. We derive the optimal jamming signal for various digital amplitude-phase modulated constellations. We show that it is not always optimal to match the jammer's signal to the victim signal in order to maximize the error probability at the victim receiver. Connections between the optimum jammer obtained in this analysis and the well-known pulsed jammer, popularly analyzed in the context of spread spectrum communication systems are illustrated. Further, we evaluate the value of the knowledge of the victim's modulation schemes by comparing the performance of the optimal jamming signals with conventional additive white Gaussian noise jamming. Numerical results are presented in order to validate the theoretical inferences presented.**

I. Introduction

Jamming has traditionally been studied in the context of spread spectrum communications [1]. Barrage noise jamming, partial-band/narrow-band jamming and pulsed jamming are the most common jamming techniques considered in wireless communication systems. Most of the earlier literature that considered physical layer jamming attacks assumed either tone jamming (a victim is attacked by sending either a single or multiple jamming tones) [2] or additive white Gaussian noise (AWGN) jamming (partial band or broadband jamming) [2], [3]. The convexity properties of error probability with respect to the AWGN jamming signal power against a binary-valued victim signal were considered in [4]. An information theoretic study of jamming was considered in [3], [5]. In [3], independent Gaussian input and noise (which is the jamming signal) signals were shown to be a saddle point solution for the mutual information game between the victim and the jammer. In [5], the capacity of a wireless channel was analyzed in the presence of correlated jamming. Although various aspects of AWGN jamming have been considered under different scenarios, the question of optimal jamming against digital amplitude-phase modulated constellations is not yet fully answered.

Deviating from AWGN or tone jamming, we ask in this paper "What is the optimum statistical distribution for power constrained jamming signals in order to maximize the error probability of digital amplitude-phase modulated constellations?" The motivation for this work comes from a similar question raised in the past -"What is the worst case power constrained noise distribution for binary-input channels?" [6]. In [6], the worst case performance, in terms of maximizing the error probability and/or minimizing the capacity, achieved by any noise distribution was investigated when binary data was transmitted. The results presented in this paper are different from the results discussed in [6] in terms of 1) the system model and 2) the obtained worst case jamming signal distribution. In [6], the worst case noise distribution was shown to be a shifted version of the input signal distribution by ignoring the presence of AWGN noise introduced by the wireless channel. These results do not hold true for the scenarios considered in this paper mainly because we also consider the effects of AWGN noise in our system model formulation.

It is assumed that the victim receiver is not operating in an anti-jamming mode, i.e., the decision regions for the victim receiver remain the same irrespective of the presence or absence of a jamming signal. For instance, the decision boundary for a symmetric binary signaling scheme (signal levels given by $\pm A$ where A is the amplitude of signaling) will be taken to be 0 (irrespective of the presence or absence of jamming). Such jamming scenarios can occur when the jammer intends to disrupt communication between the transmitter and the victim receiver while the receiver is unaware of the presence of a jammer. Improved jamming techniques, such as the ones proposed in this paper, help military and/or practical wireless communication systems jam their adversaries' received signal before they can interpret any sensitive information.

The jammer is aware of the modulation scheme of the communication signal and also the power levels of the communication and the jamming signals at the victim receiver (using power control information, location and/or path loss calculations). These assumptions enable to analyze the worst case jamming performance against standard modulation schemes. We first show that the optimal power-constrained jamming signal shares time only between two signal levels i.e., a binary distribution, along any signaling dimension (in-phase and quadrature). Further, it will be shown that the jammer assumes the statistical distribution of well-known modulation schemes under special conditions, and is not always matched to the victim signal. These results are then extended to the more practical non-coherent scenario where there is a phase mismatch between the jammers' signal and the victim signal.

The rest of this paper is organized as follows. The system model and the structure of the optimal jamming signal distribution that maximizes the error probability are introduced in Section II. The optimal jamming signal distribution when the victim and the jammers' signals are phase aligned is derived in Section III. In Section IV, the jammers' statistical distribution is derived for the case when there is a random unknown phase offset between the victim and the jamming signals. Finally conclusions are drawn in Section V.

II. System Model and Optimum Jamming Signal Distribution

We assume that the data conveyed in the legitimate communication signal is mapped onto a known digital amplitude-phase constellation. The low pass equivalent of the transmitted signal is represented as $s(t) = \sum_{m=-\infty}^{\infty} \sqrt{P_S} s_m g(t - mT)$, where P_S is the average received signal power, $g(t)$ is the real valued pulse shape and T is the symbol interval. The random variables s_m denote the modulated symbols, distributed as $f_S(s)$ and are assumed to be uniformly distributed among all possible constellation points. Without loss of generality, the average energy of $g(t)$ and modulated symbols $E(|s_m|^2)$ are normalized to unity.

