Capacity of Correlated Jamming Channels.

Muriel Médard
Advanced Networks Group, MIT Lincoln Laboratory
Room C-277, 244 Wood Street, Lexington, MA 02173
medard@ll.mit.edu

Abstract

We derive the capacity of an AWGN channel where a jammer can make use of a (legitimate) sender's signal, intercepted through eavesdropping, to disrupt the legitimate user. Such a phenomenon is called correlated jamming. We derive the capacity of a correlated jamming channel with phase or time jitter in the channel tapping or jamming.

1 Introduction.

Correlated jamming, the situation where the jammer may correlate his signal to that of the legitimate user, poses a particular risk in certain types of channels. The subject has received attention in the wireless domain, for instance in the form of repeat-back jamming ([1, 2, 3, 4]). Correlated jamming may also yield a particularly nefarious attack in the area of optical communications, since a fiber may be physically tapped and have a signal injected into it.

Correlated jamming has also received attention in the information-theoretic literature. The effect of correlated jamming on SNR when the jammer has complete or incomplete information about the legitimate sender was examined in ([6]). Pessimum inteference was studied by Blachman ([7, 8]), who gives bounds on the capacity. A more general form of correlated jamming was studied by Başar and Başar in [9, 11, 10]. In [9], the optimum encoder-decoder structure and most nefarious noise are found unde a square-difference distortion measure for a finite number of transmissions of a Gaussian process over an AWGN channel with correlated jamming. In [11, 10], channel feedback is added. The jamming signal is subject to a power constraint but is allowed to be arbitrarily correlated with the encoded legitimate signal.

The purpose of this paper is to establish exact capacity results for channels with correlated jamming when the jammer has full or partial knowledge of the user's signal and when the jammer must contend with phase or time jitter. We use an approach combining optimal detection applied to entropy and convexity of entropy. We derive, in section 2, our results for correlated jamming, without making any restrictive assumptions about the capabilities of the jammer. The jammer is assumed to have perfect knowledge of the legitimate signal that is sent and he inserts a jamming signal by making use of his knowledge of the legitimate signal. In section 3, we consider eavesdropper correlated jamming, where the jammer derives his knowledge of the legitimate signal by eavesdropping. As we shall see, the jammer actually does not need very extensive capabilities to

disrupt communications significantly. The results are congurent with the results for the Gaussian test channel studied in [9] . In sections 4 and 5, we next extend our analysis to take into account the fact that, under some conditions, coherence and synchronicity may not be maintained by the jammer. We conclude and give directions for further research in section 6.

2 The correlated jamming attack.

We first consider how the jammer can disrupt communications when it has access to the legitimate signal. Let us first establish our notation. We assume an AWGN model for the channel noise. Let T be the time interval during which we transmit. By sampling at baseband at the Nyquist rate, W, we can reduce the continuous-time channel to a discrete-time channel where WT complex symbols are sent. The input symbols form the vector $\underline{X}_{2WT} = (X[1], \cdots X[2WT])$ where $X[i]$ is the real part of the i^{th} sample of the transmitted signal, sampled at the Nyquist rate of W Hz, and $X[WT+i]$ is the imaginary part of i^{th} sample. We denote by σ_X^2 the the average energy constraint on the real (complex) component of the transmitted signal. We assume an AWGN model for the channel noise. The noise vector is $\underline{N'}_{2WT}$, where all $2WT$ symbols are real IID zero-mean Gaussian distributed with variance σ_N^2. The signal received by the legitimate user in the absence of jamming is the vector $\underline{X}_{2WT} + \underline{N'}_{WT}$.

Let the average energy constraint on the jammer over the bandwidth W and time T be E_{Jammer}. Let $\underline{J}_{2WT}$ be the signal the jammer uses to disrupt $\underline{X}_{2WT} + \underline{N'}_{2WT}$. If $\underline{J}_{2WT}$ were uncorrelated with $\underline{X}_{2WT}$, then we know that it would be selected to be AWGN ([14, pg. 337]). Given the nature of common sources of AWGN in communications channels, we impose the condition that the jamming signal $\underline{J}_{2WT}$ must be independent of the AWGN noise component $\underline{N'}_{2WT}$. The jammer inserts his jamming signal $\underline{J}_{2WT}$ into the received signal of the legitimate user. We shall denote the attenuation at the point of jamming by γ. The legitimate receiver must attempt to recover $\underline{X}_{2WT}$ from the signal

$$\underline{Z}_{2WT} = \underline{X}_{2WT} + \sqrt{\gamma}\underline{J}_{2WT} + \underline{N'}_{2WT}. \tag{1}$$

Figure 1 shows the system considered in this section. The jammer seeks to minimize

$$I\left(\underline{Z}_{2WT}; \underline{X}_{2WT}\right) = h\left(\underline{X}_{2WT}\right) - h\left(\underline{X}_{2WT}|\underline{Z}_{2WT}\right). \tag{2}$$

