Mitigating Jamming Attack: A Game Theoretic Perspective

Qiwei Wang, Thinh Nguyen, Khanh Pham, and Hyuck Kwon

***Abstract*—In this paper, the problem of minimizing the damaging effect on the frequency hopping (FH) spread-spectrum satellite is formulated using the two-player asymmetric zero-sum game framework. The payoff is modeled as the channel capacity of the defender under white additive Gaussian noise. The defender and attacker are capable of spreading their signals over a pre-specified frequency band. Two scenarios are considered: (a) both the attacker and defender know each other's strategies, and (b) the defender knows the attacker's strategy, but not vice versa. In each of these scenarios, we further consider whether the players have knowledge about the environments. We show how to analytically determine optimal strategies for the players in each scenario, and provide simulation results to verify our approach.**

***Index Terms*—zero-sum game, Nash equilibrium, power control, jamming attack**

I. Introduction

Satellite jamming has its roots in radio frequency (RF) jamming [1]. RF jamming is a simple idea. Its aim is to degrade the signal's integrity between a pair of senders and receivers by transmitting noise with sufficient power on the same communication band as the sender and receiver in order to lower the signal-to-noise ratio (SNR) of their transmission. Consequently, RF jamming can reduce or effectively cut off the communication link between the sender and receiver. RF jamming has been used to disrupt radar systems that guide aircraft and missiles. It is also used to disrupt radio broadcast stations in wartime or during tense periods in enemy countries [2]. Currently, there has been a rise in the number of cases in which RF jamming techniques are used to launch denial of service (DoS) attacks in WiFi and cellular networks [3]. Notably, wireless sensor networks are most vulnerable to RF jamming attacks due to their limited transmission power and capability of mitigating attacks [4], [5].

Central to a successful attack is the capability of the jammer, which includes the following: (1) transmission power and (2) information about the frequency on which the good signal is transmitted. The reason for this is clear because the noise generated by the jammer needs to have sufficient power and to be on the same band as the good signal in order to reduce the SNR of the good signal. For satellite communications, the transmission between earth-based terminals is relayed by a satellite. Thus, an effective way for the jammer to attack is through the relay, i.e., the satellite, since it is more difficult to attack the terminal. The difficulty comes from the fact that the jammer needs to be in proximity of the receiver, which it may know, or it might increase the potential of being detected. Thus, in this paper, we will analyze the frequency hopping (FH) radio jamming and mitigation in which, both the jammer and the defender will employ their optimal strategies based on what they know from a zero-sum game theoretic setting. Specifically, our contributions include:

1) Formulate the problem of minimizing the damaging effect of satellite jamming attacks using the two-player asymmetric zero-sum game framework. The payoff is modeled as the channel capacity of the defender under white additive Gaussian noise. The defender and attacker are capable of spreading their signals over a pre-specified frequency band.
2) Provide performance analysis for the *Perfect Information Game*. In this scenario, both attacker and defender are rational and intelligent entities with perfect knowledge of the game. We show that there exists an optimal Nash equilibrium (NE) strategy for each player. Furthermore, we obtain a closed-form for the NE strategies that turns out to be a *modified* version of the well-known water-filling problem [6]. Any deviation from their own NE strategy would reduce their payoffs.
3) Provide performance analysis for the *Defender-biased game (typical cases)*. In this scenario, an attacker has partial information about the game, while the defender has perfect information about the game. We show that the defender will take advantage of this lack of knowledge and play an optimal strategy to obtain a payoff that is higher than the rate obtained if the attacker would play the NE strategy with perfect information. This is the important property of a game that has NE.
4) Provide performance analysis for the *Attacker-biased game (rare cases)*. We analyze the special case when the attacker knows the defender's strategies, but the defender does not know the attacker's strategy due to imperfection information. We provide an algorithm to find the corresponding payoffs.

We note that for the Perfect Information Game, while it is not difficult to obtain the closed-form solutions for the optimal strategies mathematically, it is not trivial to immediately see

Q. Wang is with the School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, OR 97330, USA e-mail: wangqi@oregonstate.edu

T. Nguyen is with the School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, OR 97330, USA e-mail: thinhq@eecs.oregonstate.edu

K. Pham is with the Air Force Research Laboratory, e-mail: khanh.pham.1@us.af.mil

H. Kwon is with the Department of Electrical Engineering and Computer Science, Wichita State University, Wichita, KS 67260, USA e-mail: hyuck.kwon@wichita.edu

Manuscript received XXX, XX, 2015; revised XXX, XX, 2015.

that the optimal strategies would follow the *modified* water-filling solution. For example, if the game payoff is not the information capacity, but rather the bit-error rate [7], then the payoff as a function of attacker/defender strategies is no longer convex/concave. As a result, there would be no NE and no closed-form results for NE can be obtained. Also, it is rare that one can obtain a closed-form result for NE. Instead, algorithms are often used to find the NE(s). Furthermore, it is not obvious why both defender and attacker will try to follow the water-filling solution, rather than just the defender, since in the classic power control problem, the water-filling solution is applied in non-game theoretic settings. Overall, our paper emphasizes a fundamental approach to satellite jamming by analyzing beyond the typical cases of real-world. In fact, we provide an analysis for the case where the attacker has the advantage over the defender, which of course rarely happens. As argued in the security community, it is the special cases, not the common cases, that will break a security system. Thus, rather than taking a myopic view, our work assumes that a variety of information, e.g., satellite communication parameters or channel conditions, might be leaked through other means, such as espionage.

II. Related Work

Early literature on defense techniques against RF jamming attacks typically focused on narrow band jamming. Specific techniques such as transversal filters [8] or the singular-value decomposition (SVD)-based method [9] are proposed to suppress single-tone attacks. On the other hand, when information on jamming frequency is not known at the defender, defense schemes using channel codes such as convolutional codes, or Bose-Chaudhuri-Hocquenghem (BCH) codes, have been shown to be highly effective [10]. However, these techniques introduce extra latency and bandwidth. Recently, a number of adaptive anti-jamming techniques have been proposed for global positioning system (GPS) satellites [11]. For example, these schemes include adaptive antenna array [12] and frequency/time domain filtering [13]. Another type of anti-jamming technique uses spread-spectrum methods such as frequency hopping [14], [15], [7] to evade the jammer. Specifically, in [15], a detect/transmit mode switch mechanism is proposed to identify the jamming frequency statistics, and an optimized frequency hopping strategy is proposed based on the Markov decision process [15]. In [7], the defender observes the jamming statistics and, based on this, generates a frequency hopping pattern to minimize the error rate caused by jamming. Other spread-spectrum-based techniques such as a scheme using notch filters on the base band [16] are also shown to be effective against jamming attack. More recently, many novel approaches have been proposed on jamming/anti-jamming attacks. [17] improves the attack efficiency towards a wireless smart grid network by dynamically implementing spoofing and jamming. The optimality is found by dynamic programming. A security-aware efficient data transmission scheme for Intelligent Transportation System (ITS) is introduced in [18] by cloud-based server using dynamic server selection methodology.

All of the aforementioned techniques assume that attackers are not sufficiently knowledgeable about the defender. On the other hand, a sophisticated attacker can employ different jamming strategies adaptively to reduce the effectiveness of a defense strategy. Essentially, both the defender and attacker play a game in which the defender tries to maximize some payoff, e.g., throughput, and the attacker tries to minimize it. Therefore, the game theory approach [19] is often employed to study channel security as well as spectrum allocation [20], [21]. Work based on game theory in the context of FH jamming [22], [23], [24] has also been done. For example, in [22], the NE of an uncoordinated frequency hopping (UFH) scenario is characterized by showing a mixed strategy for the transmitter, receiver, and jammer. A more sophisticated scenario, namely quorum-based FH rendezvous, is analyzed in [24]. Unlike the other FH techniques that simply randomly pick a frequency band, a quorum-based FH rendezvous uses a quorum rule to pick the transmission channel, and the jammer chooses the attack channel in the same way. In this case, the NE of a three-player game is shown not to exist, but does exist for a simplified two-player game. Additionally, recent research has focused on the gaming analysis of a timing channel [25], [26], [27], [28]. In [25], W. Xu et. al described the timing channel anti-jamming technique. The timing channel is able to transmit data encoded by the time duration of a signal. The power allocation game between the transmitter and the defender in a timing channel can be modeled as a non-zero-sum Stackelberg Game. Unlike Nash equilibrium, a Stackelberg equilibrium assumes that one player is leading while the other is following. In the game analyzed in [26], [27], [28], the transmitter is modeled as the leader and the attacker is the follower. It is proved that a Nash equilibrium and a Stackelberg equilibrium both exist, and the latter performs better for the transmitter. While the analysis is thorough for a timing channel with specific payoff functions, our work takes a more generalized approach by defining the payoff as the total capacity.

