Jamming a TDD Point-to-Point Link Using Reciprocity-Based MIMO

Marcus Karlsson, Emil Björnson and Erik G Larsson

Jamming a TDD Point-to-Point Link Using Reciprocity-Based MIMO

Marcus Karlsson, Emil Björnson and Erik G. Larsson

Abstract—**We present a method for jamming a time-division duplex link using a transceiver with a large number of antennas. By utilizing beamforming, a jammer with M antennas can degrade the spectral efficiency of the primary link more than conventional omnidirectional jammers under the same power constraint, or perform equally well with approximately $1/M$ of the output power. The jammer operates without any prior knowledge of channels to the legitimate transmitters, or the legitimate signals by relying on channel reciprocity.**

I. Introduction

Reciprocity-based multiple-input multiple-output (MIMO) refers to the subset of MIMO systems which rely on channel reciprocity: the fact that for a given frequency band, the channel response between two transceivers is the same in both directions. Perhaps the ultimate form of reciprocity-based MIMO is massive MIMO: a cellular wireless technology, conceived in [1], in which the base station is equipped with hundreds or more antennas. Operating in time-division duplex (TDD) mode, the base station learns the uplink and downlink channels simultaneously from uplink pilots. The base station can then multiplex spatially, in the same time-frequency resource, to all active terminals and achieve a high spectral efficiency. Since 2010, several testbeds have emerged, and the basic technology is maturing, gaining both academic attention, e.g. [2]–[4], as well as industrial attention, e.g. Terragraph and Project ARIES.

The introduction of software-defined radio, and mature hardware has turned jamming from a hardware to a software issue, making it readily available to almost anyone. Today anyone with access to the Internet, a few $100 and some technical know-how can create a jammer with the ability to jam LTE systems [5], [6]. Jamming of GPS receivers [7], or jamming of private/professional mobile radio systems [8] used by first responders have been observed, and can have drastic effects. Vulnerabilities in CDMA systems are discussed in [9], while [6], [10], [11] discuss options of jamming mitigation in OFDM systems.

A. Prior Work

In broad terms, the jamming literature can be divided into two categories: jammers without any information about the legitimate system or channel state information (CSI), and jammers with CSI and/or information about the legitimate signal. It has been shown that in the former case, barrage jamming and omnidirectional jamming are optimal [12]–[17]. In the latter case, more effective techniques can be used [13], [15]–[19]. For example, if the jammer has CSI and knowledge of the structure of the legitimate signal, the jammer can beamform noise to the target or focus jamming on the training phase of the legitimate link to increase jamming performance. As a jammer and a legitimate transmitter can naturally be seen as two non-cooperative opponents, jamming problems are sometimes analyzed using a game-theoretic approach [20]–[23].

In the reciprocity-based MIMO context, physical layer security has been studied with both passive and active eavesdroppers, see e.g. [24] for an overview. In [25], the authors study a passive multi-antenna eavesdropper in a multi-cell setup. Moreover, jamming of massive MIMO systems has also been analyzed for some specific scenarios [26]–[28]. In [26], [27], massive MIMO technology is used to *mitigate* jamming, and in [28] the authors discuss the scenario where a single-antenna jammer aims to degrade the performance of a massive MIMO base station as much as possible.

B. Specific Contributions

As opposed to other multi-antenna jammers using perfect CSI or knowledge of the legitimate signal in order to device a potent jamming strategy [15], [17], [18], [20], [21], [29]–[31], our proposed jammer does not rely on prior knowledge of the channel state, or of the legitimate signal, but is able leverage the reciprocity inherent to TDD-systems to estimate the channel to the target, outperforming an omnidirectional barrage jammer. The jammer only has limited knowledge of the legitimate link: an upper bound on the maximum excess delay (number of taps) of the frequency-selective channel, the carrier frequency of the legitimate link, and the time duration of each transmission slot (all of which could be estimated, but are assumed to be known here). Throughout the paper, we assume that the legitimate transmitters use Gaussian codebooks, for which every transmitted sample is equally important. In practice, the transmitted block is typically composed symbols of different importance, for example pilots and payload data. In that case, targeting the pilots with the jamming can be an effective strategy, see, e.g., [17], [18], [28]. However, in order to target the pilots specifically, additional information about the signal transmitted by the legitimate system would be needed. The proposed jammer does not have or need such additional information, which is a big advantage.

The initial idea of using a reciprocity-based MIMO jammer to attack a point-to-point TDD link was presented by us

The authors are with the Department of Electrical Engineering (ISY), Linköping University, 581 83 Linköping, Sweden (email: {marcus.karlsson, emil.bjornson, erik.g.larsson}@liu.se).

This work was supported in part by the Swedish Research Council (VR), and ELLIIT.

A preliminary version of parts of this work was presented at the Asilomar Conference on Signals, Systems and Computers, 2014 [32].

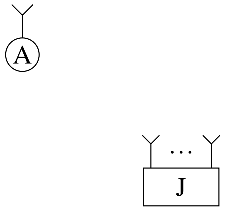


Fig. 1. The system consists of two legitimate, single-antenna users, (A)lice and (B)ob, as well as a malicious multi-antenna transmitter—(J)eff—who aims to disrupt the communication between Alice and Bob.

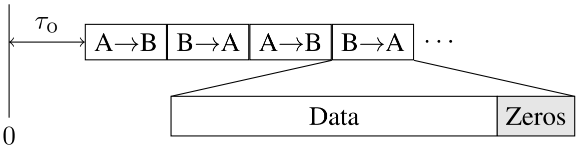


Fig. 2. The legitimate transmission starts at time τ_{O} with Alice transmitting to Bob. After this, Alice and Bob take turns transmitting every other frame. Each frame is τ_{F} samples long. The last $L-1$ is the guard interval where neither Alice nor Bob transmits, leaving $\tau_{\text{F}}-(L-1)$ useful symbols.

in [32], in which we covered the frequency-flat case. In most systems, however, the channel is frequency selective, which complicates both the analysis and the algorithm design. Comparing the jamming scheme presented here to the one presented in [32] (see Sections IV-B and V) shows that the former is superior to the latter for frequency-selective channels. This paper further gives a more detailed description of the proposed jamming scheme and considers a slightly different, more rigorous performance metric. The paper also discusses possible countermeasures the legitimate link can use, and a clear motivation to the use of reciprocity-based MIMO technology.

In this paper, we treat the problem in the time domain, but it could in principle equivalently be treated in the frequency domain. Assuming a cyclic prefix and orthogonal frequency-division multiplexing (OFDM) transmission, each subcarrier could then be described by the model in [32]. However, the estimation of the frame timing (Section III-A) is not straightforward in the frequency domain. Moreover, the jammer would have to know/estimate the length of the cyclic prefix used in the legitimate link and fuse the estimates given by the different subcarriers. The jammer would further have to allocate power over the subcarriers in order to increase jamming performance.

II. System Model

We consider a system consisting of two legitimate users (terminals) communicating over a legitimate link in TDD mode.[1] The terminals are equipped with a single antenna each and are considered to be identical. In addition, there is a multi-antenna jammer present, seen in Fig. 1, whose goal is to disrupt the communication over the legitimate link as much as possible. In other words, the jammer wants to degrade the legitimate link to the extent that communication with an adequate rate is impossible. We adopt the nomenclature common in the field and call the two terminals Alice and Bob. We further call the jammer Jeff [16].

A. The Legitimate Link

Alice and Bob split the transmission time equally and transmit every other *transmission frame*, where each transmission frame consists of $\tau_{\text{F}}=\tau_{\text{C}}/2$ samples, where τ_{C} is the length of the coherence interval, measured in samples. We assume an underspread channel [34, Section 2.3.2], i.e., the coherence time is much larger than the delay spread. We let Alice denote the terminal transmitting in odd transmission frames and Bob denote the terminal transmitting in even transmission frames, see Fig. 2. If the terminals switch order, they also switch names.

We refer to the time instant when the jammer starts listening to the legitimate link as time zero, or $n=0$. The number of samples from time zero to the start of the first transmission frame is called the *frame offset* and is denoted by $\tau_{\text{O}}\in\mathbb{N}$, illustrated in Fig. 2. We let $\mathrm{F}_k(\tau)$ denote the collection of samples $(k-1)\tau_{\text{F}}+\tau$ through $k\tau_{\text{F}}+\tau-1$ and call $\mathrm{F}_k(\tau)$ a frame. In other words, $\mathrm{F}_k(\tau)$ contains all samples n such that

$$n\in\mathrm{F}_k(\tau)\Leftrightarrow n-\tau\in\left[(k-1)\tau_{\text{F}},k\tau_{\text{F}}-1\right].$$

In particular we define $\bar{\mathrm{F}}_k\triangleq\mathrm{F}_k(\tau_{\text{O}})$ (the kth transmission frame), as this will be used frequently throughout the paper.

Alice and Bob communicate over a multipath, underspread channel transmitting the zero-mean, unit-variance, complex symbols $s_{\text{A}}[n]$ and $s_{\text{B}}[n]$, respectively. The multipath channel is modeled with L taps, where each tap experiences quasi-static fading. The signal Alice receives (when Jeff is silent) can be expressed as

$$r[n]=\sqrt{\rho_{\text{P}}}\sum_{l=0}^{L-1}h[l]s_{\text{B}}[n-l]+\epsilon[n],\tag{1}$$

where $\epsilon[n]\sim\mathcal{CN}(0,1)$ is normalized independent noise and $h[l]$ is the lth channel tap, normalized so that

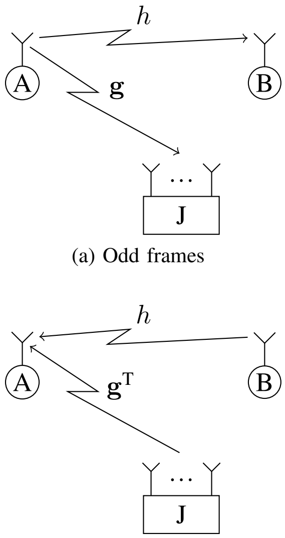
$$\mathbb{E}\left[\sum_{l=0}^{L-1}|h[l]|^2\right]=1.$$

We denote the normalized transmit power used by either of the two terminals by ρ_{P}. The legitimate link further uses a guard interval of $L-1$ samples in the end of each frame. This assumption, apart from being required by TDD operation (to facilitate switching between transmit and receive mode), will have a very small impact on the results—as we assume an underspread channel—and will make the analysis of the jamming problem more tractable.

B. The Jammer

Jeff is located in the vicinity of Alice and Bob, see Fig. 3. During odd frames of the legitimate transmission, a portion of the signal intended for Bob reaches Jeff (Fig. 3a). The signal

[1] As a special case of this, there is the direct mode operation in the TETRA standard, where two terminals communicate device-to-device. This mode is, for example, used in situations where base station coverage is poor or in covert operations [33].



(a) Odd frames

(b) Even frames

Fig. 3. The legitimate channel between the two terminals (A)lice and (B)ob is denoted by h, while the jamming channel between Alice and (J)eff is denoted by $\mathbf{g}$. In odd frames, when Alice is transmitting to Bob, part of the transmitted signal is picked up by Jeff. Jeff uses this signal and exploits channel reciprocity to jam Alice in the subsequent (even) frame.

Jeff receives on antenna m at time instant n is given by

$$y_m[n] \triangleq \sqrt{\rho_{\mathrm{P}}} \sum_{l=0}^{L-1} g_m[l] s_{\mathrm{A}}[n-l] + \eta_m[n], \tag{2}$$

where $g_m[l]$ is the channel from the terminal to Jeff's mth antenna and $\eta_m[n] \sim \mathcal{CN}(0,1)$ is (normalized) independent noise. Just like for the legitimate link, the channel taps are modeled as independent block fading processes. Note that $s_{\mathrm{A}}[n] = 0$ for the last $L-1$ samples in each frame, however, Jeff is unaware of this particular transmission strategy. Hence the introduction of the guard interval constitutes a worst-case scenario for the jammer, since these samples are treated as any other samples in the frame but only contain noise.