It is assumed that the transmitted signal passes through an AWGN channel (received power is constant over the observation interval) while being attacked by a jamming signal represented as $j(t) = \sum_{m=-\infty}^{\infty} \sqrt{P_J} j_m g(t - mT)$, where P_J is the average jamming signal power as seen at the victim receiver and j_m denote the jamming signals that are distributed as $f_J(j)$ with $E(|j_m|^2) \leq 1$. Assuming a coherent receiver and perfect synchronization, the received signal after matched filtering and sampling at the symbol intervals is given by

$$y_k = y(t = kT) = \sqrt{P_S} s_k + \sqrt{P_J} j_k + n_k, \ k = 1, 2, .. \quad (1)$$

where n_k is the zero-mean additive white Gaussian noise whose pdf is denoted by $f_N(n)$ and variance by σ^2. Let $\text{SNR} = \frac{P_S}{\sigma^2}$ and $\text{JNR} = \frac{P_J}{\sigma^2}$.

A. Motivation

Consider a BPSK signaling scenario with $P_S = 1$, $P_J = 1$ and $\sigma^2 = 0$ (i.e. the channel does not add any noise). If the jammer were aware of the signals sent by the transmitter, then it could negate them by sending the opposite of the transmit signal, i.e., the jammer sends a -1 symbol to destroy a $+1$ symbol. However, this is not possible in real time as the jammer can not demodulate the transmit signal before transmission occurs. Hence, it sends a random BPSK signal to disrupt the communication. The receiver can decode the symbols correctly half of the time i.e., when it gets ± 2. For the other half of the time when it gets 0, it makes a random guess regarding the transmit signal with probability $\frac{1}{2}$ of being correct. Thus the overall error probability is $\frac{1}{4} = 0.25$. On the other hand, the error probability is 0.1587 if an AWGN signal ($\sigma^2 = 1$) is used as a jamming signal [1]. For this toy example, the BPSK modulated jammer increased the error probability by 57.5% compared to the AWGN jammer (under similar power constraints) which suggests that there are interesting avenues to pursue beyond AWGN jamming.

B. Optimum Jamming Signal Distribution

The average probability of error[1] at the victim receiver that uses a maximum likelihood (ML) detector is given by

$$p_e(j, P_S, P_J) = \\ 1 - \int_s \int_\Omega f_N\left(y - \sqrt{P_S} s - \sqrt{P_J} j\right) f_S(s) dy ds, \quad (2)$$

where y is the received signal, j is the jamming signal, and Ω indicates the ML decision region for s. For instance, when the signal levels are $\pm A$, $\Omega = \text{real}(y) < 0$ when $s = -A$ and $\Omega = \text{real}(y) > 0$ when $s = +A$.

The jammer intends to maximize this error probability by transmitting a sequence of symbols j_m which are to be chosen based on P_S and P_J. The optimization problem for such a jammer can be formulated as

$$\begin{aligned} &\max_{f_J} \int_j p_e(j, P_S, P_J) f_J(j) dj \text{ s.t. } E(|j|^2) \leq 1, \\ &\triangleq \max_{f_J} E\Big(p_e(j, P_S, P_J)\Big) \text{ s.t. } E(|j|^2) \leq 1. \end{aligned} \quad (3)$$

Let $\bar{y}_k = [\Re y_k, \Im y_k]^T$ where $\Re y_k$ indicates the real (in-phase) part of y_k and $\Im y_k$ indicates the imaginary (quadrature) part of y_k. Along similar lines we can define $\bar{s}_k, \bar{j}_k$ and $\bar{n}_k$ for all $k = 1, 2, \ldots, K$. Then (1) is rewritten as

$$\bar{y}_k = \sqrt{P_S} \bar{s}_k + \sqrt{P_J} \bar{j}_k + \bar{n}_k, \ k = 0, 1, \ldots, K. \quad (4)$$

Since $p_e(j, P_S, P_J)$ is a continuous function (since n_k is Gaussian, standard p_e expressions are defined in terms of the erfc function which is continuous) defined on the support of $\bar{j}$ (which is a compact subset of $\mathbb{R}^2$), using Carathéodory's theorem [7], [8], it can be shown that the optimal jamming signal (i.e., the solution for (3)) can be represented as a randomization between at most two vectors $\bar{j}^{(1)}$ and $\bar{j}^{(2)}$ (similar optimization problems were considered in [7], [8] and references therein). Thus the optimal jamming signal pdf is given by

$$\begin{aligned} &f_{\bar{J}}(\bar{j}) = \lambda \delta(\bar{j} - \bar{j}^{(1)}) + (1 - \lambda) \delta(\bar{j} - \bar{j}^{(2)}), \ \lambda \in [0, 1] \\ &\lambda |\bar{j}^{(1)}|^2 + (1 - \lambda) |\bar{j}^{(2)}|^2 \leq 1, \end{aligned} \quad (5)$$

where λ and $(1 - \lambda)$ are the probabilities with which the jammer sends $\bar{j}^{(1)}$ and $\bar{j}^{(2)}$ respectively and $\delta(\bar{j})$ is the Dirac-delta function. Thus, the problem of finding an optimum jamming signal distribution is now reduced to finding λ, $\bar{j}^{(1)}$ and $\bar{j}^{(2)}$ rather than a continuous distribution $f_J(\bar{j})$. We next derive the statistics of the optimal jamming signal against digital amplitude-phase modulated constellations.

