# Securing Space Communication Systems Against Reactive Cognitive Jammer

Danda B. Rawat[‡] and Min Song[†]
[‡]Department of Electrical Engineering. Georgia Southern University, Statesboro, GA, USA. E-mail: db.rawat@ieee.org.
[†]Department of Computer Science, Michigan Technological University, Houghton, MI, USA. E-mail: MinS@mtu.edu.

***Abstract*—In this paper, we propose an anti-jamming game for space communication systems where a cognitive jammer reactively senses channels using energy detection and jams the channel using "detect and jam" strategy while the legitimate transmitter-receiver pair uses a joint frequency hopping and power/rate adaptation approach to avoid the impact of the jamming. Jamming and anti-jamming process between legitimate satellite link and a jammer is formulated as a zero-sum game. The proposed game takes into account of the signal propagation delay, detection performance (signal detection and jamming start time) of a jammer, received jamming power from the jammer, and hopping and jamming costs. Performance of the proposed approach is evaluated with the help of simulations and the proposed approach outperforms other existing methods.**

## I. Introduction

Wireless networks are vulnerable to different types of attacks including jamming attacks. In a jamming attack, an adversary jams a channel by injecting a signal with enough power to block legitimate communication to (i) degrade the carrier-to-interference-plus-noise-ratio (CINR)[1] at the intended receiver and/or (ii) make denial-of-communication for legitimate users [1]. Frequency hopping is regarded as an anti-jamming technique for jamming attacks. Frequency hopping can be accomplished either $proactively$ or $reactively$. In a proactive frequency-hopping [2], transmitter and its receiver hop to new frequency based on their shared hopping sequences that is previously agreed upon, while in a reactive frequency-hopping [3], transmitter and its receiver hop to a new channel when they detect jamming in the current channel. In traditional wireless networks, different approaches have been proposed for anti-jamming such as spread spectrum (e.g., [4]) in physical layer, frequency hopping (e.g., [5], [6]) in link layer, and random linear coding based anti-jamming (e.g., [7]) in network layer. Due to the advances in cognitive radio technology, attackers are becoming more intelligent making the anti-jamming process more complex and difficult. An attacker with cognitive radio capabilities can use "detect and jam" strategies by reactively sensing wireless channels and transmitting a jamming signal with enough power to jam active channels.

Frequency hopping technique avoids jamming attacks to get high throughput [5], [8]–[13]. However, if a frequency hopping sequence is totally random, the transmitter and its receiver may not be able to meet (rendezvous) in the hopped channel within a bounded time to exchange pending messages. When the frequency hopping sequence is pre-shared between the transmitter and its receiver, the rendezvous process is easy. However, an internal jammer or a jammer with cognitive capabilities can easily recognize the hopping sequence and chase the hopping pattern to jam the channels. Furthermore, traditional common control channel (CCCH) based coordination methods for frequency hopping are always vulnerable to jamming attacks [5], [13] since fixed CCCH can be easily jammed by the jammer. Therefore, it is necessary to design a robust, resilient and effective mechanism to detect and avoid jamming attacks to provide uninterrupted service for legitimate wireless users.

In [9], [10], Markov Decision Process and game theory have been proposed to avoid jamming in cognitive radio networks. In [13], cognitive jamming problem is investigated for satellite communications using sliding window based jam detection mechanism. In [11], anti-jamming game is presented to minimize the worst-case damage caused by attackers. However, none of these existing works consider the delay for signal detection and propagation, and successful signal detection performance in the response time of a jammer and thus these approaches cannot be directly applied to avoid jamming attacks in satellite communication systems for a jammer with a "detect and jam" strategy.

In this paper, we investigate a counter-measure anti-jamming game to maximize an expected payoff in time-bounded space communication systems where a cognitive jammer reactively senses and jams the active channel. The payoff of the legitimate link derived in this paper takes into account of signal detection performance of a jammer, achievable data rate of a legitimate link, cost incurred by jamming and hopping, and frequency hopping probability depending on a given channel condition. The proposed game outperforms the other existing methods.

The remainder of the paper is organized as follows: we present the system model in Section II followed by an frequency hopping and power adaptation game in Section III. We illustrate numerical results obtained from simulations in Section IV, and present conclusions in Section V.

## II. System Model and Proposed Approach

A typical space communication model considered in this paper is shown in Fig. 1, where $A$ is a satellite, $B$ is a ground station and $J$ is a jammer. Note that in satellite/space

[1] The CINR could be degraded because of variety of impairments such as noise, rain, atmospheric attenuation, etc. But, in this paper, we are considering CINR deterioration because of cognitive jamming.