The jammer cannot control the first term of the RHS of (2) and must therefore strive to maximize the second term, which may be rewritten as

$$h\left(\underline{X}_{2WT}|\underline{Z}_{2WT}\right) = h\left(\underline{X}_{2WT} - A\left(\underline{Z}_{2WT}\right)|\underline{Z}_{2WT}\right) \tag{3}$$

for some constant matrix A, since a constant shift leaves entropy unchanged. Therefore, since entropy is reduced by conditioning,

$$h\left(\underline{X}_{2WT}|\underline{Z}_{2WT}\right) \leq h\left(\underline{X}_{2WT} - A\left(\underline{Z}_{2WT}\right)\right). \tag{4}$$

In particular, we may pick A to be the linear least squared error (LLSE) estimate of $\underline{X}_{2WT}$ from $\underline{Z}_{2WT}$. The variance of the estimate error $\underline{X}_{2WT} - A\left(\underline{Z}_{2WT}\right)$ is

$$\Lambda_{\underline{X}_{2WT}} - \Lambda_{(\underline{X}_{2WT}, \underline{Z}_{2WT})} \Lambda_{\underline{Z}_{2WT}}^{-1} \Lambda_{(\underline{Z}_{2WT}, \underline{X}_{2WT})}$$

which we shall denote Λ_{Error}. Since, for a given autocorrelation matrix, entropy is maximized by a Gaussian distribution, we have that ([13, pg. 234]),

$$h\left(\underline{X}_{2WT} - A\left(\underline{Z}_{2WT}\right) | \underline{Z}_{2WT}\right) \leq \frac{1}{2} ln\left((2\pi e)^{2WT} \mid \Lambda_{Error} \mid\right) \tag{5}$$

where $| \; |$ denotes the absolute value of the determinant.

Let us now establish what signalling scheme the sender should use and what jamming scheme the jammer should use. To do so, we shall first assume a WGN signal for the sender. We shall determine the optimal jamming scheme for a WGN sender's signal. The jammer attempts to minimize $I\left(\underline{Z}_{2WT}; \underline{X}_{2WT}\right)$ by changing the transition probabilities of the channel connecting $\underline{Z}_{2WT}$ and $\underline{X}_{2WT}$. Next, we shall assume that the jammer uses the jamming scheme that is optimal for a WGN sender's signal. We shall then allow the sender to vary its signal and shall determine that the maximum rate is achieved by sending a WGN signal. Thus, since the mutual information is a concave function in the input probability and a convex function in the set of transition probabilities [14, pp. 89–91], we shall have shown that the best signalling scheme for the sender is a WGN signal and shall have determined what the jammer's scheme is for that signalling case. Our approach is different from [9], which does not consider capacity, but our results are congruent with those of [9].

We first assume that the transmitter picks a Gaussian signal $\underline{X}_{2WT}$ scheme for the AWGN over which it sends. By selecting $\underline{J}_{2WT}$ to be Gaussian and jointly Gaussian with $\underline{X}_{2WT}$ and $\underline{N'}_{2WT}$, the LLSE estimate $\underline{X}_{2WT} - A\left(\underline{Z}_{2WT}\right)$ is also the minimum variance error (MVE) estimate and the Bayesian estimate. If $\underline{J}_{2WT}$ is Gaussian, then $\underline{X}_{2WT} - A\left(\underline{Z}_{2WT}\right)$ is a Gaussian vector error which is independent of the signal from which the estimate was obtained, therefore both (4) and (5) hold with equality. Moreover, any value of Λ_{Error} allowed by our constraints may be achieved by picking $\underline{J}_{2WT}$ Gaussian and jointly Gaussian with $\underline{X}_{2WT}$. Hence, the jammer will pick $\underline{J}_{2WT}$ Gaussian and jointly Gaussian with $\underline{X}_{2WT}$.

Let us now determine the form of $\Lambda_{\underline{J}_{2WT}}$ which the jammer will pick. Since conditioning reduces entropy, we may use the chain rule for entropies to write

$$h(\underline{X}_{2WT} | \underline{Z}_{2WT}) \leq \sum_{i=1}^{TW} h(X[i] || Z[i]) + \sum_{i=TW+1}^{2TW} h(X[i] || Z[i]). \tag{6}$$

The $X[i]$s are IID, the $N'[i]$s are IID and the $X[i]$s and the $N'[i]$s are mutually independent. Hence, from (1), we see that (6) may be achieved with equality by taking $J[i]$ to be independent of all $N'[j]$, $X[j]$ for all $j \neq i$. Thus, from (2)-(6), minimizing the LHS of (2) becomes equivalent to minimizing

$$\sum_{i=1}^{2WT} h\left(X[i]\right) - h\left(X[i] | Z[i]\right). \tag{7}$$

Note that $\underline{J}_{2WT}$ and $\underline{X}_{2WT}$ are Gaussian and jointly Gaussian implies that $\underline{X}_{2WT}$ and $\underline{Z}_{2WT}$ are Gaussian and jointly Gaussian. We have ([15])

$$h\left(X[i]\right) - h\left(X[i] | Z[i]\right) = \frac{1}{2}\left(ln\left(\sigma_X^2\right) + ln\left(\sigma_Z^2\right) - ln\left(\left| \begin{array}{cc} \sigma_X^2 & \sigma_{XZ} \\ \sigma_{XZ} & \sigma_Z^2 \end{array} \right|\right)\right). \tag{8}$$