III. Perfect Channel Knowledge

In this section, we analyze the statistics of the optimal jammer when it has perfect channel knowledge i.e., phase and time synchronous with the victim signal. In all the analysis that follows, it is assumed that the receiver is unaware of the

[1] With a slight abuse of notation, we use p_e to denote the probability of error. The variables that it depends on are shown within brackets. For example, $p_e(P_S)$ indicates that p_e is a function of the signal power P_S.

$$p_e(\lambda, |j^{(1)}|, |j^{(2)}|, \mathrm{SNR}, \mathrm{JNR}) \approx \left(1 - \frac{1}{\sqrt{M}}\right)\frac{1}{2}\Bigg\{\lambda\left[\mathsf{erfc}\left(\sqrt{\mathrm{SNR}}\frac{d_{\mathsf{min}}}{2} + \sqrt{\mathrm{JNR}}|j^{(1)}|\right) + \mathsf{erfc}\left(\sqrt{\mathrm{SNR}}\frac{d_{\mathsf{min}}}{2} - \sqrt{\mathrm{JNR}}|j^{(1)}|\right)\right] + (1-\lambda)\left[\mathsf{erfc}\left(\sqrt{\mathrm{SNR}}\frac{d_{\mathsf{min}}}{2} + \sqrt{\mathrm{JNR}}|j^{(2)}|\right) + \mathsf{erfc}\left(\sqrt{\mathrm{SNR}}\frac{d_{\mathsf{min}}}{2} - \sqrt{\mathrm{JNR}}|j^{(2)}|\right)\right]\Bigg\} \quad (7)$$

$$\sqrt{2\mathrm{SNR}d^2_{\min}\mathrm{JNR}}\,\mathsf{exp}\left(-\frac{\mathrm{SNR}d^2_{\min}}{2}\right) < \sqrt{1-\lambda_{opt}}\Bigg\{\mathsf{exp}\left(-\left(\sqrt{\mathrm{SNR}\frac{d^2_{\min}}{2}} - \sqrt{\frac{\mathrm{JNR}}{(1-\lambda_{opt})}}\right)^2\right) - \mathsf{exp}\left(-\left(\sqrt{\mathrm{SNR}\frac{d^2_{\min}}{2}} + \sqrt{\frac{\mathrm{JNR}}{(1-\lambda_{opt})}}\right)^2\right)\Bigg\}, \quad (8)$$

presence of the jammer and hence the decision regions for the data detection remain the same as if there were no jammer. We first derive the optimum jamming signal distribution against a M-QAM victim signal and later show that this can be simplified for specific modulation schemes.

Since the victim signal and the jammers' signal are coherent, 2-dimensional modulation schemes such as M-QAM can be analyzed by considering them as two independent $\sqrt{M}$-PAM signals along the in-phase and quadrature dimensions [9]. For the system model in (4), p_e of a M-QAM victim signal along any signaling dimension in an AWGN channel and with a jamming signal $\bar{j}$ is given by

$$p_e(j, \mathrm{SNR}, \mathrm{JNR}) \approx \left(1 - \frac{1}{\sqrt{M}}\right)\frac{1}{2}\times \left[\mathsf{erfc}\left(\sqrt{\mathrm{SNR}}\frac{d_{\mathsf{min}}}{2} + \sqrt{\mathrm{JNR}}j\right) + \mathsf{erfc}\left(\sqrt{\mathrm{SNR}}\frac{d_{\mathsf{min}}}{2} - \sqrt{\mathrm{JNR}}j\right)\right], \quad (6)$$

where $j = \Re\bar{j}$ or $\Im\bar{j}$, M is the order of the constellation and d_{min} is the minimum distance of the underlying modulation scheme [9]. It is easy to see that (6) is symmetric in $\pm j$ and hence $p_e(j, \mathrm{SNR}, \mathrm{JNR}) = p_e(|j|, \mathrm{SNR}, \mathrm{JNR})$. Further it is not hard to show that $p_e(|j|, \mathrm{SNR}, \mathrm{JNR})$ is a non-decreasing function of $|j|$ and hence p_e is maximized on the boundary defined by $E(|j|^2) = 1/2$ (it is $1/2$ because we consider only one signaling dimension). Using the fact that the optimum jamming signal distribution is given by (5) and that $p_e(j, \mathrm{SNR}, \mathrm{JNR}) = p_e(|j|, \mathrm{SNR}, \mathrm{JNR})$, the overall p_e along any signaling dimension is given by (7), where $j^{(i)} = \Re\bar{j}^{(i)}$ or $\Im\bar{j}^{(i)}$ for $i = 1, 2$.