978-1-4799-8406-0/15/$31.00 ©2015 IEEE

communications, signal propagation of a ground station is so directional that the signal from ground station may not be overheard by the jammer whereas the beam of the satellite is so wide that a jammer can easily overhear the transmissions from a satellite transmitter as shown in Fig. 1.

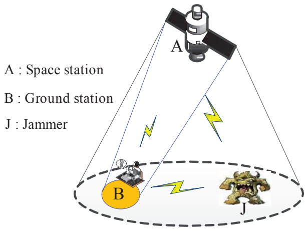

Fig. 1. System model with satellite $A$, ground station $B$, and a jammer $J$.

For a jammer, only way to detect whether there is a transmission from ground station to space station is by overhearing the acknowledgment (ACK or negative ACK) signal sent by the space station to its transmitter. Alternatively, the jammer could be close enough to the ground station so that sidelobes help it to overhear the transmission. Similarly, for a jammer, to detect a signal in a channel when ground station is a receiver and space station is a transmitter, jammer has to be tuned to listening mode and use signal sensing/detection algorithms. Once the jammer detect the active communication in a channel, it sends jamming signal with enough power towards receiver to deteriorate the signal/CINR at the receiver.

### A. Communication Model

We assume that there are $N$ independent sub-channels $\mathcal{F} = \{f_1, \ldots, f_N\}$, each sub-channel is time-slotted and allocated a bandwidth $B_n$. These sub-channels are used to transmit information from transmitter to its receiver in time slotted wireless systems. We assume that the channel utilization/access by users is exponentially distributed with mean $\mu$. The received signal for a link (a user) in $n$th channel can be written as

$$y_n(t) = h_n p_n x_n(t) + q_n(t), \tag{1}$$

where $h_n$ is channel gain, $p_n$ is the transmit power with a power constraint $\sum_{n=1}^{N} p_n \leq \overline{P}$, $x_n(t)$ is the transmit signal, $q_n(t)$ is the additive white noise that corrupts the received signal, and the received signal power is $p_{r_n} = h_n p_n$. We assume that transmitter supports $M$ different power levels on any given channel to provide set of different rates. The set of power is denoted by $\mathcal{P} = \{p_1, p_2, \ldots, p_M\}$ as shown in Fig. 2. Without loss of generality, we consider that $p_1 < p_2 < \ldots, < p_M$. Let $p_{j_n}$ be the injected power by the jammer in $n$th channel with $\sum_{n=1}^{N} p_{j_n}(i) \leq I$, which means jammer also has a power constraint.

The performance of a link in space communication system can be measured using CINR, which is given as

$$\gamma_n = \frac{h_n p_n}{\alpha_n p_{j_n} + N_0 B_n}, = \frac{p_{r_n}}{\alpha_n p_{j_n} + N_0 B_n}, \tag{2}$$

where $0 \leq \alpha_n \leq 1$ is a channel gain between the jammer and legitimate receiver, $N_0$ is the power spectral density of the noise and is given by $N_0 = k\tau$ for a receiver system temperature $\tau$ and Boltzmann constant $k = 1.38e^{-23} W/Hz$-$K$. From information theory, the achievable rate of a link in $n$th channel can be expressed as

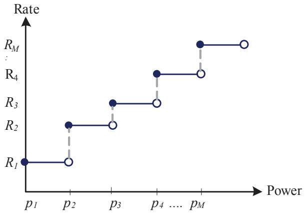

Fig. 2. Rate vs. Power Relationship

$$R_n = B_n \log_2(1 + \gamma_n) \tag{3}$$

We assume that the link cannot decode packets correctly and the communication fails when CINR drops below certain threshold (i.e., minimum required CINR value) in a given sub-channel [14]. Using equation (3), the time taken by a receiver to successfully decode/receive $D$ bits (including channel coding bits) can be calculated as

$$T_n = \frac{D}{B_n \log_2(1 + \gamma_n)}. \tag{4}$$

### B. Jamming Model

For a jammer with "detect and jam" strategy, channel sensing and signal detection approach used by the jammer plays a role on how fast the jammer can detect and send a jamming signal to jam the active channel. When a jammer detects a signal in a channel by using sensing approaches (with cognitive radio/capabilities), it launches a jamming attack by sending a random signal towards the intended receiver to damage the signal or to deteriorate CINR at the receiver. A jammer tests the received signal under two hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ in discrete time domain with sample index $j$ as

$$\begin{aligned} \mathcal{H}_0 &: \quad Y_n(j) = q_n(j) \\ \mathcal{H}_1 &: \quad Y_n(j) = g_n x_n(j) + q_n(j) \end{aligned} \tag{5}$$

where $g_n$ is the channel gain between legitimate transmitter and the jammer.