Remark: There are two implicit assumptions in this model. First, the coherence time is defined as the minimum of the coherence times of the three considered channels: Alice–Bob, Alice–Jeff and Bob–Jeff. Second, L is an upper bound on the excess delay for the three considered channels, which implies that some taps, in any of the three considered channels, may be zero. Note that L is assumed to be known to the jammer.

Stacking the measurements for each antenna in (2) on top of each other, gives the M-dimensional received vector

$$\begin{aligned} \mathbf{y}[n] &\triangleq [y_1[n], y_2[n], \ldots, y_M[n]]^{\mathrm{T}} \\ &= \sqrt{\rho_{\mathrm{P}}} \sum_{l=0}^{L-1} \mathbf{g}[l] s_{\mathrm{A}}[n-l] + \boldsymbol{\eta}[n], \end{aligned} \tag{3}$$

where

$$\mathbf{g}[l] \triangleq [g_1[l], g_2[l], \ldots, g_M[l]]^{\mathrm{T}}$$

and

$$\boldsymbol{\eta}[n] \triangleq [\eta_1[n], \eta_2[n], \ldots, \eta_M[n]]^{\mathrm{T}}.$$

The noise samples are assumed to be identically distributed, as well as spatially and temporally white.

Based on these received signals, Jeff constructs the $M \times 1$ *jamming signal* $\mathbf{z}[n]$, to be transmitted in the subsequent frame (Fig. 3b). When Jeff transmits this jamming signal with transmit power ρ_{J}, Alice receives

$$\begin{aligned} r[n] \triangleq{}& \sqrt{\rho_{\mathrm{P}}} \sum_{l=0}^{L-1} h[l] s_{\mathrm{B}}[n-l] \\ &+ \sqrt{\rho_{\mathrm{J}}} \sum_{l=0}^{L-1} \mathbf{g}^{\mathrm{T}}[l] \mathbf{z}[n-l] + \epsilon[n]. \end{aligned} \tag{4}$$

Compared to (1), (4) has one extra term, due to the active jammer, namely

$$r_{\mathrm{J}}[n] \triangleq \sqrt{\rho_{\mathrm{J}}} \sum_{l=0}^{L-1} \mathbf{g}^{\mathrm{T}}[l] \mathbf{z}[n-l], \tag{5}$$

called the *received jamming signal*. This received jamming signal is the only thing Jeff can affect in (4). How Jeff constructs the jamming signal is described in detail in Section III-B.

Later, it will be useful to consider the all the received samples in an entire frame. The τ_{F} symbols Alice receives can be written in matrix form as

$$\begin{aligned} \mathbf{r} &\triangleq [r[1], r[2], \ldots, r[\tau_{\mathrm{F}}]]^{\mathrm{T}} \\ &= \sqrt{\rho_{\mathrm{P}}} \mathbf{H}_{\mathrm{F}} \mathbf{s}_{\mathrm{B}} + \sqrt{\rho_{\mathrm{J}}} \mathbf{G}_{\mathrm{F}}^{\mathrm{T}} \mathbf{z} + \boldsymbol{\epsilon}, \end{aligned} \tag{6}$$

where $\mathbf{H}_{\mathrm{F}} \in \mathbb{C}^{\tau_{\mathrm{F}} \times \tau_{\mathrm{F}}}$ is a lower-triangular Toeplitz matrix with first column equal to

$$[h[0], h[1], \ldots, h[L-1], 0, \ldots, 0]^{\mathrm{T}}$$

and $\mathbf{G}_{\mathrm{F}}^{\mathrm{T}} \in \mathbb{C}^{\tau_{\mathrm{F}} \times M\tau_{\mathrm{F}}}$ is a lower-triangular block Toeplitz matrix, with the same structure as $\mathbf{H}_{\mathrm{F}}$, but with $h[l]$ replaced by $\mathbf{g}^{\mathrm{T}}[l]$. Moreover,

$$\mathbf{s}_{\mathrm{B}} \triangleq [s_{\mathrm{B}}[1], \ldots, s_{\mathrm{B}}[\tau_{\mathrm{F}}]]^{\mathrm{T}} \in \mathbb{C}^{\tau_{\mathrm{F}}},$$

$$\mathbf{z} \triangleq \left[\mathbf{z}^{\mathrm{T}}[1], \ldots, \mathbf{z}^{\mathrm{T}}[\tau_{\mathrm{F}}]\right]^{\mathrm{T}} \in \mathbb{C}^{M\tau_{\mathrm{F}}},$$

and

$$\boldsymbol{\epsilon} \triangleq [\epsilon[1], \ldots, \epsilon[\tau_{\mathrm{F}}]]^{\mathrm{T}} \in \mathbb{C}^{\tau_{\mathrm{F}}}.$$

III. Jamming Scheme

This section describes the jamming scheme from Jeff's perspective. Recall that Jeff has no information about the transmitted legitimate signals, so in order to perform the steps described here, Jeff assumes a few things about the legitimate signal: i) The legitimate link uses Gaussian codebooks; ii) The legitimate symbols are uncorrelated. It is important to note that the analysis hereafter does *not* rely on these assumptions being true: the scheme will work when practical codebooks are used and when the symbols are correlated (which they would be in practice). However, if the jammer knows about, for example, what codebooks are used, this can be used to improve the jamming performance [35].

To jam the legitimate link, Jeff first estimates the frame offset, τ_{O}, by analyzing the received signal during N_{F} frames. The idea is to use the covariance matrix in each frame, to see when the statistics of the received signal in (3) changes. This will give the time instance where two frames meet, and thereby the frame offset. From this estimate, denoted

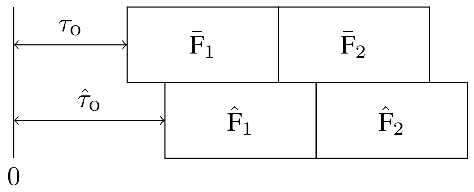


Fig. 4. On top are the two first frames of the legitimate transmission, below are the first two frames of the legitimate transmission according to the jammer's estimate. Because the jammer has to estimate the frame offset $\tau_{\rm O}$, these frames might not overlap perfectly. The error in frame offset estimate results in a contaminated channel estimate as well as missed jamming opportunity.

$\hat{\tau}_{\rm O}$, Jeff defines the *estimate* of the transmission frame as $\hat{\rm F}_k \triangleq {\rm F}_k(\hat{\tau}_{\rm O})$. The relationship between the transmission frame $\bar{\rm F}_k$ and the estimated transmission frame $\hat{\rm F}_k$ is shown in Fig. 4 (for overestimation of $\tau_{\rm O}$).

Once the frame offset has been estimated, the jammer performs a two-step process to disrupt the legitimate link, illustrated in Fig. 3. First, in odd frames, Jeff is silent and collects samples from the transmitting terminal. In the subsequent (even) frame, Jeff transmits a jamming signal, based on the samples received in the previous frame. In other words, Jeff operates in "half-duplex"[2], hence, only one direction in the legitimate communication is targeted. Note that Jeff does not target either of the terminals specifically, but targets the terminal transmitting in odd frames (which by our definition is Alice). There is no direct way for Jeff to distinguish the identities of the two terminals.

The preceding estimation of the frame offset is crucial for this two-step process to work. If the frame offset estimate is inaccurate, $\hat{\rm F}_k$ will contain samples from two different frames, which will contaminate the constructed jamming signal. As an effect, part of the jamming signal will be directed towards the transmitting terminal rather than the receiving one. Moreover, Jeff will spend time jamming when he should be listening, and vice versa.

The covariance matrix of the received signal will differ between frames, as the covariance matrix depends on the realization of the channel in each particular frame. We denote the L-tap channel realization between the transmitting terminal and the jammer in frame $\bar{\rm F}_k$ by

$$\mathbf{G}_k \triangleq [\mathbf{g}_k[0], \mathbf{g}_k[1], \ldots, \mathbf{g}_k[L-1]] \in \mathbb{C}^{M\times L}.$$

For sample $n \in \bar{\rm F}_k$, the received signal at the jammer is

$$\mathbf{y}[n] = \sqrt{\rho_{\rm P}}\mathbf{G}_k\mathbf{s}[n] + \boldsymbol{\eta}[n], \tag{7}$$

where the transmitted symbols

$$\mathbf{s}[n] = \begin{cases} [s_{\rm A}[n], \ldots, s_{\rm A}[n-(L-1)]]^{\rm T}, & \text{odd } k \\ [s_{\rm B}[n], \ldots, s_{\rm B}[n-(L-1)]]^{\rm T}, & \text{even } k \end{cases}$$

are assumed to be uncorrelated[3]. The conditional covariance matrix of the received signal in frame $\bar{\rm F}_k$, given $\mathbf{G}_k$, is

$$\mathbf{Q}_k \triangleq \mathbb{E}\left[\mathbf{y}[n]\mathbf{y}[n]^{\rm H} \middle| \mathbf{G}_k\right] = \rho_{\rm P}\mathbf{G}_k\mathbf{G}_k^{\rm H} + \mathbf{I}_M. \tag{8}$$

It is important to note that we can only write the covariance matrix for a frame $\bar{\rm F}_k = {\rm F}_k(\tau_{\rm O})$, since for any other value of τ, the received signal in frame ${\rm F}_k(\tau)$ originates from two different distributions and hence, is not stationary.

A. Estimating the Frame Offset

To estimate the frame offset, Jeff considers multiple a priori equiprobable hypotheses:

$$\mathcal{H}_\tau : \tau = \tau_{\rm O}.$$

That is, under $\mathcal{H}_\tau$, τ is the true frame offset and thus $\mathbf{Q}_k$ is the covariance matrix of the received signal in ${\rm F}_k(\tau)$. The optimal decision rule, that minimizes the probability of error, is to choose the frame offset estimate corresponding to the hypothesis that maximizes the posterior probability $\Pr(\mathcal{H}_\tau|\mathbf{y})$ [36, Section 3.8].

The posterior probability is intractable (owing to the statistical dependence between subsequent samples[4] and the guard interval); instead Jeff uses

$$\prod_{k=1}^{N_{\rm F}}\prod_{i=1}^{\tau_{\rm F}} \Pr(\mathcal{H}_\tau|\mathbf{y}_k^i), \tag{9}$$

which would be the actual posterior probability, if all samples were independent. Here, $\mathbf{y}_k^i$ is the ith sample in frame ${\rm F}_k(\tau)$. Maximizing (9) with respect to τ is equivalent to minimizing

$$l(\tau) \triangleq -\sum_{k=1}^{N_{\rm F}}\sum_{i=1}^{\tau_{\rm F}} \log\left(f_{\mathbf{y}_k^i|\mathcal{H}_\tau}(\mathbf{y}_k^i|\mathcal{H}_\tau)\right)$$

with respect to τ, where $f_{\mathbf{y}_k^i|\mathcal{H}_\tau}(\cdot)$ is the probability density function of $\mathbf{y}_k^i$ under $\mathcal{H}_\tau$. For a fixed channel $\mathbf{G}_k$, under $\mathcal{H}_\tau$, the received signal in frame ${\rm F}_k(\tau)$ has a complex Gaussian distribution with zero mean and covariance $\mathbf{Q}_k$, i.e.,

$$f_{\mathbf{y}_k^i|\mathcal{H}_\tau}(\mathbf{y}|\mathcal{H}_\tau) \triangleq \frac{1}{(2\pi)^M|\mathbf{Q}_k|}\exp\left(-\mathbf{y}^{\rm H}\mathbf{Q}_k^{-1}\mathbf{y}\right).$$

This gives

$$\begin{aligned} l(\tau) = &\sum_{k=1}^{N_{\rm F}}\sum_{i=1}^{\tau_{\rm F}}\left(\log|\mathbf{Q}_k| + \left(\mathbf{y}_k^i\right)^{\rm H}\mathbf{Q}_k^{-1}\mathbf{y}_k^i\right) \\ &+ \text{constant}, \end{aligned} \tag{10}$$

which is a function of the true covariance matrices $\{\mathbf{Q}_k\}$. These matrices are unavailable to the jammer, and hence, have to be estimated. The maximum likelihood (ML) estimate of $\mathbf{Q}_k$ under $\mathcal{H}_\tau$ is denoted by $\hat{\mathbf{Q}}_k(\tau)$ and is given by the following theorem, [37, Theorem 2]:

Theorem 1. *Let* $\mathbf{S}$ *be the unbiased sample covariance matrix estimate of* $\mathbf{Q}$ *and let the multiplicities of the eigenvalues of* $\mathbf{Q}$*, denoted* $q_1, \ldots, q_r$*,* $(\sum_i q_i = M)$ *be known.* $\mathbf{S}$ *is by definition a positive semi-definite matrix, so it can be written in terms of its eigenvalue decomposition as* $\mathbf{U}\boldsymbol{\Lambda}_{\rm S}\mathbf{U}^H$*, where* $\mathbf{U}$ *is a unitary*

[2] Technically, the jammer could listen and transmit at the same time ("full-duplex"), however this is a much more challenging task.