We will now state 3 theorems that establish the optimal jamming signal distribution against M-QAM victim signals. Due to lack of space, we only sketch the proofs of these theorems.

Theorem 1: QPSK is the optimal jamming signal when the victim signal uses M-QAM and $\mathrm{SNR}\frac{d^2_{\min}}{2} << \mathrm{JNR}$.

Remark 1: The theoretical p_e when QPSK is used as a jamming signal is given by substituting $|j^{(1)}| = |j^{(2)}| = \frac{1}{\sqrt{2}}$ and $\lambda = \frac{1}{2}$ in (7)*. The slope of the error probability with respect to* SNR *i.e.,* $\frac{\partial p_e}{\partial \mathrm{SNR}}$ *within a proportionality constant when* $\mathrm{SNR}\frac{d^2_{\min}}{2} << \mathrm{JNR}$ *can be approximated as*

$$\text{AWGN}: \frac{-1}{\sqrt{\mathrm{SNR} \times \mathrm{JNR}}}; \text{QPSK}: \frac{-2}{\sqrt{\mathrm{SNR} \times \mathsf{exp}\left(\mathrm{JNR}\right)}}, \quad (9)$$

which shows that the error probability for a QPSK jammer decays more slowly with JNR *when compared to the AWGN jammer. Thus from a jammers' perspective it is advantageous to use QPSK when compared to traditional AWGN.*

Sketch of the proof: Since $E(|j|^2)=\frac{1}{2}$, we have $\lambda|j^{(1)}|^2 + (1-\lambda)|j^{(2)}|^2 = \frac{1}{2}$. Using this relationship, (7) can be written as a function of $|j^{(1)}|$ denoted by $p_e(\lambda, |j^{(1)}|, \mathrm{SNR}, \mathrm{JNR})$. $|j^{(1)}| = \{0, \frac{1}{\sqrt{2\lambda}}, \frac{1}{\sqrt{2}}\}$ are the solutions to $\frac{\partial p_e(\lambda, |j^{(1)}|, \mathrm{SNR}, \mathrm{JNR})}{\partial |j^{(1)}|}$=0. To prove the optimality of QPSK, we need to show that $p_e(\lambda, |j^{(1)}|, \mathrm{SNR}, \mathrm{JNR})$ is maximized at $|j^{(1)}|$=$\frac{1}{\sqrt{2}}$ (we will discuss the solutions $|j^{(1)}|$=0,$\frac{1}{\sqrt{2\lambda}}$ in Theorems 2 and 3). The second derivative of p_e with respect to $|j^{(1)}|$ i.e., $\frac{\partial^2 p_e(\lambda, |j^{(1)}|, \mathrm{SNR}, \mathrm{JNR})}{\partial |j^{(1)}|^2}|_{|j^{(1)}|=\frac{1}{\sqrt{2}}}$ has 4 terms each of which can be shown to be < 0 when $\mathrm{SNR}\frac{d^2_{\min}}{2} << \mathrm{JNR}$. Further, this holds true irrespective of the value of λ (it can be seen from (7) that p_e is the same irrespective of λ when $|j^{(1)}|$=$|j^{(2)}|$=$\frac{1}{\sqrt{2}}$). However, since the entropy of the binary jamming signal distribution is maximized when $\lambda = \frac{1}{2}$ [10], we define that the optimal jamming signal distribution is given by the parameters $\lambda = \frac{1}{2}$,$|j^{(1)}|$=$|j^{(2)}|$=$\frac{1}{\sqrt{2}}$, in other words, the optimal jamming signal is QPSK.

Theorem 2: $\{|j^{(1)}|, |j^{(2)}|\} = \left\{0, \frac{1}{\sqrt{2(1-\lambda_{opt})}}\right\}$ is the optimal jamming signal along any signaling dimension when $\frac{\partial p_e(\lambda, |j^{(1)}|, \mathrm{SNR}, \mathrm{JNR})}{\partial |j^{(1)}|}|_{|j^{(1)}|=0} = 0$ and $\frac{\partial^2 p_e(\lambda_{opt}, |j^{(1)}|, \mathrm{SNR}, \mathrm{JNR})}{\partial |j^{(1)}|^2}|_{|j^{(1)}|=0} < 0$ where λ_{opt} is given by $\frac{\partial p_e(\lambda, |j^{(1)}|, \mathrm{SNR}, \mathrm{JNR})}{\partial \lambda}|_{|j^{(1)}|=0} = 0$ and (8).