III. Jamming Attack: A Spread-Spectrum Game

A. Game Theoretic Overview

A zero-sum game involves two players: an attacker and a defender. Using their respective strategies, the defender tries to maximize a pre-specified expected payoff, and the attacker tries to minimize it. From its perspective, the defender will try to maximize the expected payoff with an optimal randomized strategy. On the other hand, from its perspective, the attacker will try to minimize the expected payoff using its own optimal strategy. In the classical setting, both attacker and defender are assumed to know each other's strategy.

Let us now consider the defender's perspective. Since the attacker knows the defender's strategy, the defender reasons that the attacker will try to play the strategy that minimizes the expected payoff. Being rational, the defender will play an optimal strategy that obtains the maximum payoff. Similarly, from the attacker's viewpoint, the attacker will try to use its optimal strategy to minimize the payoff given that the defender has already maximized the payoff with some strategy. When the optimal payoffs for attacker and defender are equal, this is considered to be a Nash equilibrium.

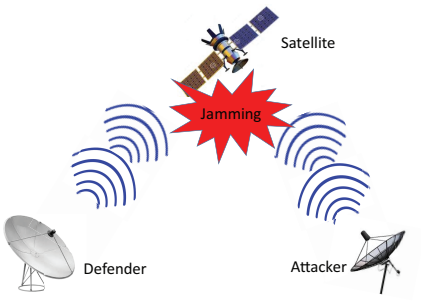


Figure 1. A typical scenario of a uplink radio interference and mitigation with potential satellite communications applications.

B. Game Model

Fig. 1 shows a typical scenario where an attack occurs at a satellite. The defender transmits information to the satellite using the spread-spectrum technique, where the transmitted signal is spread over multiple transmission bands. On the other hand, the attacker tries to reduce the information rate by transmitting noise via spread-spectrum techniques, i.e., jamming the defender's signal. A jamming attack is successful if the attacker is able to greatly reduce the defender's information rate.

Table I shows the notations that are used:

N	Number of discrete frequency bins
B	Bandwidth per frequency bin
P_D	Total power received at satellite relay from the defender
P_A	Total power received at satellite relay from the attacker
P_N	Average noise power over all frequency bins
$\mathbf{n} \in \mathbb{R}_+^N$	Vector whose ith element denotes the average additive white noise power on frequency bin i
$\mathbf{x} \in \mathbb{R}_+^N$	Strategy of defender, received power on certain frequency bin i is $\mathbf{x}_i$
$\mathbf{y} \in \mathbb{R}_+^N$	Strategy of attacker, defined similarly as $\mathbf{x}$
$\mathcal{X}$	Feasible set of defender strategies. $\mathcal{X} = \{\mathbf{x} \in \mathbb{R}_+^n \mid \sum_i^N \mathbf{x}_i \leq P_D\}$.
$\mathcal{Y}$	Feasible set of attacker strategies. $\mathcal{Y} = \{\mathbf{y} \in \mathbb{R}_+^n \mid \sum_i^N \mathbf{y}_i \leq P_A\}$.
$\mathbf{x}^*$, $\mathbf{y}^*$	Optimal strategy used by defender and attacker, respectively
$p, p^* \in \mathbb{R}$	Expected payoff and optimal payoff, respectively

Table I
NOTATIONS

We assume a free space path loss model, as shown in Fig. 1, because both the defender and the attacker are typically in the line of sight (LOS) to the satellite relay. In addition, this paper considers a decoder and forward type relay satellite, and does not include the typical satellite channel characteristics, e.g., nonlinearity in a satellite transponder, a rain loss, etc. This paper focuses on the effects on the data rate of the channel from a transmitter to a relay satellite under a jamming attack environment. The power at the relay satellite received from the defender and the attacker can be simplified as $\mathbf{x}_i = P_{DTi}\left(\frac{\sqrt{G_{DT}G_R}\lambda_i}{4\pi d_{DR}}\right)^2$ and $\mathbf{y}_i = P_{ATi}\left(\frac{\sqrt{G_{AT}G_R}\lambda_i}{4\pi d_{AR}}\right)^2$, respectively, at a certain frequency bin i, where G_{DT} and G_{AT} are the transmit antenna gain of the defender and attacker, respectively; d_{DR} and d_{AR} are the distance from the defender and the attacker to the relay satellite, respectively; G_R is the receiver antenna gain at the relay satellite; and λ_i is the wavelength at the hopping frequency i. Therefore, if $\mathbf{x}_i$ and $\mathbf{y}_i$ are determined, then the corresponding transmit power P_{DTi} and P_{ATi} at frequency bin i can be computed using the other known parameters. Hence, this paper focuses on the computation of $\mathbf{x}_i$ and $\mathbf{y}_i$ using game theory. The satellite jamming game is modeled as a zero-sum game. The objective of the defender is to maximize the information rate, while the objective of the attacker is to minimize this rate. Assuming that the channels have white additive Gaussian noise, if the defender plays strategy $\mathbf{x}$ and the attacker plays strategy $\mathbf{y}$, then the information rate, i.e., the maximum bit rate [29] that can be transmitted by the defender is

$$f(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{N} B \log\left(1 + \frac{\mathbf{x}_i}{\mathbf{n}_i + \mathbf{y}_i}\right). \tag{1}$$

We note that the maximum bit rate, or the channel capacity, is widely used as game payoff in literature. In [30], an OFDM transmitter's payoff is modeled as the sum of the capacity of all sub-channels, taking into account of fading channel gains as well as possible power costs. Here in Eq. (1) we suppose a more general representation. We now begin with the scenario where both attacker and defender know each other's strategies and the payoff matrix. This is called the Perfect Information Game.

C. Perfect Information Game

Similar to the classic zero-sum game discussed above, if the defender knows the attacker's strategy, and vice versa, then the goal for the defender is to find the optimal strategy $\mathbf{x}^*$ that maximizes the payoff, in particular the information rate, which is

$$\max_{\mathbf{x}\in\mathcal{X}} \min_{\mathbf{y}\in\mathcal{Y}} f(\mathbf{x}, \mathbf{y}).$$

Similarly, the goal for the attacker is to find its optimal strategy $\mathbf{y}^*$ that minimizes the information rate which is:

$$\min_{\mathbf{y}\in\mathcal{Y}} \max_{\mathbf{x}\in\mathcal{X}} f(\mathbf{x}, \mathbf{y}).$$

It is not immediately clear whether this game has a NE as the classic zero-sum game . The NE is obtained when there exists a pair $(\mathbf{x}^*, \mathbf{y}^*)$ such that $\max_{\mathbf{x}\in\mathcal{X}} \min_{\mathbf{y}\in\mathcal{Y}} f(\mathbf{x}, \mathbf{y}) = \min_{\mathbf{y}\in\mathcal{Y}} \max_{\mathbf{x}\in\mathcal{X}} f(\mathbf{x}, \mathbf{y})$.

Our first result is that this game does indeed have a NE. Our proof relies on the following theorem from the work of J. Neumann [31].

Theorem 1. *Let $\mathbf{x} \in \mathcal{X}$ and $\mathbf{y} \in \mathcal{Y}$, if $f(\mathbf{x}, \mathbf{y})$ is concave in $\mathbf{x}$ for any $\mathbf{y}$, and $f(\mathbf{x}, \mathbf{y})$ is convex in $\mathbf{y}$ for any $\mathbf{x}$. Then:*

$$\max_{\mathbf{x}\in\mathcal{X}} \min_{\mathbf{y}\in\mathcal{Y}} f(\mathbf{x}, \mathbf{y}) = \min_{\mathbf{y}\in\mathcal{Y}} \max_{\mathbf{x}\in\mathcal{X}} f(\mathbf{x}, \mathbf{y}).$$

Definition 1. *$f(\mathbf{x})$ is a convex function if for $0 \leq a \leq 1$ and for any $\mathbf{x}$, $\mathbf{y}$, the following applies:*

$$f(a\mathbf{x} + (1-a)\mathbf{y}) \leq af(\mathbf{x}) + (1-a)f(\mathbf{y}).$$

Similarly, $f(\mathbf{x})$ is a concave function if

$$f(a\mathbf{x} + (1-a)\mathbf{y}) \geq af(\mathbf{x}) + (1-a)f(\mathbf{y}).$$

We are now ready to prove the first result.