[3] If the symbols are correlated, for example if the legitimate link employs waterfilling, this only has a minor impact on jamming performance.

[4] The samples can be "made independent" if the jammer only considers every Lth sample. This will reduce the computational load, at the cost of jamming performance.

matrix and $\mathbf{\Lambda}_{\mathrm{S}}$ is a diagonal matrix with $\lambda_1^{\mathrm{S}} > \cdots > \lambda_M^{\mathrm{S}}$ on the diagonal [5]*. The maximum likelihood estimate of $\mathbf{Q}$ is*

$$\mathbf{U}\mathbf{\Lambda}_{\mathrm{ML}}\mathbf{U}^H,$$

where $\mathbf{\Lambda}_{\mathrm{ML}}$ is a diagonal matrix with diagonal elements

$$\underbrace{\lambda_1^{\mathrm{ML}} = \cdots = \lambda_1^{\mathrm{ML}}}_{q_1} > \underbrace{\lambda_2^{\mathrm{ML}} = \cdots = \lambda_2^{\mathrm{ML}}}_{q_2} > \dots$$
$$> \underbrace{\lambda_r^{\mathrm{ML}} = \cdots = \lambda_r^{\mathrm{ML}}}_{q_r} \geq 0.$$

Each diagonal element is the ML *estimate of the corresponding eigenvalue, computed as*

$$\lambda_k^{\mathrm{ML}} \triangleq \frac{\tau_{\mathrm{F}} - 1}{\tau_{\mathrm{F}} q_k} \sum_{i \in \mathcal{I}_k} \lambda_i^{\mathrm{S}},$$

where $\mathcal{I}_k \triangleq \left\{ \sum_{i=1}^{k-1} q_i + 1, \dots, \sum_{i=1}^{k} q_i \right\}$.

Replacing the true covariance matrices in (10) with their ML estimates results in

$$\hat{l}(\tau) \triangleq \sum_{k=1}^{N_{\mathrm{F}}} \sum_{i=1}^{\tau_{\mathrm{F}}} \left(\log \left| \hat{\mathbf{Q}}_k(\tau) \right| + \left(\mathbf{y}_k^i\right)^{\mathrm{H}} \hat{\mathbf{Q}}_k^{-1}(\tau) \mathbf{y}_k^i \right) + \text{constant}, \tag{11}$$

and the frame offset estimate is finally given by

$$\hat{\tau}_{\mathrm{O}} \triangleq \underset{\tau \in \{0,1,\dots,\tau_{\mathrm{F}}-1\}}{\operatorname{argmin}} \ \hat{l}(\tau). \tag{12}$$

Note that $l(\cdot)$ in (10) is not a log-likelihood function in general, since there is a statistical dependence between the received samples. However, in the flat fading case, when $L = 1$, the posterior probability $\Pr(\mathcal{H}_\tau|\mathbf{y})$ equals the expression in (9) and hence, in this case, (10) is a log-likelihood function. In addition, we only need to consider $\tau \in \{0, 1, \dots, \tau_{\mathrm{F}} - 1\}$ in (12) since $\hat{l}(\tau)$ is (almost) periodic with period τ_{F}. The periodicity arises because Jeff only seeks to find at what time index the statistics of the channel change.

B. Choosing the Jamming Signal

Once Jeff has an estimate of the frame offset, he knows when to listen and when to transmit: starting at sample $\hat{\tau}_{\mathrm{O}}$ i) listen to τ_{F} samples; ii) jam for τ_{F} samples; iii) repeat. Jeff can then construct the jamming signal in each frame, by using the samples received in the previous frame. We first show how to optimize the jamming signal in the case when Jeff knows the L-tap channel $\mathbf{G}$ perfectly, and next how this optimization can be done in practice, when Jeff has no a priori knowledge of $\mathbf{G}$. In this section, everything takes place in a single frame, hence, we omit the frame index for improved readability.

In order to inflict the maximum amount of damage to the legitimate transmission, the received jamming signal, (5), should be Gaussian and its expected power should be maximized. Looking at an entire frame, (6), we see that in order to maximize the expected power of the received jamming signal, for a fixed $\mathbf{G}_{\mathrm{F}}$, Jeff should maximize

$$\left|\left|\mathbf{G}_{\mathrm{F}}^{\mathrm{T}}\mathbf{z}\right|\right|_2^2 = \mathbf{z}^{\mathrm{H}}\mathbf{G}_{\mathrm{F}}^{*}\mathbf{G}_{\mathrm{F}}^{\mathrm{T}}\mathbf{z}$$

subject to a power constraint on $\mathbf{z}$. The solution to this problem is to pick $\mathbf{z}$ to be the dominant eigenvector of $\mathbf{G}_{\mathrm{F}}^{*}\mathbf{G}_{\mathrm{F}}^{\mathrm{T}} \in \mathbb{C}^{M\tau_{\mathrm{F}} \times M\tau_{\mathrm{F}}}$. However, there are a few concerns with this method: Even for a moderate number of antennas and a short frame, the matrix dimensions could be in the order of 10000×10000, so the sheer size of this matrix may prove problematic for Jeff. On top of storing this matrix, Jeff would have to calculate the dominant eigenvector.[6]

Instead, Jeff considers a “typical” received jamming sample $r_{\mathrm{J}}[n]$ (cf. (5)), where n is such that Jeff can ignore any edge effects. Jeff then solves the following maximization problem:

$$\underset{\{\mathbf{v}[k]\}}{\text{maximize}} \ \mathbb{E}\left[\left| \sum_{l=0}^{L-1} \mathbf{g}^{\mathrm{T}}[l]\mathbf{z}[n-l] \right|^2 \middle| \mathbf{G} \right], \tag{13a}$$

subject to

$$\mathbf{z}[n] = \sum_{k=0}^{K-1} \mathbf{v}[k] w[n-k],$$
$$\sum_{m=1}^{M} \sum_{k=0}^{K-1} |v_m[k]|^2 \leq 1. \tag{13b}$$

$w[n]$ in (13b) is zero mean complex Gaussian white noise with unit variance and

$$\mathbf{v}[k] \triangleq [v_1[k], \dots, v_M[k]]^{\mathrm{T}} \in \mathbb{C}^M, \ k = 0, \dots, K-1$$

decides how Jeff weighs the noise and is referred to as the beamforming vector associated with the kth filter tap.[7]

Interpreting the problem stated in (13), Jeff aims to construct a jamming signal $\mathbf{z}$ that maximizes the expected received jamming power of a typical sample. Jeff considers jamming signals constructed by filtering Gaussian white noise, and chooses the coefficients of the filter (the beamforming vectors) to maximize the objective function (13a). The last constraint ensures that $\mathbb{E}\left[\mathbf{z}^{\mathrm{H}}[n]\mathbf{z}[n]\right] \leq 1$, so the average transmit power is less than ρ_{J}. The solution to (13) gives the optimal jamming signal generated through a K-order moving average process (cf. (13b)), but does not guarantee that this is the optimal construction overall. However, maximizing the received jamming signal for a typical sample is intuitively reasonable and letting $K > 1$ in (13b) forces the jammer to take the effects of the frequency-selective channel into account.

Note that this strategy is not optimal for the $L-1$ samples in the beginning of the frame, since these have a different structure. For example, the first received sample is only affected by the first tap, $\mathbf{g}[0]$, and thus to maximize the received jamming power of the first sample, Jeff should choose the jamming signal $\mathbf{z}[0] = \mathbf{g}^*[0]$. Doing this would require Jeff to estimate $\mathbf{g}[0]$, which is difficult since the channel taps are “tangled”,

[5] Note that this is not restrictive, as the eigenvalues of the sample covariance matrix are different with probability 1, whenever $\tau_{\mathrm{F}} \geq M$.

[6] When only one or a few eigenvalues/eigenvectors are required, computing the entire eigenvalue decomposition is unnecessary, and the power method is more efficient, see for example [38, Section 4.5.1].

[7] The number of filter taps, K, is not necessarily equal to the number of channel taps, L. See Section V-A for a brief discussion.

and are difficult to untangle without any further knowledge of the transmitted symbols. Furthermore, there is no guarantee that this choice of jamming signal will be a good fit when considering the subsequent channel taps.

The optimal beamforming vectors for the problem in (13) are given by the following theorem:

Theorem 2. *Let*

$$\bar{\mathbf{G}} \triangleq (\mathbf{I}_K \otimes \mathbf{G}^T)^H \boldsymbol{\Psi} (\mathbf{I}_K \otimes \mathbf{G}^T) \in \mathbb{C}^{MK \times MK}$$

where $\boldsymbol{\Psi}$ *is a* $KL \times KL$ *matrix such that*

$$\boldsymbol{\Psi}_{ij} = \begin{cases} 1, & \text{if } n_i + m_i = n_j + m_j, \\ 0, & \text{otherwise,} \end{cases}$$

where $m_i \triangleq \lceil \frac{i}{L} \rceil$ *and* $n_i \triangleq (i - 1 \mod L) + 1$.[8] *Furthermore, let* $\mathbf{v} \in \mathbb{C}^{MK} \triangleq \left[\mathbf{v}^T[0], \ldots, \mathbf{v}^T[K-1]\right]^T$. *The solution to problem (13) is to choose* $\mathbf{v}$ *as the dominant eigenvector of* $\bar{\mathbf{G}}$.