Sketch of the proof: As mentioned earlier, $|j^{(1)}|$=0 is a solution for $\frac{\partial p_e(\lambda, |j^{(1)}|, \mathrm{SNR}, \mathrm{JNR})}{\partial |j^{(1)}|} = 0$. When this is true, the optimal value of λ denoted by λ_{opt} is obtained by solving

$\frac{\partial p_e(\lambda,|j^{(1)}|,\mathrm{SNR},\mathrm{JNR})}{\partial\lambda}\big|_{|j^{(1)}|=0} = 0$. Further, it can be proved that $\frac{\partial^2 p_e(\lambda_{opt},|j^{(1)}|,\mathrm{SNR},\mathrm{JNR})}{\partial|j^{(1)}|^2}\big|_{|j^{(1)}|=0}$ will be < 0 only when λ_{opt} satisfies (8). By symmetry, $\left\{\frac{1}{\sqrt{2\lambda_{opt}}}, 0\right\}$ is also a solution. Such a solution is known as on-off keying since the jammer sends power on only one of the two possible values $j^{(1)}$ or $j^{(2)}$.

Remark 2: When on-off keying is optimal, it can be shown that p_e is equivalent to the probability of error achieved when the jammer uses QPSK signaling (i.e., $|j^{(1)}| = |j^{(2)}| = \frac{1}{\sqrt{2}}$) and either transmits with power $\frac{P_J}{\lambda_{opt}}$ or shuts off transmission, with probability λ_{opt} and $(1-\lambda_{opt})$ respectively. Such a jamming signal is equivalent to a pulsed jammer albeit modulated by a QPSK signal rather than AWGN [1], [2]. Exploiting this equivalence, we next explicitly characterize the range of SNR *and* JNR *where on-off keying/pulsed jamming is optimal.*

Theorem 3: For a given SNR and JNR, the optimum strategy for a QPSK modulated jammer is to share time between two different power levels (one of which is 0) when $\mathrm{JNR} \leq \hat{\mathrm{JNR}}$ and continuous jamming else where. $\hat{\mathrm{JNR}}$ is defined by a unique jamming signal power $\hat{P}_J$ such that the tangent to p_e at $\hat{\mathrm{JNR}}$ (for a given SNR) passes through the origin. Such a jamming signal is popularly known as the pulsed-jammer.

Sketch of the proof: When QPSK is used as the jamming signal i.e., $\lambda = \frac{1}{2}, |j^{(1)}| = |j^{(2)}| = \frac{1}{\sqrt{2}}$, it can be shown that for the p_e in (7), there exists a single inflection point JNR^* such that p_e is convex when $\mathrm{JNR} \leq \mathrm{JNR}^*$ and concave elsewhere. When p_e is convex, the error probability can be increased by time sharing between two different power levels (by Jensen's inequality) [10] under the constraint that the average power is still P_J. Specifically, there exists a $\hat{\mathrm{JNR}} \geq \mathrm{JNR}^*$ such that the tangent to p_e (for a given SNR) at $\hat{\mathrm{JNR}}$ passes through the origin [4, Lemma 2]. Then, the achievable p_e when $\mathrm{JNR} \leq \hat{\mathrm{JNR}}$ is given by

$$\lambda p_e\left(\frac{1}{2}, \frac{1}{\sqrt{2}}, \mathrm{SNR}, \frac{\mathrm{JNR}}{\lambda}\right) + (1-\lambda) p_e\left(\frac{1}{2}, \frac{1}{\sqrt{2}}, \mathrm{SNR}, 0\right), \quad (10)$$

where, the optimal value of λ can be found by using the first and second derivatives of (10). Since (10) is equivalent to the p_e shown in Theorem 2, it is not hard to see that the optimal value of λ is given by λ_{opt} (discussed in Theorem 2). When $\mathrm{JNR} \geq \hat{\mathrm{JNR}}$ i.e., the concave region, the achievable p_e is described by $p_e\left(\frac{1}{2}, \frac{1}{\sqrt{2}}, \mathrm{SNR}, \mathrm{JNR}\right)$ which is indicative of continuous jamming. This concludes the proof of the theorem.

Numerically solving the optimization problem (finding the optimal jamming signal) under an average power constraint is difficult for a general range of SNR and JNR. Similar optimization problems have been solved using global optimization techniques such as particle swarm optimization in [7]. In this paper, we use the optimization toolbox in Matlab.

Table I shows the optimal values of the three unknown parameters against a 16-QAM victim signal for a general case in which $\mathrm{SNR} \gtreqless \mathrm{JNR}$. Since the in-phase and quadrature dimensions are equivalent in such a coherent scenario, it is seen that the optimal jamming signal is the same along any signaling dimension as mentioned earlier.

TABLE I

OPTIMAL JAMMING SIGNAL DISTRIBUTION AGAINST A 16-QAM VICTIM SIGNAL, $\mathrm{JNR} = 10\ dB$.