The test statistics for distinguishing between two hypotheses using energy detection for a jammer is given as

$$T(Y_n) = \frac{1}{W} \sum_{j=0}^{W-1} |Y_n(j)|^2 \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \lambda \tag{6}$$

where $W$ is the sensing window length and $\lambda$ is decision threshold.

Note that, in space communication systems, distance between transmitter and its receiver is large, and it plays a significant role in jamming attacks using detect and jam strategies. We assume that the signal propagation time is given as $\delta_{AB}$[2] (between an intended transmitter-receiver pair), $\delta_{JA}$

[2] Here $\delta_{AB} = \frac{1}{c}\left[\sqrt{(R+h)^2 - R^2 cos^2\theta} - Rsin\theta\right]$ seconds for radius of the Earth ($R$), orbital altitude ($h$), satellite elevation angle($\theta$), and the speed of light ($c$).

(between a jammer and transmitter) and $\delta_{JB}$ (between the jammer and receiver). All of these times for signal propagation are in milliseconds but they have a significant role in jamming and anti-jamming game in space communication systems. Note that if a given channel is used for entire communication to transmit $D$ bits, the necessary condition for successful transmission of $D$ bits using (4) is $T_n \leq T_r$, where $T_r$ is the response time of the jammer and is given as

$$T_r = \delta_{JB} + \delta_{JA} - \delta_{AB} + W = \Delta_{JBJA} + W. \quad (7)$$

Otherwise, the transmitter and its receiver must hop to another suitable channel. Thus, the transmission strategies of satellite links must be adaptive to the attackers' strategies. We assume that a jammer depends on probability of detection and false alarm while sensing channels.

The probability of detection $P_d$ and false alarm $P_f$ for a jammer is given as [15]

$$P_d = Q\left[\frac{\lambda - (1+\beta)N_0 B_n}{N_0 B_n \sqrt{(1+2\beta)2/W}}\right] \quad (8)$$

$$P_f = Q\left[\frac{\lambda - N_0 B_n}{N_0 B_n \sqrt{2/W}}\right] \quad (9)$$

where $\beta = E\{[g_n x_n(j)]^2\}/N_0 B_n$.

For a jammer, response time $\mathbf{T_r}$ in (7) is a random variable which depends on signal propagation times and channel sensing window $W$, and follows the distribution of $W$. Considering probability of false alarm, we obtain the average successful detection duration for a transmitter that follows exponential distribution with mean $\mu$ according to our system model as

$$\overline{T_r} = E\{\mathbf{T_r}\}[1 - P_f] = \mu \exp\left(-\frac{W + \Delta_{JBJA}}{\mu}\right)[1 - P_f] \quad (10)$$

Then, the successful signal detection can be expressed as

$$\overline{T}_d \;=\; \frac{\overline{T_r}}{\mu} = \exp\left(-\frac{W+\Delta_{JBJA}}{\mu}\right)[1 - P_f] \quad (11)$$

Next, for a jammer, successful signal detection *performance* $S_d \in [0, 1]$ is defined as

$$S_d = \theta P_d + (1-\theta)\overline{T}_d, \quad (12)$$

where $\theta \in [0, 1]$ is a constant that weights between $P_d$ and $\overline{T}_d$. Note that when $\theta = 1/2$ both $P_d$ and $\overline{T}_d$ have equal weights in the detection performance.

Once a jammer detects a signal, we assume that the jammer emits the enough power level on a channel to destroy the signal where, for a given received power $p_{r_n}$ and CINR $\gamma_n$ at the receiver, the jamming power $p_{j_n}$ is

$$p_{j_n} = \frac{\frac{p_{r_n}}{\gamma_n} - N_0 B_n}{\alpha_n}. \quad (13)$$

Similar to [16], jammer chooses its discrete value of jamming power that satisfies its average power constraint. We consider that the $\mathcal{A}_J$ is the set of strategies (containing $M$ different power levels) of a jammer and is given as

$$\mathcal{A}_J = \{p_{j_n}, 0 \leq j \leq M - 1\} \quad (14)$$

From the jammer's perspective, the sensing performance of the jammer is optimized by maximizing the successful detection performance ($S_d$) and then sending jamming signal using the suitable power strategy chosen from its power strategy set $\mathcal{A}_J$.