Proof. The proof is given in Appendix A. □

The matrix $\bar{\mathbf{G}}$ in Theorem 2 is a $KM \times KM$ block Toeplitz, Hermitian matrix:

$$\bar{\mathbf{G}} = \begin{pmatrix} \mathbf{B}_0 & \mathbf{B}_1 & \cdots \\ \mathbf{B}_1^{\mathrm{H}} & \mathbf{B}_0 & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

where each block $\mathbf{B}_k$ is an $M \times M$ (Hermitian) matrix comprising a sum of outer products of different combinations of columns of $\mathbf{G}$. More specifically

$$\mathbf{B}_k \triangleq \sum_{i=k}^{L-1} \mathbf{g}^*[i]\mathbf{g}^{\mathrm{T}}[i-k]$$

corresponds to the autocorrelation of the received signal with lag k, and $\mathbf{B}_k = \mathbf{0}_M$ (the $M \times M$ zero matrix) for $k > L - 1$. In particular, the blocks on the diagonal are the autocorrelation with lag 0, i.e.,

$$\mathbf{B}_0 = \mathbf{G}^*\mathbf{G}^{\mathrm{T}} = \sum_{i=0}^{L-1} \mathbf{g}^*[i]\mathbf{g}^{\mathrm{T}}[i].$$

However, Jeff has no knowledge of the channel, $\mathbf{G}$, so to be able to find the weights $\{v_m[l]\}$, he needs to estimate $\bar{\mathbf{G}}$. Also, as previously mentioned, Jeff cannot effectively estimate the individual channel taps. Instead, Jeff estimates each of the L blocks of size $M \times M$ by using the biased sample covariance estimate

$$\hat{\mathbf{B}}_k \triangleq \frac{1}{\tau_{\mathrm{F}} - k}\mathbf{Y}\mathbf{Y}^{\mathrm{H}}[k], \tag{14}$$

where

$$\mathbf{Y} \triangleq [\mathbf{y}^1, \mathbf{y}^2, \ldots, \mathbf{y}^{\tau_{\mathrm{F}}}]$$

and

$$\mathbf{Y}[k] \triangleq [\underbrace{\mathbf{0}, \ldots, \mathbf{0}}_{k \text{ zero vectors}}, \mathbf{y}^{k+1}, \mathbf{y}^{k+2}, \ldots, \mathbf{y}^{\tau_{\mathrm{F}}-k}]$$

are the $M \times \tau_{\mathrm{F}}$ received symbol matrix and the received symbol matrix with lag k, respectively.

For (14) to be a reasonably good estimate[9], we must have $\tau_{\mathrm{F}} \gg L$, which is implied in the underspread channel assumption. Worth noting is that for the diagonal blocks, (14) actually estimates $\mathbf{B}_0 + \mathbf{I}$, effectively giving the estimate of $\bar{\mathbf{G}} + \mathbf{I}$. However, for the purpose of finding the dominant eigenvector, estimating $\bar{\mathbf{G}} + \mathbf{I}$ or $\bar{\mathbf{G}}$ makes no difference since their eigenvectors are identical.

C. Locating the Jammer

One problem the jammer faces is to remain undetected during transmission. A jammer that is easily located will quickly be found and terminated. Adding more antennas increases the jammer's ability to beamform which makes the jammer more difficult to locate, as we will exemplify below.

Consider two single-antenna terminals placed at the same distance from the jammer. The first terminal is the jammer's target, and the second terminal aims to detect whether or not a jammer is present by comparing the received signal power to a threshold. This power detection can be seen as a first step in locating the jammer. The detector moves in a circle around the jammer so that the large-scale fading stays constant over the measurements. Let $\mathbf{g}_{\mathrm{T}}^{\mathrm{H}}$ and $\mathbf{g}_{\mathrm{D}}^{\mathrm{H}}$ denote the M-dimensional channels from the jammer to the target and the detector, respectively. In this discussion, for the sake of argument, the jammer is assumed to know $\mathbf{g}_{\mathrm{T}}$ perfectly. We assume that the jammer transmits unit variance symbols aimed at the target, using the beamforming vector $\mathbf{b} \triangleq \mathbf{g}_{\mathrm{T}}/M$.

1) Line of Sight: In line of sight the two channel vectors are steering vectors satisfying

$$\mathbf{g}_{\mathrm{T}}^{\mathrm{H}}\mathbf{g}_{\mathrm{T}} = \mathbf{g}_{\mathrm{D}}^{\mathrm{H}}\mathbf{g}_{\mathrm{D}} = M$$

that only depend on the azimuth angle to the jammer. Here we assume a uniform linear array with antenna elements spaced a half wavelength apart at the jammer. The received jamming power at the detector, $|\mathbf{g}_{\mathrm{D}}^{\mathrm{H}}\mathbf{b}|^2$, when the target is located in the direction of $\pi/6$, is showed in Fig. 5. We see that for an omnidirectional ($M = 1$) jammer, the received power is the same in all directions, making the jammer relatively easy to locate. For a jammer with more antennas, the received jamming power is always less in any other direction than that of the target. The more antennas the jammer has, the more difficult the jammer is to locate. This is so because, with half-wavelength spaced antennas, the beamwidth scales proportionally to $1/M$. For antenna spacings larger than half a wavelength, there will be grating lobes [34]; however, the size of the total angular sector "covered" by the main beam and its associated grating lobes substantially scales proportionally to $1/M$. Note that the total transmit power is $1/M$, so a large array uses less transmit power than a smaller one but still manages to transfer the same amount of jamming power to the target.

2) Rayleigh Fading: In independent Rayleigh fading the channels are random. In this illustrative example, we assume the channels are flat fading and

$$\mathbf{g}_{\mathrm{T}}, \mathbf{g}_{\mathrm{D}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_M).$$

The expected received jamming power at the detector is

$$\mathbb{E}\left[|\mathbf{g}_{\mathrm{D}}^{\mathrm{H}}\mathbf{b}|^2\right] = \frac{1}{M^2}\mathbb{E}\left[|\mathbf{g}_{\mathrm{D}}^{\mathrm{H}}\mathbf{g}_{\mathrm{T}}|^2\right] = \frac{1}{M}$$

[8] $\lceil x \rceil$ is the smallest integer that is larger than or equal to x.

[9] One could just as well choose the unbiased estimator for $\mathbf{B}_k$ (where the denominator would be $\tau_{\mathrm{F}} - k - 1$) instead of the biased estimate chosen in (14) without any noticeable effects for the analyzed scenarios.

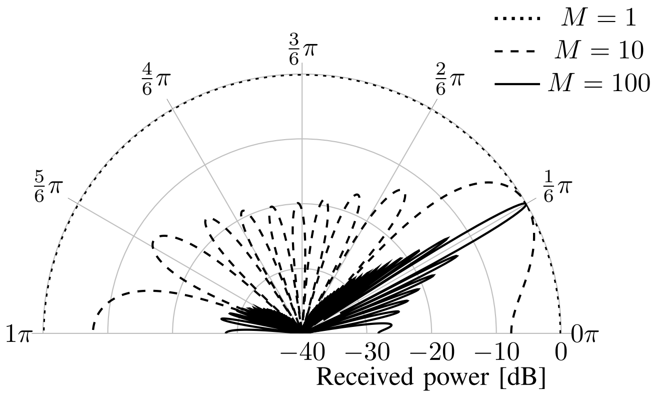


Fig. 5. The received jamming power at terminal with line-of-sight and perfect channel knowledge at the jammer. The target terminal is located in the direction of $\pi/6$ radians, and the plot shows the received jamming power for a terminal at any point on the semi-circle. For omnidirectional transmission, the received signal strength is constant. With beamforming, the jammer can scale down the output power with $1/M$ while keeping the received jamming power at the target constant. With many antennas the beam is very narrow, making detection of the jammer more difficult for any other direction than that of the target.

while the expected received jamming power at the target is

$$\mathbb{E}\left[|\mathbf{g}_{\mathrm{T}}^{\mathrm{H}}\mathbf{b}|^2\right] = \frac{1}{M^2}\mathbb{E}\left[|\mathbf{g}_{\mathrm{T}}^{\mathrm{H}}\mathbf{g}_{\mathrm{T}}|^2\right] = 1 + \frac{1}{M}.$$

That is, on average the target receives (approximately) M times more power than the detector.

D. Extensions and Defensive Countermeasures

The assumed system model involves single-antenna terminals that do not actively try to counteract the jammer; the jamming signal is just treated as additional noise. In this section, we briefly discuss how the current model can be extended, what the terminals can do to mitigate jamming, and how these countermeasures affect the jamming procedure in Section III.

1) Multi-antenna terminals: For the entirety of this discussion, we let the legitimate terminals have multiple antennas, but restrict ourselves to the frequency-flat case. We also omit the frame index and denote each new variable with $\tilde{(\cdot)}$, to avoid confusion with its frequency-selective counterpart. Note that [16] analyzes the optimal jamming signal for this exact case when perfect CSI is assumed at both the jammer and the legitimate link. Thus, we focus on how multiple antennas at the terminals affects the jamming procedure in Section III, which assumes no a priori CSI.

The targeted terminal (T) is equipped with M_{T} antennas and the unaffected terminal (U) is equipped with M_{U} antennas. In the general case, the received symbol vector at the jammer can be written as

$$\tilde{\mathbf{y}} \triangleq \tilde{\mathbf{G}}\tilde{\mathbf{s}} + \tilde{\boldsymbol{\eta}}, \tag{15}$$

where $\tilde{\mathbf{G}}$ is the channel from the terminal, $\tilde{\mathbf{s}}$ is the transmitted symbol vector and $\tilde{\boldsymbol{\eta}}$ represents noise. Specifically, when T transmits,

$$\tilde{\mathbf{s}} = \tilde{\mathbf{s}}_{\mathrm{T}} \in \mathbb{C}^{M_{\mathrm{T}}} \text{ and } \tilde{\mathbf{G}} = \tilde{\mathbf{G}}_{\mathrm{T}} \in \mathbb{C}^{M \times M_{\mathrm{T}}},$$

where $\tilde{\mathbf{s}}_{\mathrm{T}}$ is the transmitted vector and $\tilde{\mathbf{G}}_{\mathrm{T}}$ is the channel to the jammer. When U transmits,

$$\tilde{\mathbf{s}} = \tilde{\mathbf{s}}_{\mathrm{U}} \in \mathbb{C}^{M_{\mathrm{U}}} \text{ and } \tilde{\mathbf{G}} = \tilde{\mathbf{G}}_{\mathrm{U}} \in \mathbb{C}^{M \times M_{\mathrm{U}}},$$

where $\tilde{\mathbf{s}}_{\mathrm{U}}$ is the transmitted vector and $\tilde{\mathbf{G}}_{\mathrm{U}}$ is the channel to the jammer. The received signal at T is

$$\tilde{\mathbf{r}} \triangleq \tilde{\mathbf{H}}\tilde{\mathbf{s}}_{\mathrm{U}} + \tilde{\mathbf{G}}_{\mathrm{T}}^{\mathrm{T}}\tilde{\mathbf{z}} + \tilde{\boldsymbol{\epsilon}}, \tag{16}$$

where $\tilde{\mathbf{H}} \in \mathbb{C}^{M_{\mathrm{T}} \times M_{\mathrm{U}}}$ denotes the legitimate channel between the U and T, $\tilde{\mathbf{z}}$ denotes the jamming signal and $\tilde{\boldsymbol{\epsilon}}$ denotes the noise.

First, consider the case when the transmit antennas do not cooperate, i.e., no beamforming is used and all antennas transmit independent streams of data. When U transmits, this means

$$\tilde{\mathbf{s}}_{\mathrm{U}} = [s_1, \ldots, s_{M_{\mathrm{U}}}]^{\mathrm{T}},\ \mathbb{E}\left[\tilde{\mathbf{s}}_{\mathrm{U}}\tilde{\mathbf{s}}_{\mathrm{U}}^{\mathrm{H}}\right] = \mathbf{I}_{M_{\mathrm{U}}}.$$

The received signal at the jammer in (15) then has the same form as (7), only the columns of the channel matrix represents different transmit antennas in (15) and different channel taps in (7). Since the conditional covariance matrix of the received signal, (8), is the only thing used by the jammer when estimating the frame offset the case of multiple non-cooperative transmit antennas can be treated in the same framework as multiple channel taps (Section III-A).