SNR (dB)	λ_{opt}	$\Re\bar{j}^{(1)}$	$\Re\bar{j}^{(2)}$	$\Im\bar{j}^{(1)}$	$\Im\bar{j}^{(2)}$
-2	0.5	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$
4	0.5	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$
10	0.5	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$
16	0.5	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$
19	0.4633	$\pm$ 1.039	0	$\pm$ 1.039	0
22	0.2304	$\pm$1.473	0	$\pm$1.473	0
25	0.1193	$\pm$2.047	0	$\pm$2.047	0
28	0.0625	$\pm$2.828	0	$\pm$2.828	0

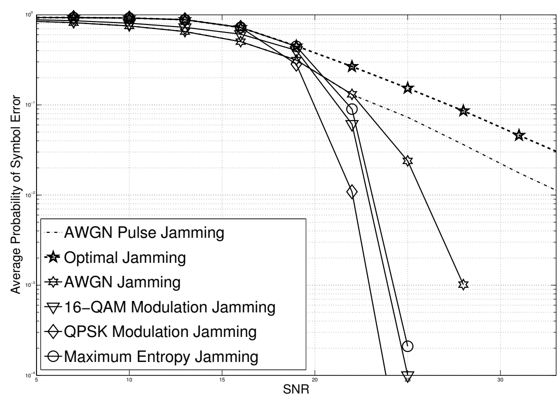

Fig. 1. Comparison of various jamming techniques against a 16-QAM modulated victim signal, $\mathrm{JNR} = 10\ dB$.

Remark 3: From Table I, it can be seen that QPSK is the optimal jamming signal only until a certain SNR *beyond which on-off keying (i.e., pulsed jammer with a QPSK distribution) is optimal. Further, the on-duration for the on-off keying scheme decreases as the* SNR *increases, which indicates that the jammer is turned on only for a short duration. However, it jams the receiver with increased signal levels in an attempt to compensate for the increased* SNR*. Notice that the on-off keying signal is not a shifted version of the input signal which is different from the results in [6] because of the effects of the additional AWGN noise introduced by the channel.*

The p_e for the 16-QAM victim signal under various jamming scenarios is shown in Fig. 1. Here 16-QAM (QPSK) jamming refers to a randomly generated 16-QAM (QPSK) modulated jamming signal, and AWGN jamming refers to a zero-mean white Gaussian noise jamming signal with variance P_J. The maximum entropy jammer maximizes the entropy of the jamming signal at the victim receiver i.e., an additional constraint $\lambda = 0.5$ [10] is imposed on the jamming signal distribution. While *maximum entropy jamming* is better than QPSK jamming, it is worse than the optimal jamming as the constraint $\lambda = 0.5$ does not allow the optimization algorithm

$$p_e(\lambda, \bar{j}, \mathrm{SNR}, \mathrm{JNR}) \approx \left(1 - \frac{1}{\sqrt{M}}\right)\frac{1}{2}\left[\mathsf{erfc}\left(\sqrt{\mathrm{SNR}}\frac{d_{\mathsf{min}}}{2} + \sqrt{\mathrm{JNR}}\mathsf{real}(\bar{j}\exp(i\phi))\right) + \mathsf{erfc}\left(\sqrt{\mathrm{SNR}}\frac{d_{\mathsf{min}}}{2} - \sqrt{\mathrm{JNR}}\mathsf{real}(\bar{j}\exp(i\phi))\right)\right] \quad (13)$$

to explore the on-off keying solution. For a fair comparison, the jamming performance of a pulsed jammer modulated with an AWGN signal [1] is also shown in Fig. 1.

AWGN-based pulsed jamming converts the exponential relationship between p_e and SNR to a linear one [1]. This also holds true for the case of the optimal jamming as seen in Fig. 1. This is similar to the behavior of p_e in a Rayleigh fading channel where it is inversely proportional to SNR. Intuitively, a symbol erased due to a deep fade is similar to the case where a symbol is disrupted by jamming. Thus the optimal jammer is capable of generating a fading channel-like scenario in an AWGN channel.

In summary, Theorem 1 shows that QPSK is the optimal jamming signal against a M-QAM victim signal when $\mathrm{SNR}\frac{d^2_{\min}}{2} << \mathrm{JNR}$. In Theorem 2, it is argued that on-off keying/pulsed jamming is an optimal strategy under certain conditions and finally Theorem 3 gives the SNR and JNR ranges where on-off keying is optimal. We used numerical optimization techniques to obtain a solution over all $\mathrm{SNR}, \mathrm{JNR}$, based on which it is conjectured that *pulsed QPSK* is an optimal signal to jam a M-QAM modulated victim signal.

TABLE II
OPTIMAL JAMMING SIGNALS IN A COHERENT SCENARIO.