## III. Frequency Hopping and Power Adaptation Game

In this section, we present a game that uses frequency hopping strategies to secure satellite communication link against reactive jammer.

### A. Attack and Defense Strategies

For each time slot, the jammer senses the channel and uses the energy detection to identify whether or not there is ongoing transmission. Once the attacker learns that the channel is being used, it sends a jamming signal toward the receiver to deteriorate the receiver's CINR. Only way for the transmitter to escape from the jammer is to adapt its power (equivalently rate as in Fig 2) to get undetected. In this case jammer forces the link to use minimum data rate [16]. But when there are multiple channels, transmitter and receiver can hop from one channel to another to avoid jamming. At the same time, the jammer can also hop to another channel to detect any active transmissions and jam the active channels. A jammer with a cognitive radio can sequentially sweep the channels to detect active one and jam it. Then, it restarts new sweep cycle randomly by choosing the power from its strategy/action set $\mathcal{A}_J$ and repeats the process. Note that when space station communicates with the ground station, a jammer can overhear the transmission and use channel sensing techniques to find whether the channel is used or not. Based on this analysis, it can send jamming signal when the channel is found active. However, when the ground station communicates with the space station, because of the directed beam pattern, the jammer may not overhear any signals from transmitter (i.e., ground station) unless it is close enough to the transmitter. In this case only way to detect whether or not there is an active communication in a given channel, is by listening for ACK or NACK signals from the legitimate receiver (i.e., space station in this case). If a jammer overhears ACK, it can increase its jamming power until it overhears NACK or no response in a given channel. Similarly, when legitimate transmitter receives NACK signal from its receiver it can increase its transmit power (equivalently rate) to overcome any loss. But even with its highest transmit power, it gets NACK then this implies that there channel is jammed. Transmitter and receivers must hop to another frequency and start communications in that channel until either they finish their communications or the channel is jammed. This process is repeated by the legitimate transmitter-receiver pair and the jammer.

### B. Rendezvous based Frequency Hopping (FH) Strategies

We assume that $L \geq 0$ out of $N$ channels are assumed to be inaccessible at the moment because of jamming attacks. A transmitter randomly chooses $K = N - L$ accessible channels for communication. After that, in each time slot, the transmitter selects an action from $\mathcal{A}_k = \{(s,p_1),\dots,(s,p_M),(h,p_1),\dots,(h,p_M)\}$ where $s_i \triangleq (s,p_i)$ represents the decision to stay on the current channel and use power $p_i$, and $h_i \triangleq (h,p_i)$ represent the decision to hop to a new channel and use power $p_i$. Let $Pr(c'|c,a_k,a_j)$ denotes the transition probability to state $c'$ from a current state $c$ when the transmitter chooses action $a_k \in A_k$ while the jammer chooses action $a_j \in A_J$. When an action $h_i$ is taken at any state that means the state of the current channel is jammed, i.e., $c = J$. If the channel is not jammed with action $s_i$, the state of the channel will be $c = 1$. Note that when the transmitter and receiver hop to another channel, the state on the new channel can be either jammed or not jammed. We assume that the transmitter and receiver pair use quorum randomized channel hopping [17], [18] for rendezvous. Let us consider a scenario where transmitter involves hopping to a new channel. For instance, for a channel $f$ in a given time slot, a transmitter accesses the channel. In the next time slot, if this channel is jammed by an attacker with an action $h_i$, the transmitter and receiver must hop to one of the $N-L$ accessible channels. In this scenario, the probability of hopping to another channel is

$$Pr(c'=1|c=J,h_i,a_j) = \frac{1}{N-L}. \tag{15}$$

However, when previously used channel is not jammed (jammer's effect is negligible in legitimate communications) for the next time slot $i+1$, the channel can be used with probability $P_{ru} = Pr(1|1,s_i,a_j)$, if $i > j$. Then, the hopping probability in this case becomes

$$Pr(c'=1|c=1,s_i,a_j) = (1-P_{ru}) \times \frac{1}{N-L-1}. \tag{16}$$

Similarly, the probability of hopping to the same channel by both transmitter-receiver pair and the jammer (when jammer was jamming the current channel and hops to another channel with a hope that the jammed transmitter will hop to the same channel that jammer is hopping) is similar to (15) and is expressed as

$$Pr(c'=J|c=J,h_i,a_j) = \frac{1}{N-L}. \tag{17}$$

When a transmitter hops to next channel, its state can be jammed (i.e., $c' = J$), or not jammed (i.e., $c' = 1$). $c' = 1$ if any of the following happens (i) the channel is not swept or already swept by the jammer or (ii) jammer hops to $f$ and uses a power level that does not disrupt the legitimate transmissions.