Therefore, we may achieve any value of (7) by picking $J[i]$ to be the sum of $X[i]$, multiplied by some factor, and of some Gaussian variable independent of $X[i]$. To minimize the LHS

of (2), we may choose for each i $J[i] = \xi_i X[i] + R[i]$. To satisfy our conditions that make (6) hold with equality, all the $R[i]$s are mutually independent and independent of all $X[j]$ for all $j \neq i$. Moreover, to satisfy the condition that the jamming signal be independent of the AWGN, we must have all the $R[i]$s independent of all $N'[j]$ for all j. Finally, since all the $X[i]$s are IID and all the $N[i]$s are IID, we may use the concavity of the ln function to establish that we want all the $R[i]$s to be IID and all the ξ_i to be equal to some ξ. We may rewrite (7) as $\sum_{i=1}^{2WT} h(Z[i]) - h(Z[i]|X[i])$ where $Z[i] = \left(1 + \sqrt{\gamma}\xi\right) X[i] + R[i] + N'[i]$. The signal seen by the jammed user therefore has a white Gaussian signal with variance $\left(1 + \sqrt{\gamma}\xi\right)^2 \sigma_X^2$ and AWGN with variance $\sigma_R^2 + \sigma_N^2$. Thus, the problem of minimizing the LHS of (2) now becomes the problem of minimizing

$$g(\xi) = \frac{1}{2} ln \left(\frac{(1 + \sqrt{\gamma}\xi)^2 \sigma_X^2 + \gamma\sigma_R^2 + \sigma_N^2}{\gamma\sigma_R^2 + \sigma_N^2} \right) \tag{9}$$

subject to

$$\xi^2 \sigma_X^2 + \sigma_R^2 \leq E_{Jammer}. \tag{10}$$

For a problem where the jammer has very high power, where $\gamma E_{Jammer} \geq \sigma_X^2$, then we may design $\underline{X}_{2WT}$ to subtract all the signal part of $\underline{Z}_{2WT}$. If the jammer cannot altogether eliminate all of the signal component, then it must allocate its power most effectively to reduce the SNR. We have that $g''(\xi) \geq 0$ and that $g'(\xi) = 0$ only for

$$\xi = -\frac{\sigma_X^2 + \gamma E_{Jammer} + \sigma_N^2 - |\sigma_X^2 - \gamma E_{Jammer} - \sigma_N^2|}{2\sqrt{\gamma}\sigma_X^2}. \tag{11}$$

We denote the above RHS by λ. Substituting and solving for ξ, we obtain that

$$\xi = \begin{cases} max\left(\lambda, -\sqrt{\frac{E_{Jammer}}{\sigma_X^2}}\right), & \text{if } \gamma E_{Jammer} \leq \sigma_X^2 \\ -\frac{1}{\sqrt{\gamma}}, & \text{if } \gamma E_{Jammer} \geq \sigma_X^2 \end{cases}. \tag{12}$$

Let us now show that the sender cannot do better than to send a WGN signal. Let us consider that we have an AWGN channel, with amplification $1 + \sqrt{\gamma}\xi$ and with noise variance $\gamma\sigma_R^2 + \sigma_N^2$. Then, we know that a WGN signal is optimal. Since the mutual information is concave in the input distribution and convex in the transition probabilities, we have a saddle point.

Note that the correlated jammer simply needs to be able to amplify negatively (i.e. amplify with a phase shift of π) $\underline{X}_{2WT}$ and to generate AWGN. The variable ξ denotes the factor by which the original signal $\underline{X}_{2WT}$ is multiplied to form the correlated component of the jamming signal $\underline{J}_{2WT}$. In particular, the jammer does not need to *detect* $\underline{X}_{2WT}$. The average mutual information obtained in (9) is indeed a capacity, because we have reduced the channel to an AWGN channel.

3 The eavesdropper correlated jamming attack.

We now examine the question of what signal should be sent by a jammer whose only access to the transmitted signal is via tapping. The jamming signal can never be such that observing it yields a better estimate of $\underline{X}_{2WT}$ than that obtained via tapping. The noise over the eavesdropper's channel is represented by the vector $\underline{N}_{2WT}$ where all $2WT$

symbols are real IID zero-mean Gaussian. The rate obtained via tapping by an eavesdropper can easily be obtained, for instance by modifying our problem to be compatible with the framework of [16, 17]. Note that, in the rest of the paper, we do not endow the information obtained by the eavesdropper about the legitimate transmitted signal with any semantic implications. A correlated jammer does not need to have information about the plaintext, but only about the signal sent by the legitimate user.

Figure 2 shows the eavesdropper correlated channel considered in this section. The attenuation at the point of jamming is denoted by γ and the attenuation at the point of tapping by α. The jammer sends a signal J. Using our previous convention for representing a complex signal, we may express the i^{th} sample of J as:

$$J[i] = \xi Y[i] + R'[i]. \tag{13}$$

The channel jammed by an eavesdropper correlated jammer sees the signal whose i^{th} time sample is given by

$$Z[i] = \sqrt{\alpha}J[i] + N'[i] = (1 + \sqrt{\gamma}\sqrt{\alpha}\xi)X[i] + \sqrt{\alpha}\xi N[i] + \sqrt{\alpha}R'[i] + N'[i]. \tag{14}$$