Second, consider the received signal at the targeted terminal (16). Forming the jamming signal $\tilde{\mathbf{z}}$ that maximizes the (conditional) expected received jamming signal

$$\mathbb{E}\left[\|\tilde{\mathbf{G}}_{\mathrm{T}}^{\mathrm{T}}\tilde{\mathbf{z}}\|^2 \middle| \tilde{\mathbf{G}}\right] = \mathbb{E}\left[\tilde{\mathbf{z}}^{\mathrm{H}}\tilde{\mathbf{G}}_{\mathrm{T}}^{*}\tilde{\mathbf{G}}_{\mathrm{T}}^{\mathrm{T}}\tilde{\mathbf{z}} \middle| \tilde{\mathbf{G}}\right]$$

follows the same principles as the optimization in [32] or the discussion in the beginning of Section III-B. Conditioned on $\tilde{\mathbf{G}}$, the answer is to choose $\tilde{\mathbf{z}}$ to be the dominant eigenvector of $\tilde{\mathbf{G}}_{\mathrm{T}}^{*}\tilde{\mathbf{G}}_{\mathrm{T}}^{\mathrm{T}}$. As an alternative, if the jammer suspects or knows that the target may use receive beamforming, the jammer could construct its jamming signal by waterfilling over the eigenvalues of $\tilde{\mathbf{G}}_{\mathrm{T}}^{*}\tilde{\mathbf{G}}_{\mathrm{T}}^{\mathrm{T}}$. This waterfilling will make the received jamming power smaller than if choosing the dominant eigenvector, but will spread the signal in several directions, making it more difficult to negate. The optimal reception strategy for the target in this case (for the special case of perfect CSI) is described in [16].

Finally, consider the case when the legitimate terminals use transmit beamforming. The transmit/receive beamforming vectors for obtaining the maximum signal-to-jamming-plus-noise ratio (assuming perfect CSI) are described in [16]. The transmit beamforming causes two major problems to the jammer in Section III. First, since the legitimate signal is directed to the other terminal, less signal power reaches the jammer, making the frame offset estimation more difficult. Second, this beamforming will obscure the jammer's perception of the channel to the target. To see this, consider transmitted legitimate signals of the form $\tilde{\mathbf{s}}_{\mathrm{T}} = \mathbf{t}s$, where $\mathbf{t}$ is the beamforming vector and s is a symbol. The effective channel from the target to the jammer is then $\tilde{\mathbf{G}}_{\mathrm{T}}\mathbf{t}$, very different from the channel to the target $\tilde{\mathbf{G}}_{\mathrm{T}}^{\mathrm{T}}$. This severely complicates the construction of the jamming signal and it is not clear if effective jamming is possible in this case.

Exactly how the jammer should face the problem with multiple antennas at the terminal in a frequency-selective system is not clear. What is clear is that multiple-antenna terminals make the jamming procedure more challenging. The extra antennas can be seen as a countermeasure, even when they do not cooperate, because of the added spatial diversity: no matter what jamming scheme Jeff employs, the received jamming power will differ between the receiving antennas. Typically, transmitting in the direction of the dominant eigenvector of $\tilde{\mathbf{G}}_{\mathrm{T}}^{*}\tilde{\mathbf{G}}_{\mathrm{T}}^{\mathrm{T}}$ focuses the jamming signal on fewer antennas than waterfilling over the eigenvalues $\tilde{\mathbf{G}}_{\mathrm{T}}^{*}\tilde{\mathbf{G}}_{\mathrm{T}}^{\mathrm{T}}$ does.

2) Frequency Hopping: If the legitimate link uses frequency hopping, it can quickly switch the frequency band used for transmission in hope to avoid the frequency band that the jammer is operating in. Assuming the same frequency band is used during at least one coherence interval, the jammer presented in Section III, with a small add-on, could deal with this. However, it is not clear what the *optimal* course of action would be and the optimal choice may also depend on what prior knowledge is available at the jammer. The simplest alternative would be to try to detect what frequency band the legitimate link is using. Once the band is found, the procedure would be the one presented in Section III. To detect what band the legitimate link is using, the jammer could measure the strength of the received signal in each band, and through a hypothesis test decide if a signal is present or not. The only difference to the jammer presented here would then be to take the probability of erroneous detection of the frequency band into account.

IV. Evaluating the Jammer Performance

How well the jammer performs depends partly on its ability to estimate the frame offset, and partly on the construction of the beamforming vectors. Note that a reliable estimate of the frame offset is imperative to choose the beamforming vectors in a good way. If the frame offset estimate is poor, the beamforming vectors will be contaminated by the channel to the other terminal. Additionally, the frame offset estimate is also crucial to jam at the correct time.

A. Performance Metric

To derive a performance metric, consider Alice's received symbols in one frame (cf. (6)):

$$\mathbf{r} = \sqrt{\rho_{\mathrm{P}}}\mathbf{H}_{\mathrm{F}}\mathbf{s}_{\mathrm{B}} + \sqrt{\rho_{\mathrm{J}}}\mathbf{G}_{\mathrm{F}}^{\mathrm{T}}\mathbf{z} + \boldsymbol{\epsilon} = \sqrt{\rho_{\mathrm{P}}}\mathbf{H}_{\mathrm{F}}\mathbf{s}_{\mathrm{B}} + \boldsymbol{\epsilon}_{\text{eff}},$$

where

$$\boldsymbol{\epsilon}_{\text{eff}} \triangleq \sqrt{\rho_{\mathrm{J}}}\mathbf{G}_{\mathrm{F}}^{\mathrm{T}}\mathbf{z} + \boldsymbol{\epsilon}$$

represents *effective* noise, with zero mean and covariance $\mathbf{R}_{\boldsymbol{\epsilon}_{\text{eff}}}$. This covariance matrix varies depending on the transmitted jamming signal $\mathbf{z}$, which is independent of the legitimate channel $\mathbf{H}_{\mathrm{F}}$ (see Section IV-B). By assuming perfect knowledge of $\mathbf{H}_{\mathrm{F}}$ at the legitimate receiver and treating the effective noise as Gaussian with covariance matrix $\mathbf{R}_{\boldsymbol{\epsilon}_{\text{eff}}}$, a lower bound on the legitimate link ergodic capacity is [39]

$$C \geq C_{\mathrm{J}} \triangleq \mathbb{E}\left[\log_2 \det\left(\mathbf{I} + \rho_{\mathrm{P}}\mathbf{R}_{\boldsymbol{\epsilon}_{\text{eff}}}^{-1}\mathbf{H}_{\mathrm{F}}\mathbf{H}_{\mathrm{F}}^{\mathrm{H}}\right)\right]/\tau_{\mathrm{F}}, \tag{17}$$

measured in bits per channel use (bpcu). When Jeff does not transmit ($\rho_{\mathrm{J}} = 0$), the corresponding lower bound on the legitimate link's ergodic capacity is

$$C \geq C_{\mathrm{P}} \triangleq \mathbb{E}\left[\log_2 \det\left(\mathbf{I} + \rho_{\mathrm{P}}\mathbf{H}_{\mathrm{F}}\mathbf{H}_{\mathrm{F}}^{\mathrm{H}}\right)\right]/\tau_{\mathrm{F}}. \tag{18}$$

Tighter bounds on the ergodic capacity for the legitimate link than (17) and (18) can be obtained if we let the terminals use waterfilling over the eigenvalues of $\mathbf{H}_{\mathrm{F}}\mathbf{H}_{\mathrm{F}}^{\mathrm{H}}$. However, when Jeff is silent, using waterfilling brings no significant gains over uniform power allocation, if the SNR is reasonably high. In addition, when Jeff is active the bounds are already quite conservative in measuring Jeff's performance as perfect CSI at the terminals is difficult to obtain in this case.

The absolute error of the frame timing estimate is $|\tau_{\mathrm{O}} - \hat{\tau}_{\mathrm{O}}|$. We denote the *average* absolute error in the frame timing estimation in number of samples by τ_{ϵ}. Based on this error, and the two bounds above, we choose the performance metric as

$$C_{\text{SE}} \triangleq \frac{\tau_{\mathrm{F}} - \tau_{\epsilon}}{\tau_{\mathrm{F}}}C_{\mathrm{J}} + \frac{\tau_{\epsilon}}{\tau_{\mathrm{F}}}C_{\mathrm{P}},$$

and call C_{SE} the legitimate link spectral efficiency (SE). Here, $\frac{\tau_{\mathrm{F}} - \tau_{\epsilon}}{\tau_{\mathrm{F}}}$ and $\frac{\tau_{\epsilon}}{\tau_{\mathrm{F}}}$ are the fractions of time when Jeff beamforms (and listens) to the correct and incorrect terminal, respectively. Note that $C_{\mathrm{P}} \geq C_{\mathrm{J}}$, so $C_{\mathrm{P}} \geq C_{\text{SE}}$.

B. Jamming Schemes

To evaluate the performance of the proposed jammer, we compare the presented scheme to a number of alternative jammers. For convenience, each jammer is associated with an abbreviation written in small caps (e.g. PROP). We compare the following jamming schemes:

- Proposed jammer (PROP): The jammer presented in Section III.
- Full genie (F-GENIE): A genie-aided version of PROP where the frame offset τ_{O} and the channel $\mathbf{G}$ are known.
- Time genie (T-GENIE): A genie-aided version of PROP where the frame offset τ_{O} is known.
- Frequency flat jammer (FLAT): A version of PROP where the frequency selectivity of the channel is ignored. This jammer was considered in [32].
- Time-reverse and conjugate (TRC): A low-complexity jammer where each antenna time-reverses, conjugates and transmits the received signal in the previous frame. The produced jamming signal can be written as

  $$\mathbf{z} = \mathbf{G}_{\mathrm{F}}^{*}\bar{\mathbf{s}}_{\mathrm{A}}^{*} + \boldsymbol{\eta}^{*},$$

  where $\bar{\mathbf{s}}_{\mathrm{A}}$ is the legitimate transmitted vector time-reversed (i.e. the first $L-1$ symbols of $\bar{\mathbf{s}}_{\mathrm{A}}$ are zero).
- Omnidirectional barrage jammer (OMNI): A jammer with a single antenna continuously transmitting white noise. The transmitted jamming signal is chosen randomly from a circular symmetric Gaussian distribution:

  $$z[n] \sim \mathcal{CN}\left(0, 1\right),$$

  independently for each n.

The two genie-aided jammers will give upper bounds on jamming performance. The difference in performance between

F-GENIE and T-GENIE is solely due to the difficulty to construct the jamming vectors, whereas the difference in performance between T-GENIE and PROP comes from the error in estimating the frame offset (which in turn affects the jamming vectors). FLAT and PROP will perform equally in the flat fading case, but we expect PROP to outperform FLAT when $L > 1$, as FLAT does not take the temporal correlations of the received signals into account. Worth noting is that OMNI is the only scheme that can ignore the frame offset estimation, and that TRC and OMNI are the only schemes which is distributed in the sense that no cooperation between antennas is needed when constructing the jamming signal.

C. *Effects of Assumptions*

Section I stated that the jammer has three key parameters given, namely the length of a frame, the number of channel taps, and the carrier frequency of the legitimate link. The consequences of knowing these parameters a priori, and how the jammer could estimate these are briefly discussed here. The development of algorithms for the actual estimation of these parameters has to be relegated to future work.

Knowing the frame length τ_F makes the frame offset easier to estimate, since we only have to consider the time *location* of the transmission frame, and not the *duration* of it. However, one could just as well include the different frame lengths τ_F in the search when finding the frame offset. This would considerably increase the computational complexity of the jammer, but the principle of finding the correct τ_F and τ_O would be the same as in Section III-A.

Knowing the upper-bound on the number of channel taps, L, will first and foremost help the jammer in the ML estimation of the covariance matrix, since the multiplicities of all eigenvalues must be known to obtain the ML estimate. Second, the jammer chooses the filter length K, based on the number of channel taps L (see Section V-A). One possible way of estimating the channel taps would be to perform an order estimation, similar to what is done in [40], or to estimate the delay spread of the channel as in [41]. One would then have to take the cost of over- and underestimating L into account. Initial simulations, not included here, show that the cost of overestimating L is mostly computational and only reduces the jamming performance slightly.