Proposition 1. *The spread-spectrum game where the information rate is the payoff has a Nash equilibrium.*

Proof. See Appendix A. □

Proposition 2. *Let P_D and P_A be the total powers of the defender signal and attacker signal received by the satellite, and let x^* be the optimal defender strategy; then the satellite hub's maximum information rate (payoff) is*

$$p^* = \sum_{i\in J} B\log\left(1 + \frac{\mathbf{x}_i^*}{(P_A + P_N^J)/|J|}\right) + \sum_{i\in(K\setminus J)} B\log\left(1 + \frac{\mathbf{x}_i^*}{\mathbf{n}_i}\right), \tag{2}$$

in which J and K denote the set of index of bins used by the attacker and defender, respectively. P_N^J denotes the amount of noise power in those bins. $|J|$ denotes the cardinality of J. When the optimal attacker and defender use all the frequency bins ($|J| = N$),

$$p^* = NB\log\left(1 + \frac{P_D}{P_A + P_N}\right).$$

Proof. Consider the attacker's viewpoint. The attacker knows that the defender knows its strategy. Naturally, the defender would try to maximize the information rate based on the given attacker's strategy $\mathbf{y}$. Thus, from the attacker's viewpoint, it will try to minimize the information rate. In other words, the attacker will solve this problem:

$$p^* = \min_{\mathbf{y}\in\mathcal{Y}} \max_{\mathbf{x}\in\mathcal{X}} \sum_{i=1}^{N} B\log\left(1 + \frac{\mathbf{x}_i}{\mathbf{n}_i + \mathbf{y}_i}\right). \tag{3}$$

First, consider the max problem from the defender's viewpoint given the attacker's strategy $\mathbf{y}$. The defender will play the optimal strategy $\mathbf{x}$ such that

$$\mathbf{x}^* = \text{argmax}_{\mathbf{x}\in\mathcal{X}} \sum_{i=1}^{N} \log\left(1 + \frac{\mathbf{x}_i}{\mathbf{n}_i + \mathbf{y}_i}\right).$$

Note that B in the equation above can be omitted since it is a constant, so the optimal solution will not change. With a slight modification, this can be viewed as the well-known problem of capacity maximization of parallel Gaussian channels. Specifically, we now consider $\mathbf{n}_i + \mathbf{y}_i$ as the average power of background noise in bin i. In particular, the optimal $\mathbf{x}^*$ can be found using the Lagrange's multiplier method. To maximize a concave function $f(\mathbf{x})$ subject to a number of constraints $g_i(\mathbf{x}) \leq 0$, $i = 1, 2, \ldots, M$, the Karush-Kuhn-Tucker (KKT) conditions state that the optimal $\mathbf{x}^*$ must satisfy the following:

$$\frac{\partial f(\mathbf{x})}{\partial \mathbf{x}_i} - \lambda_i \frac{\partial g_i(\mathbf{x})}{\partial \mathbf{x}_i}|_{\mathbf{x}=\mathbf{x}^*} = 0, i = 1, 2, \ldots, M. \tag{4}$$

Replacing $f(\mathbf{x}) = \sum_{i=1}^{N} \log\left(1 + \frac{\mathbf{x}_i}{\mathbf{n}_i + \mathbf{y}_i}\right)$ for given $\mathbf{n}_i$ and $\mathbf{y}_i$, $g_1(\mathbf{x}) = \sum_{i=1}^{N} \mathbf{x}_i - P_D$ into Eq. (4) yields

$$\mathbf{x}_i + \mathbf{n}_i + \mathbf{y}_i = \lambda^{-1}. \tag{5}$$

Now, summing up the left- and right-hand sides over i, with the total noise power $P_N = \sum_{i=1}^{N} \mathbf{n}_i$, yields

$$\lambda^{-1} = \frac{P_D + P_A + P_N}{N}. \tag{6}$$

From Eqs. (5) and (6), the optimal strategy $\mathbf{x}^*$ for the defender is

$$\mathbf{x}_i^* = \frac{(P_D + P_A + P_N)}{N} - \mathbf{y}_i - \mathbf{n}_i, i = 1, 2, \ldots, N. \tag{7}$$

Next, from the attacker's viewpoint, it will find $\mathbf{y}^*$ that minimizes Eq. (3). Substituting Eq. (7) into Eq. (3) yields the following:

$$\begin{aligned} p &= \sum_{i=1}^{N} B\log\left(1 + \frac{\mathbf{x}_i}{\mathbf{n}_i + \mathbf{y}_i}\right) \\ &= \sum_{i=1}^{N} B\log\left(1 + \frac{\frac{P_D+P_A+P_N}{N} - \mathbf{n}_i - \mathbf{y}_i}{\mathbf{n}_i + \mathbf{y}_i}\right) \\ &= \sum_{i=1}^{N} B\log\left(\frac{P_D + P_A + P_N}{N}\right) \\ &- \sum_{i=1}^{N} B\log\left(\mathbf{n}_i + \mathbf{y}_i\right), \end{aligned} \tag{8}$$

which is minimized when $\sum_{i=1}^{N} \log(\mathbf{n}_i + \mathbf{y}_i)$ is maximized. Now, using the Lagrange method with μ as the multiplier yields

$$\mathbf{y}_i = \mu^{-1} - \mathbf{n}_i, i = 1, 2, \ldots, N. \tag{9}$$

Summing the left- and right-hand sides of Eq. (9) yields

$$\mu^{-1} = \frac{P_A + P_N}{N}.$$

Therefore, the optimal strategy of the attacker $\mathbf{y}^*$ is

$$\mathbf{y}_i^* = \frac{P_A + P_N}{N} - \mathbf{n}_i. \tag{10}$$

Since $\mathbf{y}_i^* \geq 0$ is required, if from Eq. (10), $\mathbf{y}_i^* < 0$, then simply set $\mathbf{y}_i^* = 0$, ignore bin i, and re-run the analysis with the remaining $N - 1$ bins. Repeat this process to obtain a feasible solution. If J is used to denote the set of bin indexes used by the attacker with cardinality $|J|$, and P_N^J denotes the

amount of noise power in those bins, then $\mathbf{y}_i^*$ can be expressed as

$$\mathbf{y}_i^* = \begin{cases} \frac{P_A+P_N^J}{|J|} - \mathbf{n}_i, i \in J \\ 0, otherwise. \end{cases} \quad (11)$$

Next, plug $\mathbf{y}^*$ into the payoff expression Eq. (7) to find $\mathbf{x}_i^*$. If $\mathbf{x}_i^* < 0$, then set $\mathbf{x}_i^* = 0$ and ignore bin i. If K is used to denote the set of bin indexes used by the defender with cardinality $|K|$, and P_N^K denotes the amount of noise power in those bins, then $\mathbf{x}_i^*$ can be expressed as

$$\mathbf{x}_i^* = \begin{cases} \frac{P_D+P_A+P_N^K}{|K|} - \mathbf{y}_i^* - \mathbf{n}_i, i \in K \\ 0, otherwise. \end{cases} \quad (12)$$

Now, notice that $|J| \leq |K| \leq N$(see **Remark 1**). Then the following is obtained:

$$\begin{aligned} p^* &= \sum_{i \in N} B \log \left(1 + \frac{\mathbf{x}_i^*}{\mathbf{y}_i^* + \mathbf{n}_i}\right) \quad (13) \\ &= \sum_{i \in K} B \log \left(1 + \frac{\mathbf{x}_i^*}{\mathbf{y}_i^* + \mathbf{n}_i}\right) \\ &= \sum_{i \in J} B \log \left(1 + \frac{\mathbf{x}_i^*}{(P_A + P_N^J)/|J|}\right) + \\ &\quad \sum_{i \in (K \setminus J)} B \log \left(1 + \frac{\mathbf{x}_i^*}{\mathbf{n}_i}\right). \end{aligned}$$

When $|J| = |K| = N$,

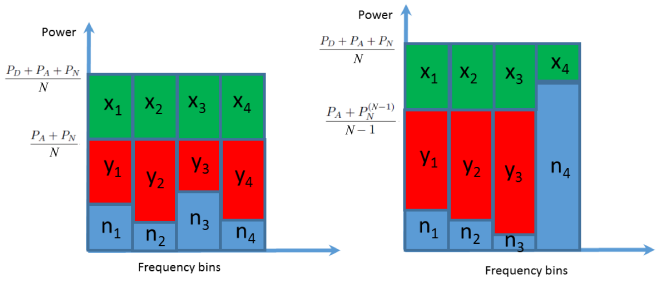
$$\begin{aligned} p^* &= \sum_{i \in N} B \log \left(1 + \frac{\mathbf{x}_i^*}{\mathbf{y}_i^* + \mathbf{n}_i}\right) \quad (14) \\ &= NB \log \left(1 + \frac{P_D}{P_A + P_N}\right). \end{aligned}$$

Now, by Proposition 1, $\max_{\mathbf{x} \in \mathcal{X}} \min_{\mathbf{y} \in \mathcal{Y}} f(\mathbf{x}, \mathbf{y}) = \min_{\mathbf{y} \in \mathcal{Y}} \max_{\mathbf{x} \in \mathcal{X}} f(\mathbf{x}, \mathbf{y})$; therefore, the payoff of the defender is $q^* = p^*$.

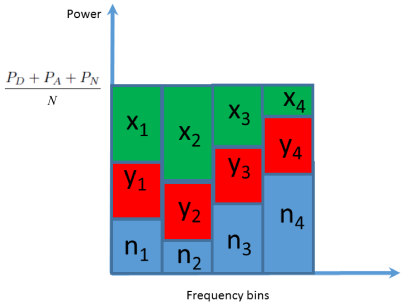
□

Remark 1: From Eq. (9), the optimal strategy for the attacker is essentially to try to fill every bin so that they have equal power. When this is not possible for some bins, it omits those bins and tries to make the power levels of the remaining bins equal. This strategy follows our intuition since any attacker's strategy that deviates from uniform distribution on the power levels, by symmetry, would allow the defender to take advantage of it. Also, note that in a low SNR scenarios where every frequency bin has low noise power compared to the total power of the receiver, then $|J| = N$ or the attacker will spread its power over all the frequency bins. Finally, the bins that will be used by the attackers will be those with the lowest noise power levels.