For ease of exposition, we assume that the variance of $N'[i]$ and that of $N[i]$ are both equal to σ_N^2. The extension to the case where they are different is straightforward. The same arguments as in the previous section show that a saddle point is reached when the sender and the jammer transmit in such a manner that the $X[i]$s are samples of a WGN process and the $R'[i]$s are also samples of a WGN process and are independent of the X and N processes. Thus, the RHS of (14) has a signal term with a white Gaussian distribution of variance $(1+\sqrt{\gamma}\sqrt{\alpha}\xi)^2\sigma_X^2$ and an AWGN component with variance $\gamma\sigma_{R'}^2 + (\gamma\alpha\xi^2+1)\sigma_N^2$. The coefficient ξ now indicates the weighting that the jammer gives to the signal $\underline{Y}_{2WT}$ obtained through tapping. Therefore, the function to minimize, which is given by (9) in the previous section, is now

$$g_{eaves}(\xi) = \frac{1}{2} ln \left(\frac{(1 + \sqrt{\gamma}\sqrt{\alpha}\xi)^2\sigma_X^2 + \gamma\sigma_{R'}^2 + (\gamma\alpha\xi^2 + 1)\sigma_N^2}{\gamma\sigma_{R'}^2 + (\gamma\alpha\xi^2 + 1)\sigma_N^2} \right). \tag{15}$$

The constraint of (10) becomes

$$\xi^2\alpha\left(\sigma_X^2 + \sigma_N^2\right) + \sigma_{R'}^2 \leq E_{Jammer}. \tag{16}$$

We may verify that any solution feasible in the eavesdropper correlated case is feasible in the correlated case studied in section 2. The minimization of (9) subject (10) cannot therefore be more than the solution to minimizing (15) subject to (16) alone. The solution of (15) subject to (16) is

$$\xi = \begin{cases} -\frac{1}{\sqrt{\gamma\alpha}}, & \text{if } \gamma E_{Jammer}\frac{\sigma_X^2}{\sigma_X^2+\sigma_N^2} \geq \sigma_X^2 \\ \mu, & \text{if } \gamma E_{Jammer}\frac{\sigma_X^2}{\sigma_X^2+\sigma_N^2} \geq \sigma_X^2, \text{ and } g_{eaves}(\mu) < g_{eaves}(\nu) \\ \nu & \text{otherwise} \end{cases} \tag{17}$$

for $\nu = -\sqrt{\frac{E_{Jammer}}{\alpha\left(\sigma_X^2+\sigma_N^2\right)}}$ and $\mu = \frac{-b+\sqrt{b^2-4ac}}{2a}$ where $a = \sigma_X^2\gamma\alpha$, $b = \sqrt{\gamma\alpha}\sigma_N^2 + \sqrt{\alpha}\gamma^{\frac{3}{2}}E_{Jammer} + \sqrt{\gamma\alpha}\sigma_X^2$ and $c = \sigma_N^2 + \gamma E_{Jammer}$. As for the correlated jamming case studied in the previous section, we see that the capabilities required for performing eavesdropper correlated jamming are amplification and phase shift of the tapped signal and addition of white noise. The conditions we impose on the jammer in (16) could be changed to take into account different constraints. For instance, a minimum noise constraint of σ_{min}^2 for the jamming signal would lead to a constraint of the form $\sigma_{R'}^2 \geq \sigma_{min}^2$. A maximum amplification amplitude of ξ_{max} would lead to a constraint of the form $\xi^2 \leq \xi_{max}^2$.

4 The effect of phase jitter.

In this section, we analyze the effect upon correlated jamming of a phase shift which is not known to the jammer. If the phase shift were known to the jammer, he could compensate for it in his jamming scheme. Such a phase shift may occur because the jammer has mistakingly evaluated the phase of the legitimate user or it may be deliberately introduced by the legitimate user after the point of tapping. Such a phase may be modelled by adding a phase shift to the legitimate signal after the eavesdropping has occured or by adding a phase shift to the jamming signal. We choose the latter approach. We denote the phase shift by ϕ. We assume that the phase shift is time-invariant, therefore we do not have bandwidth expansion which is due to changes in the phase shift. Moreover, the fact that the phase shift is constant implies that the legitimate receiver is informed of the phase shift or can determine it without affecting capacity. Therefore, the receiver can take ϕ into account when he receives the signal.

We first look at the effect of a phase shift for a given ξ and then assume a distribution fo ξ. The received signal sampled vector, $\underline{Z}_{2WT}$, is given by

$$\begin{aligned} Z[i] &= X[i] + \sqrt{\gamma}\sqrt{\alpha}\xi\left(cos\left(\phi\right)X[i] - sin\left(\phi\right)X[i+WT]\right) \\ &+ \sqrt{\gamma}\sqrt{\alpha}\xi N[i] + \sqrt{\gamma}R'[i] + N'[i] \end{aligned} \tag{18}$$

for $1 \leq i \leq WT$ and

$$\begin{aligned} Z[i] &= X[i] + \sqrt{\gamma}\sqrt{\alpha}\xi\left(cos\left(\phi\right)X[i] + sin\left(\phi\right)X[i-WT]\right) \\ &+ \sqrt{\gamma}\sqrt{\alpha}\xi N[i] + \sqrt{\gamma}R'[i] + N'[i] \end{aligned} \tag{19}$$