We assume that the jammer is perfectly synchronized in frequency relative to the legitimate link, to make the problem more tractable. In practice, the jammer would have to estimate the carrier frequency of the legitimate link in order to jam efficiently. This should not be a big problem, however, since exact frequency synchronization is not required, as the jammer does not have to decode any symbols. What is needed is for the jammer to be approximately synchronized to the extent that the channel to the target does not change significantly over the duration of a frame. Another effect of bad frequency synchronization is if the jammer wastes power by transmitting outside of the band of the legitimate link. But even very coarse synchronization will make this a non-problem. All in all, the performance of the jammer might change somewhat, but the conclusions will not change noticeably, even if the jammer has to estimate the legitimate carrier frequency.

TABLE I
THE FOUR DIFFERENT SCENARIOS STUDIED IN DETAIL.

	LLA $= 23$ dB	LLA $= 26.5$ dB
$L = 1$	—⊖— SCEN 1	- ⊖- SCEN 2
$L = 5$	—⊟— SCEN 3	- ⊟- SCEN 4

V. SIMULATIONS

We here state specific values of the parameters introduced in the previous sections and use these to evaluate the performance of the proposed jammer in Section III based on the metrics in Section IV-A. The simulations show how the proposed jammer performs in different scenarios, and how it performs in relation to the other schemes mentioned in Section IV-B.

Both the legitimate channel and the jammer channel are assumed to have a uniform delay profile, independent across the taps:

$$h[l] \sim \mathcal{CN}\left(0, \frac{1}{L}\right) \text{ and } \mathbf{g}[l] \sim \mathcal{CN}\left(\mathbf{0}, \frac{\beta}{L}\mathbf{I}\right),$$

where β represents the relative path loss of the jammer channel compared to the legitimate channel. We assume a coherence time of 1 ms and sampling time 1 µs, resulting in a frame length of $\tau_F = \tau_C/2 = 500$ samples. We further assume that Jeff listens for 50 ms, giving $N_F = 100$ frames to estimate the frame offset. For future convenience, we denote the link from Alice to Jeff by A→J, and the link from Jeff to Alice by J→A.

All jamming schemes presented in Section IV-B use the same total output power and the normalized transmit powers of the legitimate link and the jammer are fixed and equal, that is $\rho = \rho_P = \rho_J = 7$ dB. When Jeff is silent, ρ has the interpretation of the SNR of the legitimate link. Similarly, $\rho\beta$ can be thought of as the SNR of A→J as well as J→A. We say that there is a *legitimate link advantage* (LLA) equal to β^{-1}.

To see how the number of channel taps, the LLA, and the number of jammer antennas affect the performance, we focus on four scenarios, henceforth referred to as SCEN 1 through SCEN 4. In SCEN 1 and SCEN 2, we have a flat fading channel ($L = 1$), and LLA of 23 dB and 26.5 dB, respectively. In SCEN 3 and SCEN 4, we have $L = 5$ channel taps, and LLA of 23 dB and 26.5 dB, respectively. Using SCEN 1 as a reference, we can see how the performance of the jammer is affected by increasing the LLA (SCEN 2), increasing the number of channel taps (SCEN 3), or both (SCEN 4). Each scenario has the same style in all the figures, to make comparisons easy. The four different scenarios are summarized in Table I.

We choose to study scenarios with relatively large LLA (23 dB and 26.5 dB), because these are the most interesting. For small LLA, there is little difference between many of the schemes, as the scenario (for the chosen parameters) is too easy for the jammer, most schemes perform well. On the other hand, if the LLA is too large, none of the schemes have any noticeable effect on the legitimate link SE (C_{SE}). The case of $L = 5$ corresponds to a delay spread of 5 µs (or a coherence bandwidth of approximately 100 kHz) for the selected sampling time.

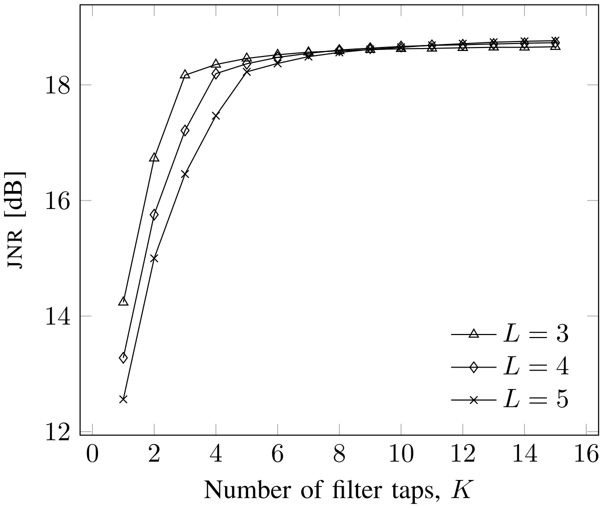


Fig. 6. The JNR, (19), for different numbers of filter taps K and channel taps L when the jammer is equipped with 100 antennas, has perfect channel knowledge, knows the frame offset τ_{O}, and the LLA is 0 dB. Even though a larger number of filter taps improves the performance of the jammer, we reach a clear point of diminishing returns after $K = L$.

We stress that "performance" refers to the performance of the *jammer*, unless explicitly stated. Specifically, improved performance means better jamming and hence a *lower* legitimate link SE.

A. Impact of Filter Length

The number of taps for the filter creating the jamming signal vector in (13b), K, is yet to be specified. The effect of the different numbers of taps, for the ideal case when the jammer knows both the realization of the channel $\mathbf{G}$ and the frame offset τ_{O} perfectly is shown in Fig. 6 (for LLA 0 dB). We show the jamming to noise ratio (JNR), defined as (cf. (4) and (5))

$$\mathrm{JNR} \triangleq \frac{\mathbb{E}\left[|r_{\mathrm{J}}[n]|^2\right]}{\mathbb{E}\left[|\epsilon[n]|^2\right]}. \tag{19}$$

Even though Fig. 6 shows that the jammer can perform better (higher JNR) with a longer filter, we assume that Jeff uses the same number of taps in the construction of the jamming signal as there are channel taps, i.e. $K = L$ in (13b). The reason being that each filter tap adds complexity, but adding more than L taps gives a relatively small increase in the JNR. Note that any given result presented subsequently could thereby be slightly improved, if the number of filter taps is increased.

B. Impact of Jammer Location

If the terminals are located at different distances from the jammer, the frame offset estimation can be simplified. Different distances means different path losses, which in turn implies that the power of the received signal at Jeff will vary between even and odd frames. If this variation in power is large enough, a detector measuring the received energy is sufficient to accurately estimate the frame offset.

To illustrate this, we consider two scenarios. In the first scenario, the distance between Jeff and Alice is 1.2 times the distance between Jeff and Bob, which gives a path loss difference of about 3 dB (assuming a path loss exponent of 3.8). Furthermore, in this example Jeff has 100 antennas, $\tau_{\mathrm{F}} = 100$, $N_{\mathrm{F}} = 10$ and $L = 1$. The true frame offset is set to $\tau_{\mathrm{O}} = 23$. The second scenario is identical, but has Alice and Bob at the same distance from Jeff, giving no (0 dB) difference in path loss. The metric used to estimate the frame offset is the (normalized) absolute difference between the energy received in even and odd frames. Jeff finds the frame offset estimate as the offset that gives the largest absolute difference, since this indicates that Jeff has successfully found the border between the high-energy even frames and the low-energy odd frames. Note that since we consider the *absolute* difference the jammer cannot distinguish between an odd-even crossing and an even-odd crossing, making the metric τ_{F}-periodic.

Fig. 7 shows an example output when the jammer considers a range of possible frame offsets. Looking at the 3 dB curve, we see the metric increases until reaching the first peak at $\tau = 23$ (which is the true frame offset in this case). This peak represents the first odd-even crossing. As mentioned earlier, the metric is periodic, so the next peak is located at $23 + \tau_{\mathrm{F}}$ and represents the first even-odd crossing. In the second scenario, where the difference in path loss is 0 dB, this estimator performs very poorly. Since all received samples on average have the same energy, it is impossible to separate the samples in odd and even frames, making the chosen metric highly volatile.

As a comparison, the proposed frame estimate metric (11) is also shown in Fig. 7 for the case with the same path loss. As seen, the metric has its minimum exactly at τ_{O} and thus manages to correctly estimate the frame offset, even in the scenario where there is no difference in path loss.

Consequently, when the difference in path loss is large enough analyzing the structure of the covariance matrix is not necessary. However, in the simulations below, we consider Alice and Bob to be located equidistant from Jeff, as this is the most difficult scenario. Jeff thus solely relies on the estimation presented in Section III-A.

C. Impact of Jamming Scheme

In Fig. 8 we see how the different transmission schemes perform in SCEN 1. As a reference the dotted line shows C_{P}, the SE of the legitimate link when Jeff is silent. We see that the performance of OMNI is the worst, followed by TRC and that OMNI barely has any effect on C_{SE}. TRC performs similarly to OMNI for small number of antennas, but improves as more antennas are added. The other four jammers have very similar performance to each other, which implies that both the frame offset and the beamforming vectors are estimated accurately, even when the number of antennas is small. Moreover, all schemes except OMNI benefit from adding more antennas.

Fig. 9 illustrates the performance of all jammers in a more challenging scenario, SCEN 4. Here the jammer is further away from the legitimate link, and the channel is now frequency selective, with five taps. Once again we find that OMNI and TRC perform the worst, now degrading the legitimate link even

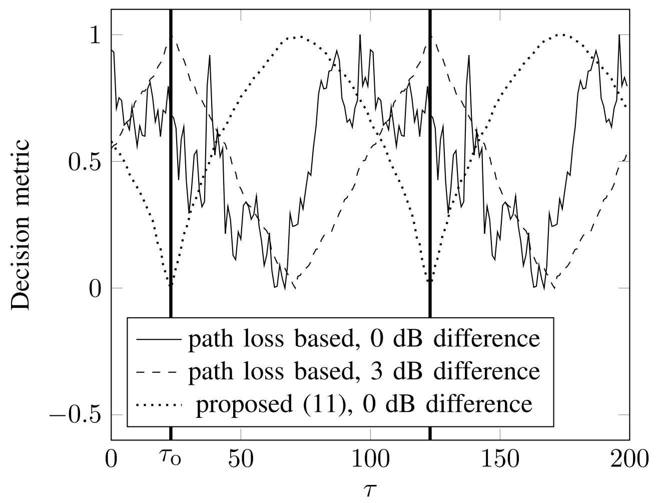


Fig. 7. Example output of the simple decision metric (normalized absolute difference in received energy between even and odd frames) for two scenarios: one where the terminal are the same distance from the jammer (0 dB difference in path loss) and one where they are at different distances from the jammer (3 dB difference in path loss). The vertical lines show the ground truth (τ_{F}-periodic). Using this metric, the jammer performs well when the difference in path loss is 3 dB but poorly when there is no difference in path loss. The proposed metric (11) can correctly estimate the frame offset, even in the 0 dB case. The range of considered frame offsets is here increased to $2\tau_{\mathrm{F}}$ to show the periodicity of both metrics. This periodicity is due to the fact that the jammer cannot distinguish between even and odd frames.