Fig. 2(a) illustrates two cases: (1) every frequency bin is used, and (2) some frequency bins are not used in the attack. In both cases, it is noted that the jammer tries to spread the power over the bins as evenly as possible. In turn, the defender also tries to spread the power evenly over every bin. These are optimal strategies for both cases.



(a)



(b)

Figure 2. Optimal power allocations of defender and attacker: (a) Perfect Information; (b) Defender-Biased.

Remark 2: In the real world, it is true that the jammer usually has limited information about the channel. However, one should not take a myopic view that all information is secure. Communication parameters can be leaked through other means (e.g., espionage). Furthermore, many educated guesses can be made about the satellite hardware and algorithms since most of this information is public. The point is that a sophisticated attacker, e.g., nation with large resources can potentially acquire this information. Thus, there is a need to analyze the perfect information scenario, i.e., the worst case scenario for the defender. Importantly, the existence of Nash equilibrium guarantees that the payoff for the attacker under this perfect information scenario is the best it can ever hope for. Thus, the defender can quantify the degree of damage for given communication parameters.

D. Defender-Biased Game

In this game, the attacker does not know the strategy of the defender. On the other hand, the defender knows the attacker's strategy and it knows that the attacker does not know its strategy. Being rational, the defender does not have to play the strategy $\mathbf{x}^* = \text{argmax}_{\mathbf{x} \in \mathcal{X}} \min_{\mathbf{y} \in]\mathcal{Y}} f(\mathbf{x}, \mathbf{y})$, since the strategy $\mathbf{x}^*$ is optimized for the worst case. Indeed, by knowing the attacker's strategy $\mathbf{y}$, the defender can achieve a higher payoff by playing the strategy as follows:

$$\mathbf{x}^* = \text{argmax}_{\mathbf{x}\in\mathcal{X}} \sum_{i=1}^{N} B\log\left(1+\frac{\mathbf{x}_i}{\mathbf{n}_i+\mathbf{y}_i}\right).$$

As previously derived in Eq. (7),

$$\mathbf{x}_i^* = \frac{(P_D+P_A+P_N)}{N} - \mathbf{y}_i - \mathbf{n}_i, i=1,2,\ldots,N. \quad (15)$$

If $\mathbf{x}_i^* < 0$ for some i, then set $\mathbf{x}_i^* = 0$, ignore the frequency bin i, and re-run the Lagrange multiplier method for the remaining $N-1$ frequency bins.

Now, consider the scenario when the attacker has no knowledge of the background noise and the defender's strategy. In this scenario, we propose the following:

Proposition 3. *If the attacker has no knowledge of the background noise and the defender's strategy, then the defender's optimal payoff is*

$$q_1^* = \sum_{i=1}^{|K|} B\log\left(1+\frac{\frac{P_D+P_N^K}{|K|}-\mathbf{n}_i}{\mathbf{n}_i+\frac{P_A}{N}}\right),$$

where K is the set of bin indexes used in the optimal strategy $\mathbf{x}^*$, $|K|$ is the cardinality of K, and P_N^K is the total noise power in $|K|$ bins used by the defender.

Proof. Without any information regarding the SNRs of the frequency bins or the defender's strategy, by the principle of insufficient reasons, the attacker would spread its power equally among N frequency bins by playing the strategy $\mathbf{y}_i = P_A/N$. Consequently, from Eq. (15), the defender will play the strategy that maximizes the payoff given $\mathbf{y}_i = P_A/N$ as

$$\begin{aligned}\mathbf{x}_i^* &= \frac{(P_D+P_A+P_N)}{N} - \frac{P_A}{N} \quad (16)\\ &- \mathbf{n}_i, i=1,2,\ldots,N.\\ &= \frac{P_D+P_N}{N} - \mathbf{n}_i,\end{aligned}$$

assuming that $\frac{P_D+P_N}{N} - \mathbf{n}_i > 0$. If for some frequency bin i, the positive power constraint is not satisfied, then the defender will ignore frequency bin i and re-run the optimization for the other remaining bins. Plugging in $\mathbf{x}^*$ and $\mathbf{y}_i = P_A/N$ into the payoff function, the optimal payoff of the defender can be obtained as

$$\begin{aligned}q_1^* &= \sum_{i=1}^{|K|} B\log\left(1+\frac{\mathbf{x}_i^*}{\mathbf{n}_i+\frac{P_A}{N}}\right) \quad (17)\\ &= \sum_{i=1}^{|K|} B\log\left(1+\frac{\frac{P_D+P_N^K}{|K|}-\mathbf{n}_i}{\mathbf{n}_i+\frac{P_A}{N}}\right).\end{aligned}$$

. □

Fig. 2(b) illustrates the power allocation of the jammer and the defender's strategies. In this scenario, the jammer simply allocates power uniformly at random over all frequency bins. On the other hand, the defender will try to equalize the power across all frequency bins as much as possible, given its power budget.

If the jammer does not know as much information as the defender, then it will not be able to play the Nash equilibrium strategy correctly. Thus, the defender will be able to take advantage of this and improve its own strategy to get a higher payoff. For instance, if the attacker does not have the exact information of noise distribution of the frequency bins, it randomly chooses some bins to allocate with more power, and other bins with less. As a result, the defender will be able to allocate more power to those less-corrupted channels and actually have a higher payoff. It turns out that, in the Defender-biased scenario, it is actually reasonable for the attacker to split its power budget evenly. Both our theoretical and simulation results show that a less-uniform noise channel (i.e, channel whose distribution noise power on the frequency is far from uniform distribution in terms of Kullback-Leibler (KL) distance will be more advantageous to the defender. That is, if the attacker's action makes the noise distribution over the channel less uniform, then the defender gains by putting more of its power in the less-corrupted frequency bins. As a result, the defender gets a better payoff. Intuitively, without any knowledge of the noise distribution, any non-uniform distribution of the attacker's power will be unwise, because it is very likely to bring more variance to the existing noise. A uniform power distribution, however, at least does not increase the difference of each channel. These cases are illustrated in Section V.

The game with Perfect Information scenario and the game with Defender Biased scenario are similar to the case of channel state information (CSI) being available at both transmitter (TX) and receiver (RX) and the case of CSI being available at only the RX in a multiple-input and multiple-output (MIMO) system. In this game, both the defender and the attacker can apply the water-filling strategy simultaneously when perfect information is available, whereas in the MIMO system, only the TX can apply the water-filling assuming the known ocean bottom level (i.e., the attacker plus noise level $\mathbf{y}_i + \mathbf{n}_i$ known to the MIMO TX). In the Defender-Biased game, only the defender can apply the water-filling strategy, whereas the attacker uses the equal power strategy. This is similar to the MIMO without CSI at TX, where the TX uses the equal power strategy because it has no information on the ocean bottom level.

E. Attacker-Biased Game

We now consider the Attacker-biased game. Here the attacker knows the defender's strategy, and it knows that the defender does not know its strategy. Similar to Section III-D, suppose the defender uses a strategy $\mathbf{x}$ that is known to the attacker; then a rational attacker will try to minimize the payoff, i.e., information rate using

$$\mathbf{y} = \text{argmin}_{\mathbf{y}\in\mathcal{Y}} \sum_{i=1}^{N} B\log\left(1+\frac{\mathbf{x}_i}{\mathbf{n}_i+\mathbf{y}_i}\right).$$

Since B is a constant, it is equivalent to minimizing the function $f(\mathbf{x},\mathbf{y}) = \sum_{i=1}^{N}\log\left(1+\frac{\mathbf{x}_i}{\mathbf{n}_i+\mathbf{y}_i}\right)$. Using the Lagrange multiplier method, similar to Section III-C yields

$$\frac{\mathbf{x}_i}{(\mathbf{n}_i+\mathbf{y}_i+\mathbf{x}_i)(\mathbf{n}_i+\mathbf{y}_i)} = \lambda. \quad (18)$$

Letting $\mathbf{z}_i = \mathbf{n}_i + \mathbf{y}_i$ and solving for $\mathbf{z}_i$ yields

$$\begin{aligned} \mathbf{z}_i &= \mathbf{n}_i + \mathbf{y}_i \\ &= \frac{-\lambda \mathbf{x}_i + \sqrt{\lambda^2 \mathbf{x}_i^2 + 4\mathbf{x}_i\lambda}}{2\lambda}. \end{aligned} \tag{19}$$

Equivalently, the optimal strategy for the attacker is

$$\mathbf{y}_i' = \frac{-\lambda \mathbf{x}_i + \sqrt{\lambda^2 \mathbf{x}_i^2 + 4\mathbf{x}_i\lambda}}{2\lambda} - \mathbf{n}_i. \tag{20}$$