for $WT+1 \leq i \leq 2WT$. We may compute the capacity of the legitimate user for a given ϕ and ξ. As in our previous sections, we first assume that the sender's signal is complex WGN. The same arguments as in the previous sections lead to the fact that the jammer chooses R' to be AWGN uncorrelated with N and X. The entropy of $\underline{Z}_{2WT}$ is $\frac{1}{2}ln\left(\left(2\pi\right)^{2WT}\left|\Lambda_{\underline{Z}_{2WT}}\right|\right)$, where $\Lambda_{\underline{Z}_{2WT}}$ is a diagonal matrix with diagonal terms

$$d = \sigma_X^2\left(1 + 2\sqrt{\gamma}\sqrt{\alpha}\xi cos\left(\phi\right) + \gamma\alpha\xi^2\right) + \left(\gamma\alpha\xi^2 + 1\right)\sigma_N^2 + \gamma\sigma_{R'}^2. \tag{20}$$

Therefore, from (18-19), the mututal information for the channel seen by the legitimate user is given by

$$WTln\left(\frac{\left|d\right|}{\left(1+\gamma\alpha\xi^2\right)\sigma_N^2 + \gamma\sigma_{R'}^2}\right). \tag{21}$$

Note that, as in the previous sections, the optimum signalling for the user when the jammer uses such a scheme is WGN. We have therefore found a saddle point.

If the jammer knows that there is phase shift and knows a distribution on the phase shift, he may take the phase shift into account in his choice of ξ. The goal of the jammer is to minimize the expected capacity of the legitimate user's channel, hence to minimize $E_\phi\left[I\left(\underline{Z}_{2WT};\underline{X}_{2WT}|\phi\right)\right]$, where the expectation is taken over ϕ, which is known to the receiver. We now examine the case where the *a priori* distribution of ϕ is uniform between 0 and 2π, i.e. all guesses about the phase by the jammer are equally poor. Using (20, 21), the goal of the jammer is to minimize

$$\frac{1}{4\pi}\int_0^{2\pi} ln\left(1 + \frac{\sigma_X^2\left(1 + 2\sqrt{\gamma\alpha}\xi cos\left(\phi\right) + \gamma\alpha\xi^2\right)}{\left(1+\gamma\alpha\xi^2\right)\sigma_N^2 + \gamma\sigma_{R'}^2}\right)d\phi. \tag{22}$$

By a change of variables, we use equation 4.292.3 in [20] to rewrite (22) as

$$g_{phase_1}(\xi) = \frac{1}{2} ln \left(a \frac{1 + \sqrt{1 - \frac{b^2}{a^2}}}{2} \right) \tag{23}$$

where $a = 1 + \frac{\sigma_X^2 \left(1+\gamma\alpha\xi^2\right)}{(1+\gamma\alpha\xi^2)\sigma_N^2 + \gamma\sigma_{R'}^2}$ and $b = \frac{2\sigma_X^2\sqrt{\gamma\alpha}\xi}{(1+\gamma\alpha\xi^2)\sigma_N^2 + \gamma\sigma_{R'}^2}$. We have $g'_{phase_1}(\xi) = 0$ and $g''_{phase_1}(\xi) > 0$ only for $\xi = 0$, therefore the jammer chooses ξ to be 0. Thus, uncorrelated jamming is preferable when the jammer has abolutely no estimate of ϕ.

5 The effect of timing jitter.

Instead of a phase offset, there may exist a timing offset introduced by the legitimate user or caused by the jammer's inability to time the jamming signal exactly. For instance, the fiber lengths may be such that a jammer cannot exactly achieve synchronization, because the jamming signal traverses a longer length of fiber than the legitimate signal. Note that, in general, a timing jitter and a phase offset will occur together. We do not consider the two together in this paper, but the techniques we develop would be applicable. Even if the jammer knows the offset exactly, he cannot compensate for such a time offset because it is not reversible, unlike a phase offset. If the legitimate user is delayed and the jammer knows this delay exactly, the jammer can introduce the same delay in the jamming signal. Let us suppose that the jammer is lagging behind the legitimate signal, perhaps because the jammer uses a piece of fiber which is slightly longer than that traversed by the legitimate signal. The received signal sampled vector, Z_{2WT}, is given by

$$Z[i] = X[i] + \sqrt{\gamma}\sqrt{\alpha}\xi \left(\beta X[i] + (1-\beta) X[i-1]\right) + \sqrt{\gamma}\sqrt{\alpha}\xi N[i] + \sqrt{\gamma}R'[i] + N'[i] \tag{24}$$

for $1 \leq i \leq 2WT$. Note that the timing offset would involve $X[i+1]$ instead of $X[i]$ if the legitimate user introduced a delay after the tapping point.