### C. Payoffs

In this work, satellite communication is said to be successful (decoding without any error) only if the CINR at the receiver is higher or equal to its minimum required value. When a transmitter successfully transmits in a channel with a transmitting rate $R_n$, the transmitter receives an award of the same rate. Thus, the payoff is defined as the reward minus the cost incurred for the communication in each channel the satellite link used, i.e.,

$$U_K = \sum_{n=1}^{K}[I_n(s_i).R_n - J_n(s_i).L_n - H_n(s_i).C_n], \tag{18}$$

where $L_n$ is the cost incurred because of successful jamming in $n$th channel and $C_n$ is the cost incurred because of hopping. $I_n(s_i) = 1$ for successful transmission using power level $p_i$ in a channel $n$. Otherwise $I_n(s_i) = 0$. $J_n(s_i) = 1$ for successful jamming in a channel $n$. Otherwise $J_n(s_i) = 0$. Similarly, $H_n(s_i) = 1$ when transmitter hops to another channel, otherwise $H_n(s_i) = 0$. Immediate payoff for a given channel $n$ can be calculated as [11]

$$u_n(c,a_k,p_{j_n},c') = \begin{cases} R_n, & \text{if } c' \neq J, a_k = s_i, p_{j_n} < p_i, \\ R_n - C_n, & \text{if } c' = 1, a_k = h_i, p_{j_n} \geq p_i, \\ -L_n, & \text{if } c' = J, a_k = s_i, p_{j_n} \geq p_i, \\ -L_n - C_n, & \text{if } c' = J, a_k = h_i, p_{j_n} \geq p_i \\ 0, & \text{otherwise.} \end{cases} \tag{19}$$

Transmitter-receiver pair and the jammer take their actions based on their previous observations which can be solved using Markov Decision Process. We restrict our analysis to Markov stationary policies, where actions of the transmitter and jammer for next slot depend on current state only.

Actions taken by the transmitter-receiver pair $a_k$ and jammer $a_j = p_{j_n}$ based on a given channel state $c$ and hopping probability (15), (16), or (17), the payoff using (19) is expressed as

$$p_n(c,a_k,a_j) = \sum_{c'} u_n(c,a_k,a_j,c')Pr(c'|c,a_k,a_j). \tag{20}$$

Then, when an initial state is $c_0$ and the detection performance of a jammer is $S_d$ in (12), the expected payoff ($E[.]$) of the transmitter-receiver pair using (20) is defined as

$$V(c,L_A,J_A) = E^{L_A,J_A}\left[\sum_n [1-S_d(n)]p_n(c,a_k,a_j)|c=c_0\right], \tag{21}$$

where $L_A \in A_k$ and $J_A \in A_J$. Objective of the transmitter is to choose a strategy $L_A \in A_k$ to maximize the expected payoff, i.e.,

$$V_t(c,J_A) = \max_{L_A \in A_k, \gamma_n} V(c,L_A,J_A), \tag{22}$$

and the objective of the jammer is to choose a strategy $J_A \in A_J$ to minimize the transmitter-receiver pair's payoff, i.e.,

$$V_j(c,L_A) = \min_{J_A \in A_J, W} V(c,L_A,J_A). \tag{23}$$

Thus, the game between transmitter-receiver pair and jammer is a zero-sum game where loss of legitimate communication is (sort of) gain for the jammer.

### D. The Nash Equilibrium of the Game

The Nash Equilibrium of a non-cooperative zero-sum game for optimal strategies $L_A^*$ and $J_A^*$ is expressed as

$$\overline{V}(c,L_A,J_A^*) \leq \overline{V}(c,L_A^*,J_A^*) \leq \overline{V}(c,L_A^*,J_A). \tag{24}$$

This implies that the payoff is least when the jammer applies its optimal strategy while transmitter has not applied its optimal strategy. Similarly, the payoff is highest when the legitimate transmitter-receiver pair applies optimal strategy while jammer is not at its best strategy. Note that when jammer's strategy $J_A$ is fixed, the legitimate link can obtain the optimal payoff by choosing the channels with least interference $\frac{\alpha_n p_{j_n} + N_0 B_n}{p_{r_n}}$. But, when a jammer is reactive, transmitter-receiver must be adaptive to the attacker's strategies.