However, we do not know λ. The following procedure is used to search for λ using an upper and a lower bound computed as follows. First, we note that by summing the left- and right-hand sides of Eq. (18),

$$\lambda = \frac{\sum_i \mathbf{x}_i}{\sum_i \left((\mathbf{n}_i + \mathbf{y}_i + \mathbf{x}_i)(\mathbf{n}_i + \mathbf{y}_i)\right)} \tag{21}$$

$$\geq \frac{P_D}{\sum_i (\mathbf{n}_i + \mathbf{y}_i + \mathbf{x}_i) \sum_i (\mathbf{n}_i + \mathbf{y}_i)} \tag{22}$$

$$= \frac{P_D}{(P_A + P_D + P_N)(P_N + P_A)}, \tag{23}$$

where Eq. (22) is due to Schwartz's inequality. Now an upper bound for λ can be found as follows:

$$\lambda = \frac{\sum_i \mathbf{x}_i}{\sum_i \left((\mathbf{x}_i + \mathbf{n}_i + \mathbf{y}_i)(\mathbf{n}_i + \mathbf{y}_i)\right)} \tag{24}$$

$$\leq \frac{P_D}{\sum_i (\mathbf{n}_i + \mathbf{y}_i)^2} \tag{25}$$

$$\leq \frac{P_D}{\sum_i \mathbf{n}_i^2 + \sum_i \mathbf{y}_i^2} \tag{26}$$

$$\leq \frac{P_D}{\frac{(\sum_i \mathbf{n}_i)^2}{N} + \frac{(\sum_i \mathbf{y}_i)^2}{N}} \tag{27}$$

$$= \frac{NP_D}{P_A^2 + P_N^2}, \tag{28}$$

where N is the number of the frequency bin used for jamming. We note that Eq. (27) is due to the well-known bound for l_1-norm and l_2-norm.

Next, an algorithm that performs the search for λ over these bounds is proposed. For each value of λ, $\mathbf{y}'$ is computed using inequality (20); then $\mathbf{y}'$ is checked to see if it satisfies all power constraints.

Proposition 4. *Let $f(\lambda) = \sum_{i=1}^{N} \mathbf{y}_i$. Then $f(\lambda)$ is monotonically decreasing in λ within the interval specified by inequality (28) and inequality (23).*

Proof. See Appendix B. □

Based on Proposition 4, a binary search algorithm with the complexity of $\log(n)$ can be used to find λ efficiently, where n is the number of partition in the search space. In our specific scenario, since we are searching for the right value of λ, if we want the value of λ to be within ϵ of the optimal value, then we can set $n = O(1/\epsilon)$. The algorithm is as follows:

while $|P_A - f(\lambda)| > \epsilon$ **do**
  if $P_A - f(\lambda) > 0$ **then**
    $\lambda_{upper} = \lambda$
  else
    $\lambda_{lower} = \lambda$
  end if
  $\lambda = (\lambda_{lower} + \lambda_{upper})/2$
end while

Then, the best strategy for the attacker $\mathbf{y}_i'$ can be found by Eq. (20).

IV. Extension to Continuous Spread-Spectrum Jamming

In this section, we extend the satellite jamming attack settings from a setting consisting of finite discrete frequency bins to the setting where signals are spread in a continuous spectrum, i.e., an uncountable infinite number of frequency bins. In particular, we will focus on the problem from the defender's perspective in a Defender-biased game.

A. Problem Formulation

To provide a brief background, we first consider the discrete time i.i.d. white Gaussian channel modeled as:

$$\mathbf{r}_i = \mathbf{s}_i + \mathbf{w}_i,$$

where $\mathbf{w}_i \sim N(0, \sigma_N^2)$ denotes the noise with average power σ_N^2, $\mathbf{s}_i$ denotes the transmitted signal, and $\mathbf{r}_i$ denotes the received signal. Furthermore, we assume that

$$\sum_{i=1}^{N} \mathbf{s}_i^2 \leq NP,$$

where P denotes the average power of a transmitted signal. It is well-known that the capacity for this channel is

$$C = \frac{1}{2} \log\left(1 + \frac{P}{\sigma_N^2}\right).$$

Furthermore, the capacity is achieved when

$$\mathbf{s}_i \sim N(0, P). \tag{29}$$

Consequently, we also have

$$\mathbf{r}_i \sim N(0, P + \sigma_N^2). \tag{30}$$

Now, we turn our attention to modeling the game. From the defender's point of view, the sum of the attacker signal and the background noise signal can be treated as one single noise signal with the total power as

$$\sigma_N^2 = P_A + P_N.$$

The strategies of the defender and the attacker are no longer sets of discrete power levels on each frequency bin. Rather, their strategies are to find the power spectrum of their signal so that the payoff functions are maximized. Specifically, in a Defender-biased game, if we denote the power spectral density of the defender and the total noise as $S(\omega)$ and $Z(\omega)$, respectively, the defender intends to find $S(\omega)$ to maximize the following payoff:

$$C = \frac{1}{2} \int_{-B/2}^{B/2} \log\left(1 + \frac{S(\omega)}{Z(\omega)}\right) d\omega. \tag{31}$$

B. Defender-Biased Game with Continues Spread-Spectrum

Proposition 5. *To maximize the payoff described in Eq.* (31)*, the power spectral density of the defender $S(\omega)$ is*

$$S(\omega) = \max(P + \sigma_N^2 - Z(\omega), 0),$$

where $Z(\omega)$ are the power spectral density of the total noise. Thus, the optimal payoff is

$$C = \frac{1}{2}\int_{-B/2}^{B/2} \log\left(1 + \frac{\max(P + \sigma_N^2 - Z(\omega), 0)}{Z(\omega)}\right) d\omega.$$

Proof. Consider in the discrete case, the covariance matrices of the transmitted signal $\mathbf{s}_i$ and the noise $\mathbf{z}_i$, which is sum of the attacker's signal and noise signal. We will show that these covariance matrices are directly related to the spectrum of the transmitted and noise signals when $N \longrightarrow \infty$. Let $\mathbf{s} = \{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_N\}$ be the vector denoting the transmitted signal, $\mathbf{z} = \{\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_N\}$ be the vector denoting the sum of noise and the attacker signal, and $\mathbf{r} = \{r_1, r_2, \ldots, r_N\}$ be the vector denoting the received signal. Then we have the following channel:

$$\mathbf{r} = \mathbf{s} + \mathbf{z}, \tag{32}$$

where $\mathbf{z}_i$ may not be independent.

Given the covariance matrix $\mathbf{K}_{zz}$ of the noise signal, the defender will try to find the covariance matrix $\mathbf{K}_{ss}$ of the transmitted signal such that it maximizes the capacity. We proceed as follows. We have

$$\begin{aligned} \mathbf{K}_{zz} &= E[\mathbf{z}\mathbf{z}^T] \\ \mathbf{K}_{ss} &= E[\mathbf{s}\mathbf{s}^T]. \end{aligned}$$

Since $\mathbf{K}_{zz}$ is a symmetric matrix, performing eigenvalue decomposition yields

$$\mathbf{K}_{zz} = \mathbf{Q}\mathbf{D}\mathbf{Q}^T,$$

where $\mathbf{D}$ is a diagonal matrix, whose diagonal entries are non-zero eigenvalues, and $\mathbf{Q}$ is the matrix whose columns are eigenvectors; thus, $\mathbf{Q}\mathbf{Q}^T = \mathbf{I}$. Next, multiplying Eq. (32) by $\mathbf{Q}^T$ yields

$$\mathbf{Q}^T\mathbf{r} = \mathbf{Q}^T\mathbf{s} + \mathbf{Q}^T\mathbf{z}. \tag{33}$$

Let $\mathbf{w} = \mathbf{Q}^T\mathbf{z}$, then

$$\begin{aligned} \mathbf{K}_{ww} &= E[\mathbf{w}\mathbf{w}^T] \\ &= E[\mathbf{Q}^T\mathbf{z}\mathbf{z}^T\mathbf{Q}] \\ &= \mathbf{Q}^T\mathbf{K}_{zz}\mathbf{Q} \\ &= \mathbf{D}. \end{aligned}$$

Therefore, $\mathbf{w}_i$ are independent. We also note that the power constraint of the signal $\mathbf{Q}^T\mathbf{s}$ and $\mathbf{s}$ are the same since

$$\begin{aligned} tr(E[\mathbf{Q}^T\mathbf{s}\mathbf{s}^T\mathbf{Q}]) &= tr(\mathbf{Q}^T\mathbf{K}_{ss}\mathbf{Q}) \\ &= tr(\mathbf{K}_{ss}\mathbf{Q}\mathbf{Q}^T) \\ &= tr(\mathbf{K}_{ss}) \\ &= NP. \end{aligned} \tag{34}$$