Victim signal	Pulsed jamming signal
BPSK	BPSK
QPSK	QPSK
4-PAM	BPSK
16-QAM	QPSK

Remark 4: Since the two dimensional M-QAM constellations were analyzed by treating them as two orthogonal $\sqrt{M}$-PAM signals, the above analysis can be directly extended to one dimensional signaling constellations such as BPSK, 4*-PAM among others. Table II summarizes the optimal jamming signals against commonly used digital amplitude-phase modulated constellations. These results indicate that matching the jamming signal to the victim signal is not always optimal.*

IV. NON-COHERENT JAMMING

In this section, jamming behavior is studied when the jammers' signal is not coherent (i.e., phase asynchronous) with the victim signal. From a jammers' perspective, the non-idealities in the channel, specifically differences between the victim and jamming signals will lower the impact of jamming at the victim receiver. For example, consider a scenario where the victim and the jammer use BPSK modulation. If the channel introduces a 90° phase offset between these two signals, then the jammers' signal does not have any impact on the victim signal (as the receiver only demodulates the projections of the signal received along the in-phase dimension). If the phase shift is known ahead of time to the jammer, it can compensate for this in the jamming signal before it is sent. This is however difficult to achieve in a real time communication system. Hence, we consider a scenario where the jammer is unaware of (or unable to compensate for) this random phase offset introduced by the wireless channel and thus treats it as a random variable.

With a random phase offset, the victim signal is given by

$$\bar{y}_k = \sqrt{P_S}\bar{s}_k + \sqrt{P_J}\mathsf{exp}\,(i\phi)\,\bar{j}_k + \bar{n}_k,\ k = 0, 1, \ldots, K, \quad (11)$$

where ϕ indicates the phase offset between the victim signal and the jamming signal at the victim receiver and is treated as a uniform random variable between 0 and 2π, and $i = \sqrt{-1}$. As in Section III, the jammer maximizes p_e at the receiver and the optimization problem is given by

$$\max_{f_{\bar{J}}} E_{f_{\bar{J}}}\left[E_\phi\Big(p_e\left(\bar{j}, P_S, P_J\right)\Big)\right] \text{ s.t. } E(|\bar{j}|^2) \le 1. \quad (12)$$

Following the analysis in Section II, the optimal jamming signal distribution i.e., the solution to (12) is again described by (5).

Even in the non-coherent case, the M-QAM signal can be analyzed by considering it as two orthogonal $\sqrt{M}$-PAM signals. However, in this case due to the random phase offset between the jammers' signal and the victim signal, projections of the jammers' signal along each signaling dimension must be considered which is different from the analysis in Section III. The p_e of a M-QAM signal along the in-phase dimension when there is a jamming signal $\bar{j}$ and a random phase offset ϕ, is given by (13) (a similar expression holds true for the quadrature signaling dimension). In (13), $\mathsf{real}(\bar{j}\exp(i\phi)) = \Re\bar{j}\cos(\phi) - \Im\bar{j}\sin(\phi)$.

Using (13) and solving the optimization problem in (12) along with (5), gives the optimal jamming signal distribution shown in Table III when $M = 16$ i.e., against a 16-QAM victim signal. It is interesting to see that once again QPSK is the optimal jamming signal until a certain SNR. Beyond this limit, on-off keying is optimal. This behavior is similar to the observations in Section III. Since on-off keying is optimal, the non-zero signal level is given by its corresponding probability as $\frac{\pm 1}{\sqrt{2\lambda_{opt}}}$ or $\frac{\pm 1}{\sqrt{2(1-\lambda_{opt})}}$. Notice that the optimization solver returned equal values for the jamming signal levels along the in-phase and quadrature dimensions (in Table III). This is due to the symmetry present along these dimensions in the case of 2-dimensional signaling (in-phase and quadrature are equally important to evaluate p_e).

Similar to the coherent scenario (see Theorem 3), the

TABLE III
OPTIMAL NONCOHERENT JAMMING SIGNAL AGAINST A 16-QAM VICTIM SIGNAL, $\mathrm{JNR} = 10\ dB$.

SNR (dB)	λ_{opt}	$\Re\bar{j}^{(1)}$	$\Re\bar{j}^{(2)}$	$\Im\bar{j}^{(1)}$	$\Im\bar{j}^{(2)}$
-2	0.5	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$
4	0.5	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$
10	0.5	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$
16	0.5	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$
19	0.5	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}}$
22	0.185	±1.642	0	±1.642	0
25	0.094	±2.304	0	±2.304	0
28	0.049	±3.211	0	±3.211	0

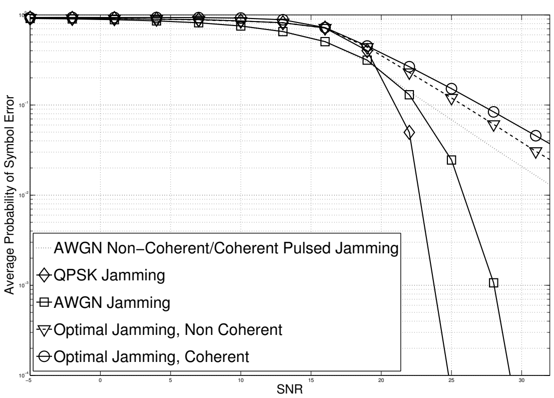

Fig. 2. Comparison of jamming techniques against a 16-QAM victim signal in a non-coherent (random phase offset) scenario, $\mathrm{JNR} = 10\ dB$.