As before, we assume that the legitimate user sends a Gaussian signal, although the signal is no longer white, since we have an ISI channel. Given such a signalling scheme, the same arguments used in the previous sections imply that the best jammer policy is to send a jamming signal which is the sum of the negatively amplified tapped signal and of AWGN uncorrelated with X and N'. Given such a jamming policy, we may show that a Gaussian signal is the best that the sender can use. In order to find the optimal choice of ξ, we shall derive the capacity of the channel in terms of ξ. The terms of the autocorrelation matrix of the received signal are

$$\Lambda_{\underline{Z}_{2WT}}[i,j] = \begin{cases} p, & \text{for } i = j \\ q, & \text{for } |i-j| = 1 \\ 0, & \text{otherwise} \end{cases} \tag{25}$$

$$\begin{aligned} p &= \sigma_X^2 \left(\left(1 + \sqrt{\gamma}\sqrt{\alpha}\beta\xi\right)^2 + (1-\beta)^2 \right) + \sigma_N^2 \left(\gamma\alpha\xi^2 + 1\right) + \gamma\sigma_{R'}^2 \\ q &= \sigma_X^2 \left(1 + \sqrt{\gamma}\sqrt{\alpha}\beta\xi\right)(1-\beta). \end{aligned} \tag{26}$$

If ξ and β are given, then the capacity of the channel is known, because it is a channel with time-invariant ISI ([18, 19, 5]), which can equivalently be considered as a channel

with colored Gaussian noise ([13]). We shall use the results of ([18]) to find the capacity of the correlated jamming channel. Let us define the spectrum of the Toeplitz matrix $\Lambda_{\underline{Z}_{2WT}}$ to be

$$|a(\lambda)|^2 = \left|\left(1+\sqrt{\gamma}\sqrt{\alpha}\xi\beta\right)+\sqrt{\gamma}\sqrt{\alpha}\xi(1-\beta)e^{i\lambda}\right|^2. \tag{27}$$

Let us define $\sigma^2 = \sigma_N^2(\gamma\alpha\xi^2+1)+\gamma\sigma_{R'}^2$. From (5.3) in ([18]), we have that the capacity is given by

$$\frac{1}{4\pi}\int_0^{2\pi} ln\left(\max\left[|a(\lambda)|^2\theta\sigma^{-2},1\right]\right)d\lambda \tag{28}$$

where $\sigma_X^2 = \frac{1}{2\pi}\int_0^{2\pi}\max\left[\theta-\sigma^2|a(\lambda)|^{-2},0\right]d\lambda$. In order to obtain a closed form solution, let us assume that the SNR is large enough that

$$\theta = \sigma_X^2 + \frac{\sigma^2}{(1+c)^2}\frac{1}{2\pi}\int_0^{2\pi}\frac{1}{1+2\frac{b}{1+c}cos(\lambda)+\left(\frac{b}{1+c}\right)^2}d\lambda \tag{29}$$

for $b=\sqrt{\gamma\alpha}\xi\beta$ and $c=\sqrt{\gamma\alpha}\xi(1-\beta)$. If we assume that $\left|\frac{b}{1+c}\right|\leq 1$, we may use, from [20], equation 3.665.2, to obtain

$$g_{delay}(\xi) = \frac{1}{2}\left[ln\left(\theta\sigma^{-2}\right)+ln\left((1+c)^2\right)\right]. \tag{30}$$

Note that our average mutual information does indeed give us a capacity, because we have reduced the channel to a time-invariant ISI chanel with AGWN.

6 Conclusions.

We have investigated the capacity of channels with correlated jamming. We have shown that correlated jamming can be a particularly nefarious attack, when compared to uncorrelated jamming. Correlated jamming can occur even when the jammer has access to only a noisy version of the legitimate user's signal and when the jammer must contend with phase or timing jitter. The implications of in-fiber correlated jamming for optical communications may be significant because, as we have shown, correlated jamming requires very simple processing on the part of the jammer and may be effective without changing the output power that would be received for an uncorrupted legitimate signal. Therefore, most traditional methods for detecting fiber tapping and jamming, which rely upon detecting variations in received power, may not be effective.

References

[1] E.A. Gerianotis, "Direct-Sequence Spread-Spectrum Communications in a Multiple-Tone and Repeat-Back Jamming Environment", in *Proceedings of the 1983 IEEE Military Communications Conference*, vol. 3, pp. 765–769.

[2] F. Qian, B.D. Van Veen, "Partially Adaptive Beamforming for Correlated Interference Rejection", *IEEE Transactions on Signal Processing*, vol. 43, no. 2, February 1995, pp. 506–515.

[3] L.C. Godara, "Beamforming in the Presence of Broadband Correlated Arrivals", *Journal of the Acoustical Journal of America*, vol. 92, no. 5, November 1992, pp .2702-2708.

[4] P. Evans, *Measured Effects of Repeater Jamming on Direct-Sequence Spread-Spectrum Receivers that Use Envelope Detectors*, M.S. Thesis, Naval Postgraduate School, Monterey, California, September 1989.

[5] W. Hirt, J.L. Massey, "Capacity of the Discrete-Time Gaussian Channel with Intersymbol Interference", *IEEE Transactions on Information Theory*, vol. 34, no. 3, May 1988, pp. 380–388.

[6] L.-H. Zetterberg, "Signal Detection Under Noise Interference in a Game Situation", *IRE Transactions on Information Theory*, vol. IT-8, no. 1, September 1962, pp. S47–S51.

[7] N.M. Blachman, "On the Capacity of a Band-Limited Channel Perturbed by Statistically Dependent Interference", *IRE Transactions on Information Theory*, vol. IT-8, no. 1, January 1962, pp. 48–55.