Since $\mathbf{w}_i$ are independent, based on the well-known capacity of additive white noise channel (Eqs. (29) and (30)), each component of $\mathbf{v} = Q^T\mathbf{s}$ must have independent Gaussian distribution. Similarly, each component of the corresponding $\mathbf{u} = Q^T\mathbf{r}$ must also have independent Gaussian distribution. Using this condition, multiplying Eq. (33) by $\mathbf{u}^T$, and taking the expectation on both sides yields

$$\begin{aligned} E[\mathbf{u}\mathbf{u}^T] &= E[(\mathbf{Q}^T\mathbf{s} + \mathbf{w})(\mathbf{Q}^T\mathbf{s} + \mathbf{w})^T] \\ &= \mathbf{Q}\mathbf{K}_{ss}\mathbf{Q}^T + \mathbf{K}_{ww} \\ &= \mathbf{Q}\mathbf{K}_{ss}\mathbf{Q}^T + \mathbf{D}. \end{aligned} \tag{35}$$

Thus,

$$\mathbf{K}_{ss} = \mathbf{Q}^T(\mathbf{K}_{uu} - \mathbf{D})\mathbf{Q}. \tag{36}$$

Since $\mathbf{u}_i$ are independent, or $\mathbf{K}_{uu}$ is a diagonal matrix, choosing

$$\mathbf{K}_{uu} = \left(P + \frac{tr(\mathbf{D})}{N}\right)\mathbf{I},$$

yields $tr(\mathbf{K}_{ss}) = NP$, which satisfies the power constraint. Therefore, the optimal transmitted signal $\mathbf{s}$ for the defender should have its covariance matrix as

$$\mathbf{K}_{ss} = \mathbf{Q}^T\left(\left(P + \frac{tr(\mathbf{D})}{N}\right)\mathbf{I} - \mathbf{D}\right)\mathbf{Q}.$$

Here we assume that the defender knows the covariance matrix of the sum of background noise and the attacker, and thus can compute the optimal $\mathbf{K}_{ss}$.

Now, we turn our attention to the continuous spectrum. If $\mathbf{z}$ is wide-sense stationary, then for $N \longrightarrow \infty$, the diagonal entries of $\mathbf{D}$ are indeed the power spectrum of $\mathbf{z}$. Thus, using the water-filling argument discussed in the previous section, the optimal spectrum of $\mathbf{s}$ would be

$$S(\omega) = \max(P + W(\omega) - Z(\omega), 0),$$

where $S(\omega)$, $W(\omega)$, and $Z(\omega)$ are the power spectral densities of $s(t)$, $w(t)$, and $z(t)$, respectively. Note that $W(\omega) = \sigma_N^2$. The corresponding optimal payoff (transmission rate) is

$$C = \frac{1}{2}\int_{-B/2}^{B/2} \log\left(1 + \frac{\max(P + W(\omega) - Z(\omega), 0)}{Z(\omega)}\right) d\omega.$$

□

V. Simulation Results

In this simulation, ten bins with an identical bandwidth of 3 kbps are used. Assume that the defender can deliver -120 dBW at the satellite relay, and the jamming attacker can deliver half of the power, i.e., -123 dbW. The total noise power is described by $SNR = P_D/P_N$.

In a real-world scenario, the attacker can use any strategy it wants. However, the attacker will inevitably do less damage to the defender with any strategy that deviates from its Nash equilibrium strategy, one that assumes both defender and attacker have perfect information about the game. To illustrate this point, Fig. 3 shows what happens if one player decides to change to some other strategy. In this case, SNR is fixed at $10dB$, and noise distribution is quantified by the *concentration index (CI)*. One bin is randomly picked, and the CI indicates the average percentage of P_N that is confined in this specific bin. In this case, when $N = 10$, $CI = 0.1$ indicates a "flat" distribution, while a higher CI indicates

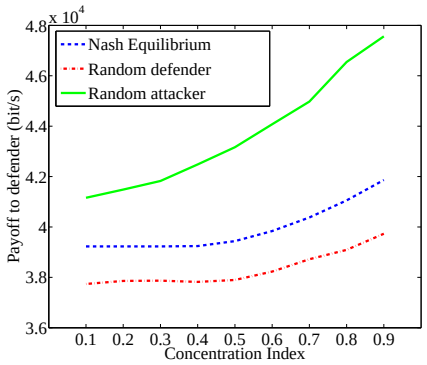


Figure 3. Illustration of Nash equilibrium

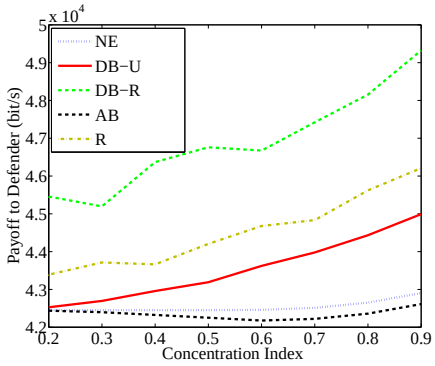


Figure 4. Payoff (rate) for scenarios under different noise distributions

a more highly-concentrated one. If the defender decides to move to some other strategy while the attacker plays its NE strategy, the defender reduces its payoff as shown by the red curve. Similarly, if the attacker changes its strategy while the defender stays with its NE strategy, the payoff to the defender becomes higher as shown by the green curve, i.e., the attacker reduces its payoff since this is a zero-sum game. As a result, at the NE, both players have no motivation to move to other strategies, and the payoff is shown by the blue curve.

Fig. 4 shows the payoff comparison for all scenarios. Five different scenarios are considered here:

- Perfect information Nash equilibrium (NE)
- Defender-biased scenario with the attacker uniformly distributing its power (DB-U): Attacker distributes its power equally to each frequency bins.
- Defender-biased scenario with the attacker randomly distributing its power (DB-R): Attacker distributes its power for each bin following the uniform distribution in $[0.25\frac{P_A}{N}, 1.75\frac{P_A}{N}]$.
- Attacker-biased scenario (AB): Defender does not know the existence of the attacker. As a result, the defender allocates its power by maximizing its capacity only according to the noise distribution.
- Random scenario (R): Defender's power allocation follows uniform distribution $[0.25\frac{P_N}{N}, 1.75\frac{P_N}{N}]$, and the attacker's power allocation follows uniform distribution $[0.25\frac{P_A}{N}, 1.75\frac{P_A}{N}]$

Comparing the DB-U and the NE scenario, the noise powers in the channels become less uniform as the CI increases, and the defender will have more advantage since it can adjust its power allocation accordingly. On the other hand, the attacker wants to make the channel as even as possible in order to "cancel out" the advantage of the defender. As expected, Fig. 4 shows that in these two scenarios, the defender can obtain a higher rate when the noise powers in the channels become less uniform. Furthermore, the information rate in the Defender-biased scenario is always higher than that of the Perfect Information scenario, as expected. The curve is flat when $CI < 0.6$, indicating the filling effect introduced by the attacker. When the channel noise is more uniform across the frequency bins, the attacker is able to fill the gap between channels with its limited power budget. Thus, the defender's gain stays constant by the attacker's filling. However, if the attacker has no idea about how the channel noise is distributed, an evenly distributed jamming power will hardly decrease the extent of variation in power for each channel. As a result, in the DB-U case, the payoff keeps increasing as the CI increases.

Comparing the AB and the NE scenarios, it is assumed that the defender always knows the channel conditions and distributes its power accordingly, but the defender does not know the existence of the attacker. As the CI increases, the attacker becomes more effective because of the increase in variation of power across the frequency bins. The attacker can distribute power according to the defender's action in order to achieve optimality. However the attacker's gain stops increasing at some value of CI. This is because from this point on, both attacker and defender discard the most noisy channel, and there will be no further change of variation.

Comparing the DB-U and DB-R scenarios, it is obvious that without the channel condition, if the attacker decides to use a randomly distributed power allocation, then the defender will be able to gain a large advantage. Even in the R scenario, where the defender uses a random strategy instead of an optimized strategy, the attacker may still get a payoff that is worse than the DB-U case. As we discussed in Section III-D, this result is not surprising. When the channel condition is not available, a random strategy of the attacker will be very likely to make the noise distribution in the frequency bins less uniform. As a result, the defender is able to take advantage of this and applies more power on those less noisy bins. If the attacker allocates its power evenly, then it at least will not increase the power differences in each bin.