equivalence between on-off keying and pulsed-QPSK holds true even in this case. The jammer uses pulsing/on-off keying when $\mathrm{JNR} \geq \hat{\mathrm{JNR}}$ where $\hat{\mathrm{JNR}}$ is defined in Section III. The performance of the various jamming signals against a 16-QAM victim signal is shown in Fig. 2. Although the p_e achieved by the optimal jamming signal (or pulsed-QPSK) is less compared to the coherent scenario (due to phase mismatch), it is still higher than the p_e achieved using pulsed-AWGN jamming.

Similar to the coherent scenario, the analysis for the M-QAM constellations can be extended to any specific modulation scheme in a non-coherent scenario. The optimal jamming signals in such a phase asynchronous scenario against the commonly used modulation schemes such as BPSK, 4-PAM, QPSK and 16-QAM are still given by Table II. However, the pulsed jamming duration (on-off keying duration) of these optimal jamming signals changes between the coherent and non-coherent (phase asynchronous) scenarios as seen from Tables I and III. Also, the gain in the SNR required to achieve a target p_e when compared to the coherent scenario, decreases by 1-2 dB due to this phase mismatch.

V. CONCLUSION

In this paper, we characterized the optimal statistical distribution for power constrained jamming signals that jam digital amplitude-phase modulated constellations in an AWGN channel. The analysis in this paper shows that modulation-based pulsed jamming signals are optimal in both coherent and non-coherent (phase asynchronous) scenarios. As opposed to the common belief that matching the victim signal (correlated jamming) increases confusion at the victim receiver, our analysis shows that the optimal jamming signals match standard modulation formats only in a certain range of signal and jamming powers. Beyond this range, on-off keying is an optimal statistical distribution for the jamming signals. An interesting relationship between these optimal jamming signals and the well-known pulse jamming signals discussed in the context of spread spectrum communications was illustrated. As expected, the performance of these optimal jamming signals was seen to be degraded when the victim and the jamming signals are not phase synchronous.

These modulation-based jamming techniques can be extended to any higher order modulation schemes by following the analysis shown in this paper. The structure of the optimal jamming signals also suggests that modulation classification techniques only need to identify the class of the modulation scheme such as PAM or QAM in order to devise an optimal jamming strategy. This significantly reduces the computational complexity involved in sophisticated modulation classification algorithms proposed in the literature. Investigating optimal jamming signals 1) in the presence of intelligent receivers, 2) in scenarios where the jammer is not aware of the power levels of the victim and the jamming signals at the victim receiver, and 3) when the jamming and the victim signals are not time aligned, or when there is a symbol rate/interval mismatch is part of our ongoing work. Further, examining optimal jamming signal distributions for fading channels, OFDM-based and MIMO-based wireless systems are interesting directions that arise from the analysis done in this work.

REFERENCES

[1] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, vol. 1. Rockville, MD: Comput. Sci. Press, 1985.

[2] R. A. Poisel, *Introduction to Communication Electronic Warfare Systems*. Artech House, 2008.

[3] R. McEliece and W. Stark, "An information theoretic study of communication in the presence of jamming", in *Proc. Int. Conf. Commun.*, 1981, pp. 45.3.1-45.3.5.

[4] M. Azizoglu, "Convexity properties in binary detection problems," *IEEE Trans. Inf. Theory*, vol. 42, pp. 1316-1321, Jul. 1996.

[5] M. Medard, "Capacity of correlated jamming channels," in *Proc. 35th Allerton Conf.,* Monticello, IL, Sep. 1997, pp. 1043-1052.

[6] S. Shamai (Shitz) and S. Verdú, "Worst-Case Power Constrained Noise for Binary-Input Channels," *IEEE Trans. Inf. Theory,* vol. IT-38, no. 5, pp. 1494-1511, Sep. 1992.

[7] C. Goken, S. Gezici, and O. Arikan, "Optimal stochastic signaling for power-constrained binary communications systems," *IEEE Trans. Wireless Commun.,* vol. 9, no. 12, pp. 3650-3661, Dec. 2010.

[8] B. Dulek and S. Gezici, "Detector randomization and stochastic signaling for minimum probability of error receivers," *IEEE Trans. Commun.,* vol. 60, no. 4, pp. 923-928, Apr. 2012.

[9] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. New York: McGraw-Hill, 2008.

[10] T. M. Cover and J. Thomas, *Elements of Information Theory*, 2nd ed. New York: Wiley, 2006.