[8] N.M. Blachman, "The Effect of Statistically Dependent Interference Upon Channel Capacity", *IRE Transactions on Information Theory*, vol. IT-8, no. 1, September 1962, pp. S53–S57.

[9] T. Başar, "The Gaussian Test Channel with an Intelligent Jammer", *IEEE Transactions on Information Theory*, vol. IT-29, no. 1, January 1983, pp. 152–157.

[10] T. Ü. Başar , T. Başar, "Optimum Linear Causal Coding Schemes for Stochastic Processes in the Presence of Correlated Jamming", in *Proceedings of the Twentieth Conference on Information Sciences and Systems*, 1986, pp. 384–386.

[11] T. Başar, T. Ü. Başar "A Bandwidth Expanding Scheme for Communication Channels with Noiseless Feedback in the Pesence of Unknown Jamming Noise", *Journal of the Franklin Institute*, vol. 317, no. 2, pp. 73–78.

[12] T. Ü. Başar , T. Başar, "Robust Linear Coding in Continuous-time Communication Systems in the Presence of Jamming and with Noisy Side Information at the Decoder", in *Proceedings of the 1982 Conference on Information Science Systems*, 1982, pp. 323–326.

[13] T.M. Cover, J.A. Thomas, *Elements of Information Theory*, John Wiley & Sons, 1991.

[14] R.G. Gallager, *Information Theory and Reliable Communications*, John Wiley & Sons, 1968.

[15] M.S. Pinsker, "Information About a Gaussian Random Stationay Process Contained in a Another Process, Stationarily Correlated With the First", Doklady Akademii Nauk, tome XCIX, no. 2, 1954, pp. 213–216.

[16] A.D. Wyner, "The Wire-Tap Channel", *The Bell System Technical Journal*, vol. 54, no. 8, October 1975, pp. 1355-1387.

[17] L.H. Ozarow, A.D. Wyner, "Wire-Tap Channel II", in *Proceedings of Eurocrypt 84*, Springer-Verlag.

[18] R.M. Gray, "On the Asymptotic Eigenvalue Distribution of Toeplitz Matrices", *IEEE Transactions on Information Theory*, vol. IT-18, no. 6, November 1972, pp. 725–729.

[19] B.S. Tsybakov, "On the Transmission Capacity of a Discrete-Time Gaussian Channel with Filter", Problemy Peredachi Informatzii, vol. 6, 1970, pp. 78–82.

[20] I.S. Gradshteyn, I.M. Ryzhik, "Table of Integrals, Series and Products", Academic Press, 1965.