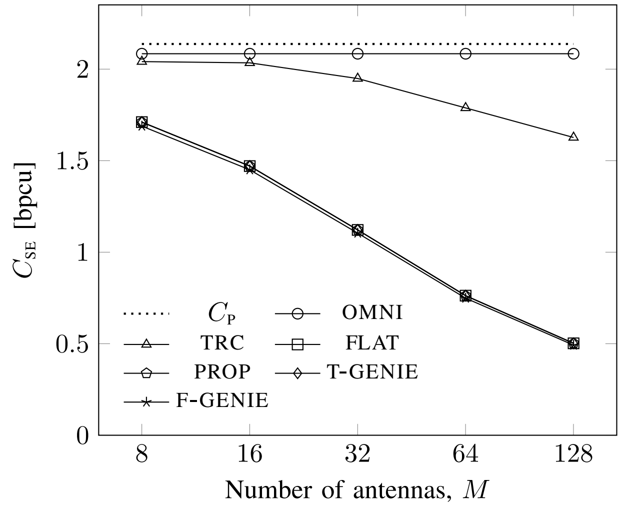


Fig. 8. A comparison of different transmission schemes for SCEN 1 (cf. Section IV-B and Table I) for a varying number of antennas at the jammer. The dotted line is the spectral efficiency without jamming. In general, all schemes which utilizes beamforming or have to estimate the frame offset benefit from more antennas. PROP performs just as well as F-GENIE, and outperforms OMNI by a large margin, even for a moderate number of antennas.

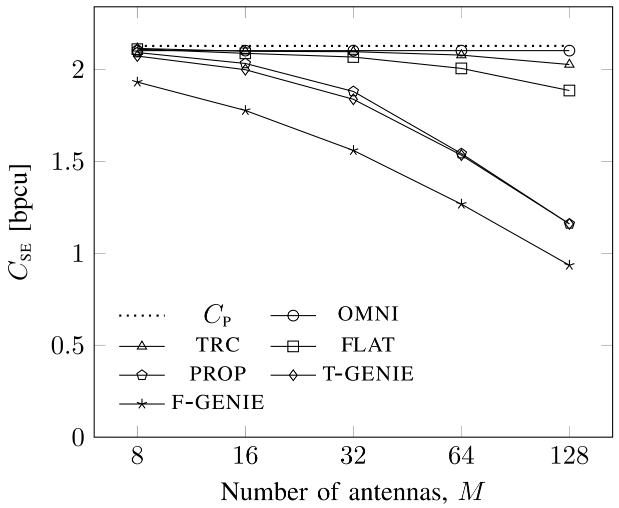


Fig. 9. A comparison of different transmission schemes for SCEN 4 (cf. Section IV-B and Table I) for a varying number of antennas at the jammer. The dotted line is the spectral efficiency without jamming. As in Fig. 8, all schemes which utilize the antenna array benefit from more antennas. When the number of antennas at the jammer is large, PROP can significantly decrease the legitimate SE, while OMNI barely affects the legitimate SE at all.

less than in SCEN 1. The four jammers derived from Section III are now spread out. FLAT fails to construct efficient jamming signals, because the effects of the frequency-selective channel are ignored. There is now a significant gap between F-GENIE and PROP which, looking at the small difference between PROP and T-GENIE, can be attributed to the construction of the jamming signals. When the number of antennas is small, all practical schemes have the same performance. However, as M grows, we see PROP outperforming OMNI by a significant margin.

D. Number of Jammer Antennas

The more antennas Jeff has, the better is his beamforming. For the F-GENIE, a decrease in J→A SNR can always be mitigated by using more antennas. To see this, consider the case of a single channel tap, the optimal beamforming vector is then given by $\mathbf{g}^*/||\mathbf{g}||$ (maximum ratio transmission), and the expected power of the received jamming signal is $\rho_{\mathrm{J}}\beta M$. So in this case, Jeff can compensate for the increased path loss by increasing his output power or having more antennas.

In A→J, on the other hand, it is not as easy see that more antennas gives a more accurate frame offset estimate.[10] This is demonstrated in Fig. 10, where the average error of the frame offset estimate is shown. We see that more antennas can compensate for both more channel taps, and higher LLA. However, in the case where both of these effects are present, quite a few additional antennas are needed to compensate for the combined effect.

The ultimate performance metric, however, is not the ability to estimate the frame timing, but how much Jeff can impair the legitimate link. Looking at Fig. 11 we see how PROP performs

[10] This is assuming that the A→J SNR is large enough. At some point, if the SNR is too low, all the jammer will see is noise, and the frame offset estimate will be a uniformly distributed random variable.

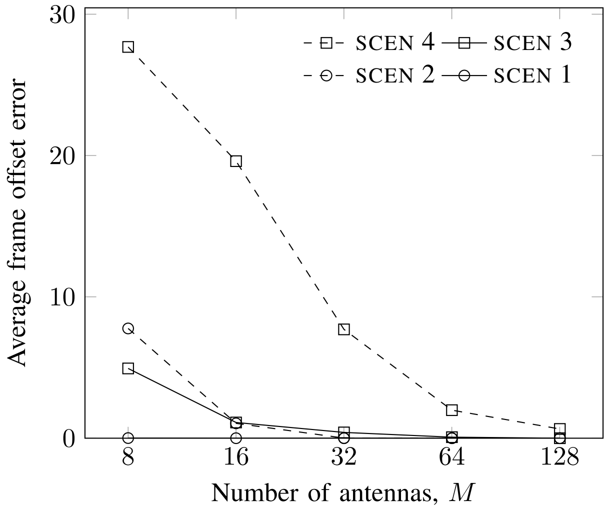


Fig. 10. The frame offset estimate gets more accurate the more antennas the jammer has. More antennas can effectively compensate for low A→J SNR, or a larger number of channel taps. To mitigate the effects of both of these complications at the same time, many additional antennas may be needed.

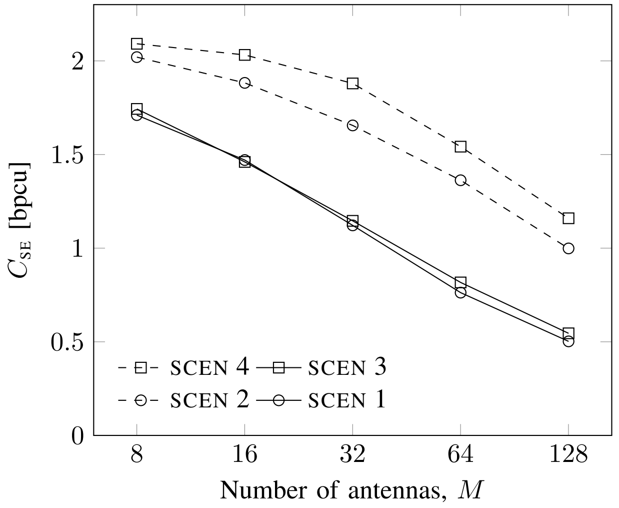


Fig. 11. Performance of the proposed jammer in the same scenarios as in Fig. 10 for different number of antennas at the jammer. For any scenario, the performance increases with M.

in the four scenarios from Table I. In all scenarios, adding more antennas always helps; Jeff can cause more damage to the legitimate link the more antennas he has, partly because the improved frame offset estimate, and partly because of the increased beamforming gain.

We can see a quite significant difference in performance between the scenarios for large M in Fig. 11, even though the frame timing estimate is of similar quality (Fig. 10). Comparing SCEN 1 and SCEN 2, the change in LLA has a considerable effect on how well Jeff can estimate the beamforming vectors. Moreover, looking at SCEN 1 and SCEN 3, we see that when the LLA is small enough the frequency selectivity of the channel makes little difference. Looking at SCEN 2 and SCEN 4, however, the added frequency selectivity makes estimation of the beamforming vectors even more difficult.

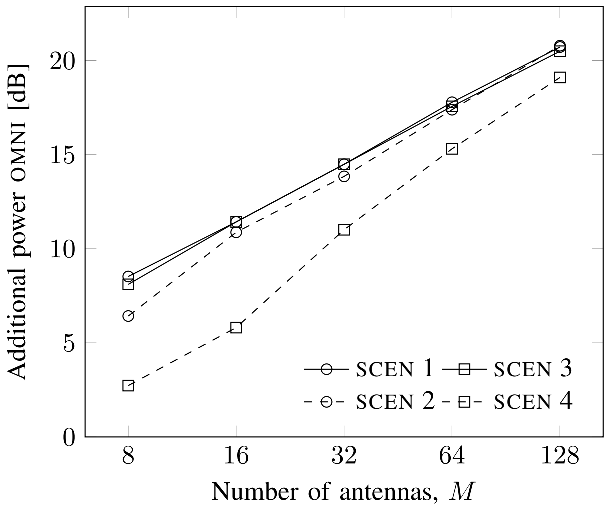


Fig. 12. The additional power needed for OMNI to have the same performance as PROP. The increase in power is proportional to the number of antennas at the jammer, M, when M is large.

Finally, we consider the case where OMNI is allowed to spend more power than PROP. Fig. 12 shows how much more transmit power OMNI has to use, to get the same performance as PROP. We see that when the number of antennas is large enough to push the frame error close to zero, the improvement is linear (note the log-log scale). When the jammer has M antennas, and M is large, we can reduce the output power by almost $10\log_{10}(M)$ dB, compared to OMNI, without sacrificing jamming performance.

VI. Conclusion

The channel reciprocity is one of the benefits of TDD links, but this reciprocity can also be exploited by an adversary. A multi-antenna jammer for TDD systems can outperform an omnidirectional barrage jammer by orders of magnitude in many scenarios with very limited knowledge of the legitimate transmission. For a jammer with M antennas, the proposed algorithm can cause substantially the same harm to a legitimate link as a single-antenna jammer with $1/M$ of the output power even without prior channel knowledge. Both increased frequency selectivity and distance between the jammer and the legitimate transmitters can be dealt with by adding more antennas. Both frame timing estimate accuracy and jamming performance increase monotonically with increasing M.

Appendix

A. Proof of Theorem 2

We write the received jamming signal as

$$\sum_{l=0}^{L-1}\mathbf{g}^{\mathrm{T}}[l]\mathbf{z}[n-l]=\sum_{l=0}^{L-1}\sum_{k=0}^{K-1}\mathbf{g}^{\mathrm{T}}[l]\mathbf{v}[k]w[n-(l+k)],$$

where $\mathbf{v}[k]=[v_1[k],v_2[k],\ldots,v_M[k]]^{\mathrm{T}}$. With

$$\mathbf{V}=[\mathbf{v}[0],\ldots,\mathbf{v}[K-1]]$$

and

$$\mathbf{W}_{k,l}[n]=w[n-(l+k-2)]$$

we can write,

$$\sum_{l=0}^{L-1} \mathbf{g}^{\mathrm{T}}[l]\mathbf{z}[n-l] = \mathbf{w}^{\mathrm{T}}[n](\mathbf{I}_K \otimes \mathbf{G}^{\mathrm{T}})\mathbf{v},$$

where $\mathbf{w}[n] = \mathrm{vec}(\mathbf{W}[n])$ and $\mathbf{v} = \mathrm{vec}(\mathbf{V})$. The expected received power (given the channel) is

$$\mathbb{E}\left(\|\mathbf{w}^{\mathrm{T}}[n](\mathbf{I}_K \otimes \mathbf{G}^{\mathrm{T}})\mathbf{v}\|_2^2 \middle| \mathbf{G} \right) = \mathbf{v}^{\mathrm{H}}\bar{\mathbf{G}}\mathbf{v},$$

where we have defined

$$\bar{\mathbf{G}} \triangleq (\mathbf{I}_K \otimes \mathbf{G}^{\mathrm{T}})^{\mathrm{H}}\mathbb{E}(\mathbf{w}^*[n]\mathbf{w}^{\mathrm{T}}[n])(\mathbf{I}_K \otimes \mathbf{G}^{\mathrm{T}}).$$

Let $\boldsymbol{\Psi} = \mathbb{E}(\mathbf{w}^*[n]\mathbf{w}^{\mathrm{T}}[n])$. This matrix will be all zeros, except for elements $\boldsymbol{\Psi}_{ij}$ where the ith and jth element of $\mathbf{w}[n]$ are the same noise sample. Because $\mathbf{W}[n]$ is a Hankel matrix, $\mathbf{W}_{i,j}[n]$ is the same noise sample as $\mathbf{W}_{k,l}[n]$ if $i+j=k+l$. Further, having the mapping from $\mathbf{W}[n]$ to $\mathbf{w}[n]$, namely the $\mathrm{vec}(\cdot)$ operator, it is a bookkeeping exercise to show that

$$\boldsymbol{\Psi}_{ij} = \begin{cases} 1, & \text{if } n_i + m_i = n_j + m_j, \\ 0, & \text{otherwise,} \end{cases}$$

where $m_i = (i-1 \mod L) + 1$ (row index) and $n_i = \lceil \frac{i}{L} \rceil$ (column index). In matrix notation, this means

$$\boldsymbol{\Psi} = \begin{pmatrix} \boldsymbol{\Psi}_0 & \boldsymbol{\Psi}_1 & \cdots \\ \boldsymbol{\Psi}_1^{\mathrm{H}} & \boldsymbol{\Psi}_0 & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix},$$

where

$$\boldsymbol{\Psi}_k = \begin{pmatrix} \mathbf{0}_{k \times L-k} & \mathbf{0}_k \\ \mathbf{I}_{L-k} & \mathbf{0}_{L-k \times k} \end{pmatrix},$$

for $k = 0, \ldots, L-1$ and $\boldsymbol{\Psi}_k = \mathbf{0}_L$ for $k \geq L$. □

REFERENCES

[1] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.