Fig. 5 further illustrates the attacker's ability to flatten the noise distribution among the bins, thus eliminating the advantage of variation for defenders. In this case, P_A and P_D are fixed, while the noise power increases from $SNR = 12.5dB$ to $5dB$. In both the perfect information and Defender-biased scenarios, the overall performance decreases as the SNR decreases. In Fig. 5(a), when the noise power is sufficiently small ($12.5dB$), the attacker is able to fill the gaps, regardless of the channel condition variation. In this case, the defender has no benefit, even when CI is large. As the noise power increases, the attacker will no longer be able to cover the variation at some points, and the benefit of the defender happens earlier when CI increases. However, as shown in Fig. 5(b), in the Defender-biased scenario, the attacker never flatten the channel. As a result, benefits for the defender always

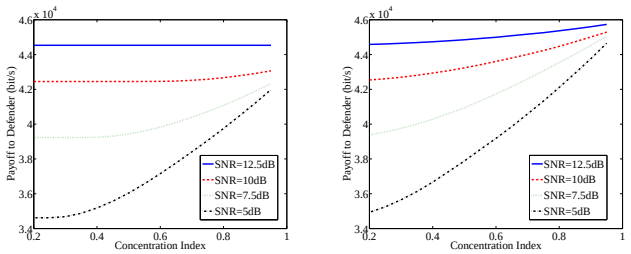


Figure 5. (a) Defender payoff (rate) in perfect information scenario; (b) in Defender-biased scenario.

exists.

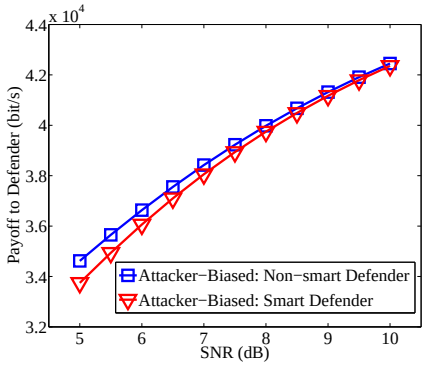


Figure 6. Performance comparison of different types of defenders.

Fig. 6 compares two different kinds of defender behavior in the Attacker-biased case. A "smart defender" distributes its power among the bins according to channel conditions, while a "non-smart defender" simply distributes power evenly. Notice that the AB scenario defined above is actually a smart defender. The result is plotted when $CI = 0.2$. It is interesting to see that in this specific scenario, a "non-smart defender" always performs better! When the "smart defender" distributes the power according to channel condition, the result is more varied. As a result, the attacker's advantage becomes even larger. In fact, Eq. (20) shows that for a "non-smart defender", the attacker can do nothing more than "flatten" the variation of the channel noise, which is the same as in the perfect information case.

Fig. 7 shows the defender payoff when the noise distribution is fixed among ten bins. In this case, 75% of the noise power is concentrated in three bins. As expected, in all scenarios, performance increases as the SNR increases. At any SNR, the two Defender-biased scenarios (DB-R and DB-U) always have better performance compared to the other two. It is obvious that the DB-R scenario will provide more advantages to the defender because of the extra variance due to the randomness of the attacker. The NE scenario comes third, and the AB scenario is the worst. Differences among the DB-U, NE, and AB scenarios decrease when the SNR increases. Given a fixed distribution of noise across the bins, the absolute difference between a bad channel and a good channel is small when the SNR is large. As a result, the defender/attacker does not have a huge benefit when given the information advantage, and their power is distributed almost evenly at the end.

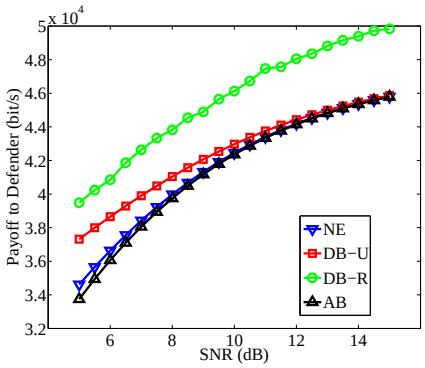


Figure 7. Comparison of all scenarios for different SNRs.

VI. Conclusion

In this paper, the FH satellite jamming attack is modeled as a zero-sum game. Specifically, the spread-spectrum attack is introduced, and the existence of NE is shown. Furthermore, analytical results on the perfect information game, Defender-biased game, and Attacker-biased game are provided. Both theoretical analysis and intuitions agree with the simulated performance results of each scenario under different channel conditions.

VII. Acknowledgment

This work was supported in part by the U.S. Air Force Summer Faculty Fellowship Program. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing official policies or endorsements, either expressed or implied, of the AFRL or the U.S. government.

Appendix A
Proof of Proposition 1

Proof. It will be shown that the Hessian $\nabla^2_{\mathbf{x}} f(\mathbf{x},\mathbf{y})$ is a semi-definite positive matrix (equivalently, its eigenvalues are greater than or equal to 0) for any given $\mathbf{x}$; thus $f(\mathbf{x},\mathbf{y})$ is convex in $\mathbf{y}$. Similarly, we will show that $\nabla^2_{\mathbf{y}} f(\mathbf{x},\mathbf{y})$ is a semi-definite negative matrix (equivalently, its eigenvalues are less than or equal to zero) for any given $\mathbf{y}$; thus $f(\mathbf{x},\mathbf{y})$ is concave in $\mathbf{x}$. The proof of Proposition 1 immediately follows using Theorem 1.

First note that

$$\nabla^2_{\mathbf{x}} f(\mathbf{x},\mathbf{y}) = \begin{bmatrix} \frac{\partial^2 f(\mathbf{x},\mathbf{y})}{\partial^2 \mathbf{y}_1} & \frac{\partial^2 f(\mathbf{x},\mathbf{y})}{\partial \mathbf{y}_1 \partial \mathbf{y}_2} & \cdots & \frac{\partial^2 f(\mathbf{x},\mathbf{y})}{\partial \mathbf{y}_1 \partial \mathbf{y}_N} \\ \frac{\partial^2 f(\mathbf{x},\mathbf{y})}{\partial \mathbf{y}_2 \partial \mathbf{y}_1} & \frac{\partial^2 f(\mathbf{x},\mathbf{y})}{\partial^2 \mathbf{y}_2}, & \cdots & \frac{\partial^2 f(\mathbf{x},\mathbf{y})}{\partial \mathbf{y}_2 \partial \mathbf{y}_N} \\ \cdots & \cdots & \cdots & \\ \frac{\partial^2 f(\mathbf{x},\mathbf{y})}{\partial \mathbf{y}_n \partial \mathbf{y}_1} & \frac{\partial^2 f(\mathbf{x},\mathbf{y})}{\partial \mathbf{y}_n \partial \mathbf{y}_{N-1}}, & \cdots & \frac{\partial^2 f(\mathbf{x},\mathbf{y})}{\partial^2 \mathbf{y}_N}. \end{bmatrix}$$

With $f(\mathbf{x},\mathbf{y}) = \frac{1}{2}\sum_{i=1}^{N} B \log\left(1 + \frac{\mathbf{x}_i}{\mathbf{n}_i + \mathbf{y}_i}\right)$,

$$\frac{\partial f}{\partial \mathbf{y}_i} = -\frac{B\mathbf{x}_i}{2(\mathbf{n}_i+\mathbf{y}_i+\mathbf{x}_i)(\mathbf{n}_i+\mathbf{y}_i)}$$
$$\frac{\partial^2 f}{\partial \mathbf{y}_i \partial \mathbf{y}_j} = \begin{cases} \frac{B\mathbf{x}_i(2\mathbf{n}_i+2\mathbf{y}_i+\mathbf{x}_i)}{2((\mathbf{n}_i+\mathbf{y}_i+\mathbf{x}_i)(\mathbf{n}_i+\mathbf{y}_i))^2} & i=j \\ 0 & i\neq j. \end{cases}$$

Since B and $\mathbf{x}_i$ are greater than or equal to zero, $\nabla^2_{\mathbf{x}} f(\mathbf{x},\mathbf{y})$ is a diagonal matrix whose eigenvalues (diagonal entries) are greater than or equal to zero, or equivalently, $\nabla^2_{\mathbf{x}} f(\mathbf{x},\mathbf{y})$ is a semi-definite positive matrix.

Similarly, for a fixed $\mathbf{y}$, it can be shown that

$$\frac{\partial f}{\partial \mathbf{x}_i} = \frac{B}{2(\mathbf{n}_i+\mathbf{y}_i+\mathbf{x}_i)}$$
$$\frac{\partial^2 f}{\partial \mathbf{x}_i \partial \mathbf{x}_j} = \begin{cases} -\frac{B}{2(\mathbf{n}_i+\mathbf{y}_i+\mathbf{x}_i)^2} & i=j. \\ 0 & i\neq j. \end{cases}$$

Thus, $\nabla^2_{\mathbf{y}} f(\mathbf{x},\mathbf{y})$ is a diagonal matrix whose eigenvalues (diagonal entries) are less than or equal to zero. Equivalently, $\nabla^2_{\mathbf{y}} f(\mathbf{x},\mathbf{y})$ is a semi-definite negative matrix.