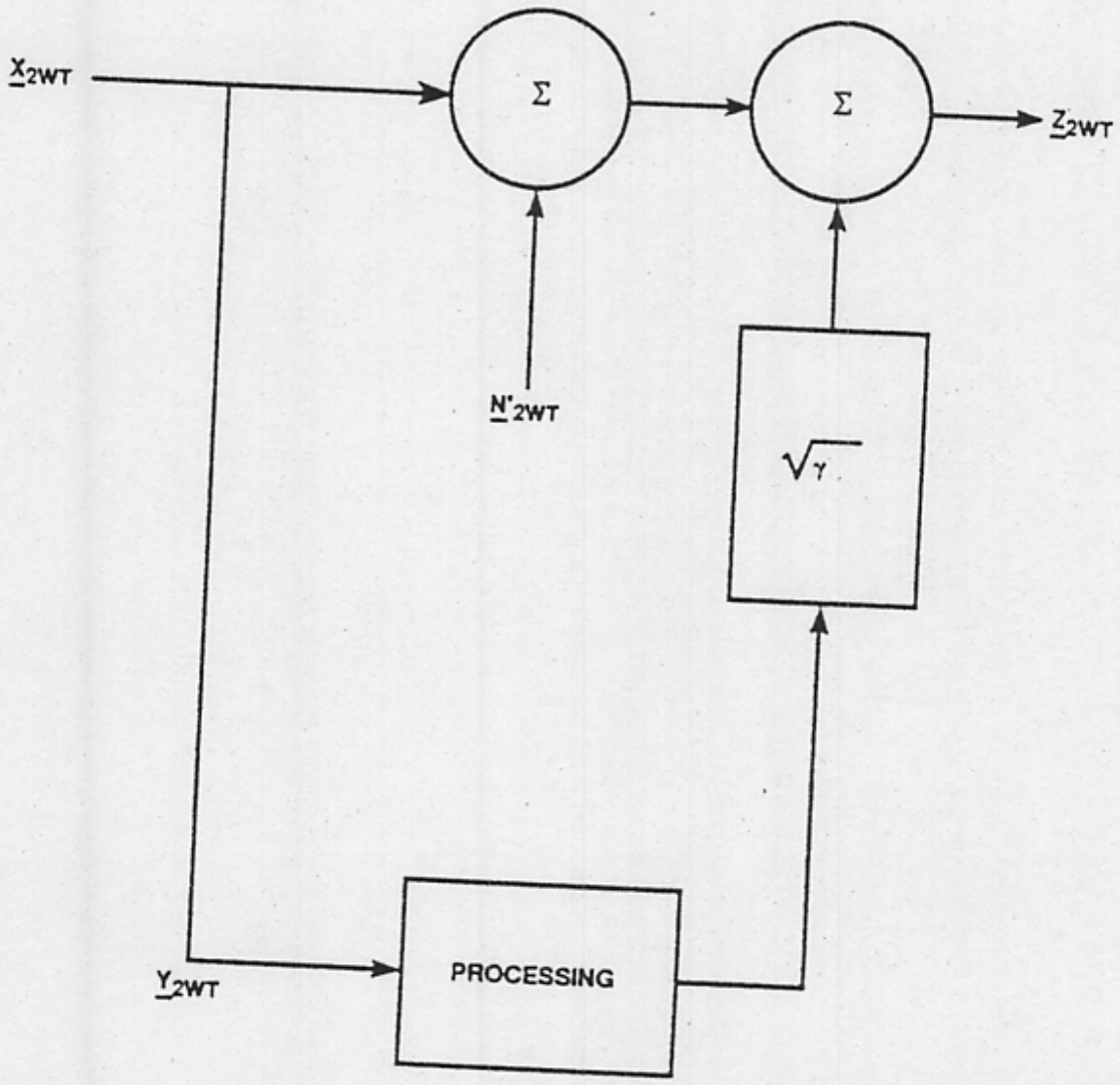

Figure 1: Correlated jamming channel.

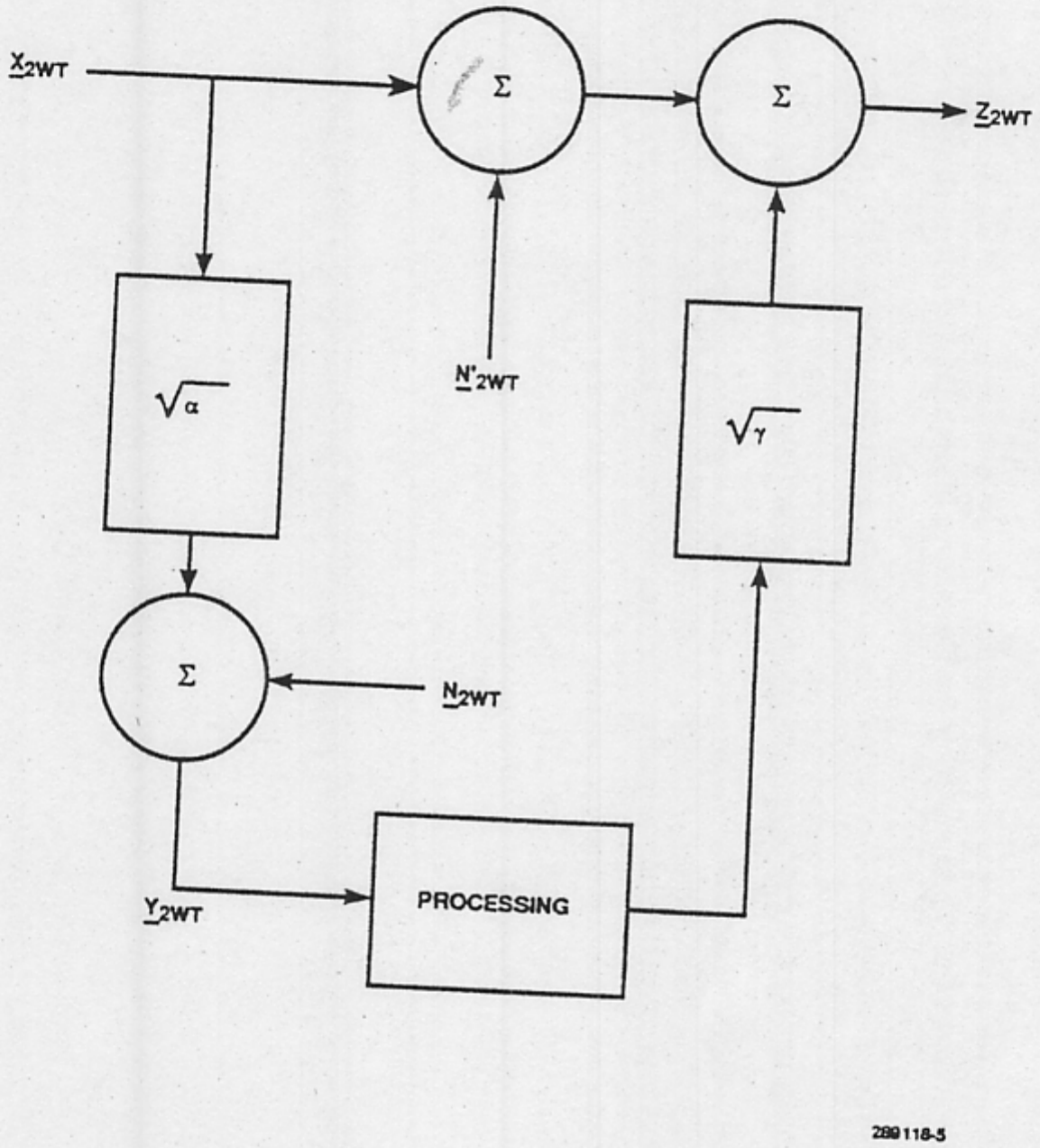

Figure 2: Eavesdropper correlated jamming channel.