[2] MAMMOET, "The MAMMOET project," https://mammoet-project.eu/.

[3] J. Vieira, S. Malkowsky, K. Nieman, Z. Miers, N. Kundargi, L. Liu, I. Wong, V. Öwall, O. Edfors, and F. Tufvesson, "A flexible 100-antenna testbed for massive MIMO," in *2014 IEEE Globecom Workshops (GC Wkshps)*, Dec. 2014, pp. 287–293.

[4] C. Shepard, H. Yu, N. Anand, E. Li, T. Marzetta, R. Yang, and L. Zhong, "Argos: Practical many-antenna base stations," in *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking*, ser. Mobicom '12. New York, NY, USA: ACM, 2012, pp. 53–64.

[5] J. H. Reed and M. Lichtman, "Virginia Tech's response to FirstNet NOI," Nov. 2012.

[6] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: Threat assessment and mitigation," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 54–61, Apr. 2016.

[7] J. A. Volpe, "Vulnerability assessment of the transportation infrastructure relying on GPS," *ResearchGate*, Jan. 2001.

[8] Regeringen och Regeringskansliet, "Göteborg 2001 (SOU 2002:122)," http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2002/01/sou-2002122/, Jan. 2002.

[9] T. Song, K. Zhou, and T. Li, "CDMA system design and capacity analysis under disguised jamming," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2487–2498, Nov. 2016.

[10] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "MIMO-based jamming resilient communication in wireless networks," in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, Apr. 2014, pp. 2697–2706.

[11] ——, "Jamming resilient communication using MIMO interference cancellation," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1486–1499, 2016.

[12] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 152–157, Jan. 1983.

[13] E. A. Jorswieck, H. Boche, and M. Weckerle, "Optimal transmitter and jamming strategies in Gaussian MIMO channels," in *2005 IEEE 61st Vehicular Technology Conference*, vol. 2, May 2005, pp. 978–982 Vol. 2.

[14] M. Lichtman, J. D. Poston, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer, and J. H. Reed, "A communications jamming taxonomy," *IEEE Security Privacy*, vol. 14, no. 1, pp. 47–54, Jan. 2016.

[15] A. Bayesteh, M. Ansari, and A. K. Khandani, "Effect of jamming on the capacity of MIMO channels," University of Waterloo, Waterloo, Ontario, Canada, Technical, 2004.

[16] Q. Liu, M. Li, X. Kong, and N. Zhao, "Disrupting MIMO communications with optimal jamming signal design," *IEEE Transactions on Wireless Communications*, vol. 14, no. 10, pp. 5313–5325, Oct. 2015.

[17] S. Sodagari and T. C. Clancy, "Efficient jamming attacks on MIMO channels," in *2012 IEEE International Conference on Communications (ICC)*, Jun. 2012, pp. 852–856.

[18] C. Shahriar, S. Sodagari, and T. C. Clancy, "Performance of pilot jamming on MIMO channels with imperfect synchronization," in *2012 IEEE International Conference on Communications (ICC)*, Jun. 2012, pp. 898–902.

[19] R. Miller and W. Trappe, "On the vulnerabilities of CSI in MIMO wireless communication systems," *IEEE Transactions on Mobile Computing*, vol. 11, no. 8, pp. 1386–1398, Aug. 2012.

[20] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Transactions on Information Theory*, vol. 50, no. 9, pp. 2119–2123, Sep. 2004.

[21] V. S. S. Nadendla, V. Sharma, and P. K. Varshney, "On strategic multi-antenna jamming in centralized detection networks," *IEEE Signal Processing Letters*, vol. 24, no. 2, pp. 186–190, Feb. 2017.

[22] D. J. Bachmann, R. J. Evans, and B. Moran, "Game theoretic analysis of adaptive radar jamming," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 47, no. 2, pp. 1081–1100, Apr. 2011.

[23] Y. E. Sagduyu, R. A. Berry, and A. Ephremides, "Jamming games in wireless networks with incomplete information," *IEEE Communications Magazine*, vol. 49, no. 8, pp. 112–118, Aug. 2011.

[24] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[25] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[26] J. Vinogradova, E. Björnson, and E. G. Larsson, "Detection and mitigation of jamming attacks in massive MIMO systems using random matrix theory," in *2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Jul. 2016, pp. 1–5.

[27] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin, "Securing massive MIMO at the physical layer," in *2015 IEEE Conference on Communications and Network Security (CNS)*, Sep. 2015, pp. 272–280.

[28] H. Pirzadeh, S. M. Razavizadeh, and E. Björnson, "Subverting massive MIMO by smart jamming," *IEEE Wireless Communications Letters*, vol. 5, no. 1, pp. 20–23, Feb. 2016.

[29] M. R. D. Rodrigues and G. Ramos, "On multiple-input multiple-output Gaussian channels with arbitrary inputs subject to jamming," in *2009 IEEE International Symposium on Information Theory*, Jun. 2009, pp. 2512–2516.

[30] X. Zhou, D. Niyato, and A. Hjorungnes, "Optimizing training-based transmission against smart jamming," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 6, pp. 2644–2655, Jul. 2011.

[31] S. Shafiee and S. Ulukus, "Capacity of multiple access channels with correlated jamming," in *MILCOM 2005 - 2005 IEEE Military Communications Conference*, Oct. 2005, pp. 218–224 Vol. 1.

[32] M. Karlsson and E. G. Larsson, "Massive MIMO as a cyber-weapon," in *2014 48th Asilomar Conference on Signals, Systems and Computers*, Nov. 2014, pp. 661–665.

[33] E. T. S. Institute, "TR 102 300-3," Jun. 2009.

[34] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge: Cambridge University Press, 2005.

[35] S. Amuru and R. M. Buehrer, "Optimal jamming against digital modulation," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2212–2224, Oct. 2015.

[36] S. Kay, *Fundamentals of Statistical Signal Processing, Volume II: Detection Theory*, 1st ed. Englewood Cliffs, N.J: Prentice Hall, Feb. 1998.

[37] T. W. Anderson, "Asymptotic theory for principal component analysis," *Ann. Math. Statist.*, vol. 34, no. 1, pp. 122–148, Mar. 1963.

[38] M. T. Heath, *Scientific Computing: An Introductory Survey*, 2nd ed. New York, NY, USA: McGraw-Hill, 2005.

[39] B. Hassibi and B. M. Hochwald, "How much training is needed in multiple-antenna wireless links?" *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 951–963, Apr. 2003.

[40] S. Kritchman and B. Nadler, "Non-parametric detection of the number of signals: Hypothesis testing and random matrix theory," *IEEE Transactions on Signal Processing*, vol. 57, no. 10, pp. 3930–3941, Oct. 2009.

[41] H. Arslan and T. Yucek, "Delay spread estimation for wireless communication systems," in *Proceedings of the Eighth IEEE Symposium on Computers and Communications. ISCC 2003*, Jun. 2003, pp. 282–287 vol.1.

Marcus Karlsson received the M.Sc in electrical engineering in 2013 from Linköping university, where he is pursuing a Ph.D degree with the Division of Communication Systems at the Department of Electrical Engineering. His main research interests are different aspects of Massive MIMO, such as physical layer security, with a focus on jamming, and initial access, with a focus on transmission without channel knowledge at the base station.

Emil Björnson Emil Björnson received the M.S. degree in Engineering Mathematics from Lund University, Sweden, in 2007. He received the Ph.D. degree in Telecommunications from KTH Royal Institute of Technology, Sweden, in 2011. From 2012 to mid 2014, he was a joint postdoc at the Alcatel-Lucent Chair on Flexible Radio, SUPELEC, France, and at KTH. He joined Linköping University, Sweden, in 2014 and is currently Senior Lecturer and Docent at the Division of Communication Systems. He teaches Master level courses on communications and is responsible for the Master programme in Communication Systems.

He performs research on multi-antenna communications, Massive MIMO, radio resource allocation, energy-efficient communications, and network design. He is on the editorial board of the IEEE Transactions on Communications (since 2017) and the IEEE Transactions on Green Communications and Networking (since 2016). He is also the first author of the textbook Optimal Resource Allocation in Coordinated Multi-Cell Systems from 2013. He is dedicated to reproducible research and has made a large amount of simulation code publicly available.

Dr. Björnson has performed MIMO research for more than ten years and has filed more than ten related patent applications. He received the 2016 Best PhD Award from EURASIP, the 2015 Ingvar Carlsson Award, and the 2014 Outstanding Young Researcher Award from IEEE ComSoc EMEA. He has co-authored papers that received best paper awards at the conferences IEEE ICC 2015, IEEE WCNC 2014, IEEE SAM 2014, IEEE CAMSAP 2011, and WCSP 2009.

Erik G. Larsson Erik G. Larsson received the Ph.D. degree from Uppsala University, Uppsala, Sweden, in 2002.

He is currently Professor of Communication Systems at Linköping University (LiU) in Linköping, Sweden. He was with the Royal Institute of Technology (KTH) in Stockholm, Sweden, the University of Florida, USA, the George Washington University, USA, and Ericsson Research, Sweden. In 2015 he was a Visiting Fellow at Princeton University, USA, for four months. His main professional interests are within the areas of wireless communications and signal processing. He has co-authored some 130 journal papers on these topics, he is co-author of the two Cambridge University Press textbooks *Space-Time Block Coding for Wireless Communications* (2003) and *Fundamentals of Massive MIMO* (2016). He is co-inventor on 16 issued and many pending patents on wireless technology.

He was Associate Editor for, among others, the *IEEE Transactions on Communications* (2010-2014) and the *IEEE Transactions on Signal Processing* (2006-2010). From 2015 to 2016 he served as chair of the IEEE Signal Processing Society SPCOM technical committee, and in 2017 he is the past chair of this committee. From 2014 to 2015 he served as chair of the steering committee for the *IEEE Wireless Communications Letters*. He was the General Chair of the Asilomar Conference on Signals, Systems and Computers in 2015, and its Technical Chair in 2012. He is a member of the IEEE Signal Processing Society Awards Board during 2017–2019.

He received the IEEE Signal Processing Magazine Best Column Award twice, in 2012 and 2014, the IEEE ComSoc Stephen O. Rice Prize in Communications Theory in 2015 and he is receiving the IEEE ComSoc Leonard G. Abraham Prize in 2017. He is a Fellow of the IEEE.