□

APPENDIX B
PROOF OF PROPOSITION 4

Proof. From Eq. (20), $f(\lambda)$ can be expressed as

$$f(\lambda) = \sum_{i=1}^{N} \left(\frac{-\lambda\mathbf{x}_i + \sqrt{\lambda^2\mathbf{x}_i^2 + 4\mathbf{x}_i\lambda}}{2\lambda} - \mathbf{n}_i \right)$$

Denote

$$f(\lambda)_i = \frac{-\lambda\mathbf{x}_i + \sqrt{\lambda^2\mathbf{x}_i^2 + 4\mathbf{x}_i\lambda}}{2\lambda} - \mathbf{n}_i$$
$$= \frac{-\mathbf{x}_i + \sqrt{\mathbf{x}_i^2 + 4\mathbf{x}_i/\lambda}}{2} - \mathbf{n}_i.$$

Then,

$$\frac{\partial f(\lambda)_i}{\partial \lambda} = \frac{\partial}{\partial \lambda}\left(\frac{-\mathbf{x}_i + \sqrt{\mathbf{x}_i^2 + 4\mathbf{x}_i/\lambda}}{2} - \mathbf{n}_i \right)$$
$$= \frac{\partial}{\partial \lambda}\left(\frac{-\mathbf{x}_i + \sqrt{\mathbf{x}_i^2 + 4\mathbf{x}_i/\lambda}}{2} \right)$$
$$= \frac{\partial}{\partial \lambda}\left(\frac{\sqrt{\mathbf{x}_i^2 + 4\mathbf{x}_i/\lambda}}{2} \right).$$

It is obvious that $\sqrt{\mathbf{x}_i^2 + 4\mathbf{x}_i/\lambda}$ is monotonically decreasing in λ, that is

$$\frac{\partial f(\lambda)_i}{\partial \lambda} = \frac{\partial}{\partial \lambda}\left(\frac{\sqrt{\mathbf{x}_i^2 + 4\mathbf{x}_i/\lambda}}{2} \right)$$
$$\leq 0.$$

Thus,

$$\frac{\partial f(\lambda)}{\partial \lambda} = \sum_{i=1}^{N} \frac{\partial f(\lambda)_i}{\partial \lambda}$$
$$\leq 0$$

□

REFERENCES

[1] B. Reiffen and H. Sherman, "Parametric analysis of jammed active satellite links," *IEEE Transactions on Communications Systems*, vol. 12, no. 1, pp. 102–103, March 1964.

[2] H. Rausch, "Jamming commercial satellite communications during wartime: An empirical study," in *Proceedings of the Fourth IEEE International Workshop on Information Assurance*, ser. IWIA '06. Washington, DC, USA: IEEE Computer Society, 2006, pp. 109–118. [Online]. Available: http://dx.doi.org/10.1109/IWIA.2006.15

[3] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*. ACM, 2005, pp. 46–57.

[4] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, May 2006.

[5] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, May 2007, pp. 1307–1315.

[6] T. M. Cover and J. A. Thomas, *The Gaussian Channel*. John Wiley and Sons, Inc., 2001, pp. 239–265. [Online]. Available: http://dx.doi.org/10.1002/0471200611.ch10

[7] M. Hannon, S. Feng, H. Kwon, and K. Pham, "Jamming statistics-dependent frequency hopping," in *IEEE Military Communications Conf.*, Nov 2016.

[8] L.-M. Li and L. Milstein, "Rejection of narrow-band interference in pn spread-spectrum systems using transversal filters," *IEEE Transactions on Communications*, vol. 30, no. 5, pp. 925–928, May 1982.

[9] K. C. Teh, C. C. Teng, A. C. Kot, and K. H. Li, "Jammer suppression in spread spectrum," in *Networks, 1995. Theme: Electrotechnology 2000: Communications and Networks. [in conjunction with the] International Conference on Information Engineering., Proceedings of IEEE Singapore International*, Jul 1995, pp. 220–224.

[10] P. Martinelli, E. Cianca, M. D. Sanctis, L. D. Paolo, A. Pisano, and L. Simone, "Robustness of satellite telecommand links to jamming attacks," in *2012 IEEE First AESS European Conference on Satellite Telecommunications (ESTEL)*, Oct 2012, pp. 1–6.

[11] C. l. Chang, "Multiplexing scheme for anti-jamming global navigation satellite system receivers," *IET Radar, Sonar Navigation*, vol. 6, no. 6, pp. 443–457, July 2012.

[12] D. Wang, J. Li, W. Gong, and S. Wu, "Attitude aided space-time multi-beamformer anti-jamming approach for satellite navigation receiver," in *2014 12th International Conference on Signal Processing (ICSP)*, Oct 2014, pp. 368–372.

[13] P. T. Capozza, B. J. Holland, T. M. Hopkinson, and R. L. Landrau, "A single-chip narrow-band frequency-domain excisor for a global positioning system (gps) receiver," *IEEE Journal of Solid-State Circuits*, vol. 35, no. 3, pp. 401–411, March 2000.

[14] K. Kim, M. Lee, and J. Lim, "Spreading technique of satellite beacon to avoid jamming attacks," in *Advanced Communication Technology (ICACT), 2012 14th International Conference on*. IEEE, 2012, pp. 778–781.

[15] M. K. Hanawal, D. N. Nguyen, and M. Krunz, "Jamming attack on in-band full-duplex communications: Detection and countermeasures," in *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, April 2016, pp. 1–9.

[16] W. Dai, C. Qiao, Y. Wang, and C. Zhou, "Improved anti-jamming scheme for direct-sequence spread-spectrum receivers," *Electronics Letters*, vol. 52, no. 2, pp. 161–163, 2016.

[17] K. Gai, M. Qiu, Z. Ming, H. Zhao, and L. Qiu, "Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2431–2439, Sept 2017.

[18] K. Gai, L. Qiu, M. Chen, H. Zhao, and M. Qiu, "Sa-east: Security-aware efficient data transmission for its in mobile heterogeneous cloud computing," *ACM Trans. Embed. Comput. Syst.*, vol. 16, no. 2, pp. 60:1–60:22, Jan. 2017. [Online]. Available: http://doi.acm.org/10.1145/2979677

[19] J. F. Nash, "Equilibrium points in n-person games," *Proceedings of the National Academy of Sciences*, vol. 36, no. 1, pp. 48–49, 1950. [Online]. Available: http://www.pnas.org/content/36/1/48.short

[20] S. Roy, L. Wu, and M. Zawodniok, "Spectrum management for wireless networks using adaptive control and game theory," in *2011 IEEE Wireless Communications and Networking Conference*, March 2011, pp. 1062–1067.

[21] J. Park and M. van der Schaar, "The theory of intervention games for resource sharing in wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 1, pp. 165–175, January 2012.
[22] B. Zhang and L. Lai, "Optimal strategies in jamming resistant uncoordinated frequency hopping systems," in *2013 47th Annual Conference on Information Sciences and Systems (CISS)*, March 2013, pp. 1–6.
[23] M. K. Hanawal, M. J. Abdel-Rahman, and M. Krunz, "Game theoretic anti-jamming dynamic frequency hopping and rate adaptation in wireless systems," in *2014 12th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, May 2014, pp. 247–254.
[24] M. J. Abdel-Rahman and M. Krunz, "Game-theoretic quorum-based frequency hopping for anti-jamming rendezvous in dsa networks," in *2014 IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)*, April 2014, pp. 248–258.
[25] W. Xu, W. Trappe, and Y. Zhang, "Anti-jamming timing channels for wireless networks," in *Proceedings of the First ACM Conference on Wireless Network Security*, ser. WiSec '08. New York, NY, USA: ACM, 2008, pp. 203–213. [Online]. Available: http://doi.acm.org/10.1145/1352533.1352567
[26] D. Yang, J. Zhang, X. Fang, A. Richa, and G. Xue, "Optimal transmission power control in the presence of a smart jammer," in *2012 IEEE Global Communications Conference (GLOBECOM)*, Dec 2012, pp. 5506–5511.
[27] D. Yang, G. Xue, J. Zhang, A. Richa, and X. Fang, "Coping with a smart jammer in wireless networks: A stackelberg game approach," *IEEE Transactions on Wireless Communications*, vol. 12, no. 8, pp. 4038–4047, August 2013.
[28] S. D'Oro, L. Galluccio, G. Morabito, S. Palazzo, L. Chen, and F. Martignon, "Defeating jamming with the power of silence: A game-theoretic analysis," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2337–2352, May 2015.
[29] T. Cover and J. Thomas, *Elements of information theory*, 2nd ed. Wiley-Interscience, 7 2006.
[30] E. Altman, K. Avrachenkov, and A. Garnaev, "A jamming game in wireless networks with transmission cost," in *Proceedings of the 1st EuroFGI International Conference on Network Control and Optimization*, ser. NET-COOP'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 1–12. [Online]. Available: http://dl.acm.org/citation.cfm?id=1762948.1762949
[31] J. v. Neumann, "Zur theorie der gesellschaftsspiele," *Mathematische Annalen*, vol. 100, pp. 295–320, 1928. [Online]. Available: http://eudml.org/doc/159291

PLACE PHOTO HERE

Qiwei Wang Biography text here.

PLACE PHOTO HERE

Thinh Nguyen Biography text here.

PLACE PHOTO HERE

Khanh Pham Biography text here.

PLACE PHOTO HERE

Hyuck Kwon Biography text here.