**Proposition 1**: For the zero-sum game with expected payoff in (21), the unique equilibrium is

$$J_A^* = p_{j_n} = \max\left\{0, \frac{h_n}{\alpha_n}\left[\frac{1}{\eta} - \frac{N_0 B_n}{h_n}\right]\right\} \tag{25}$$

$$L_A^* = p_n = \frac{p_{r_n}}{h_n} = \frac{\overline{P} h_i/\alpha_i}{\sum_{j\in\Omega} h_j/\alpha_j}, \quad i \in \Omega, \tag{26}$$

where $\Omega = \{j = 1, 2, ..., N : p_{j_n} \neq 0\}$ and $\eta$ is the unique root of the following equation

$$\sum_{n=1}^{N}\left\{\max\left\{0, \frac{h_n}{\alpha_n}\left[\frac{1}{\eta} - \frac{I + N_0 B_n}{h_n}\right]\right\}\right\} = 0. \tag{27}$$

**Proof:** From (21), (22), (23), and (24) for the system model considered in this paper, Nash Equilibrium satisfies the following optimization problems simultaneously:

$$\begin{aligned} &\underset{\{p_j\}_{\forall j}}{\text{argmin}} \ \sum_{n=1}^{N} \gamma_n, \ \text{subject to} \ \sum_{n=1}^{N} p_n \leq I \\ &\underset{\{p_{r_n}\}_{\forall n}}{\text{argmax}} \ \sum_{n=1}^{N} \gamma_n, \ \text{subject to} \ \sum_{n=1}^{N} p_n \leq \overline{P}. \end{aligned} \tag{28}$$

Problem (28) has not duality gaps and thus their Lagrangian formulations with Lagrangian multipliers $\eta$ and $\beta$ can be written for $\gamma_n$ in (2) as

$$\begin{aligned} L(\eta, J_A) &= \sum_{n=1}^{N} \frac{h_n p_n}{\alpha_n p_{j_n} + N_0 B_n} + \eta\left(\sum_{n=1}^{N} p_n - I\right) \\ L(\beta, L_A) &= \sum_{n=1}^{N} \frac{h_n p_n}{\alpha_n p_{j_n} + N_0 B_n} - \beta\left(\sum_{n=1}^{N} p_n - \overline{P}\right). \end{aligned} \tag{29}$$

Using KKT condition [19], problem (29) can be solved as

$$\begin{aligned} \frac{\partial L(\eta, J_A)}{\partial p_{j_n}} &= \frac{\alpha_n h_n p_n}{(\alpha_n p_{j_n} + N_0 B_n)^2} + \eta = 0 \\ \frac{\partial L(\beta, L_A)}{\partial p_n} &= \frac{h_n}{\alpha_n p_{j_n} + N_0 B_n} - \beta = 0 \\ \sum_{n=1}^{N} p_n = I, &\quad \sum_{n=1}^{N} p_{j_n} = \overline{P} \end{aligned} \tag{30}$$

Thus, we can have solution as (25) and (26) and by solving (27), we get the value of $\eta$ as

$$\eta = \frac{\sum_{n=1}^{N} h_n/\alpha_n}{I + \sum_{n=1}^{N}(B_n/\alpha_n)N_0}, \tag{31}$$

which prove the desired results. ■

## IV. Performance Evaluation

In this section, we present numerical results obtained from simulations to evaluate the proposed anti-jamming game to secure satallite communication against a reactive cognitive jammer for different values of system parameters using (21). We consider a space communication scenario with a legitimate transmitter-receiver pair, and a reactive cognitive jammer to measure the performance of the system in terms of expected/average payoff. We consider a set of rates $R = \{6, 9, 12, 15\}$ Mbps that are available in recent satellite systems [20]. We assume that the number of channels as $N = 15$, maximum cost of frequency hopping (FH) $C_n = 15$ Mbps, and maximum cost of jamming $L_n = 15$ Mbps. All propagation times are chosen to be smaller than 0.10 second, and $\theta = 0.5$. We used MATLAB to simulate the proposed scenario for space communication systems.

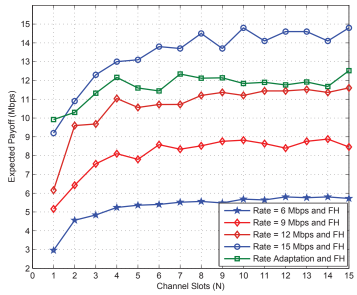

Fig. 3. Variation of expected/average payoff vs. number of channels.

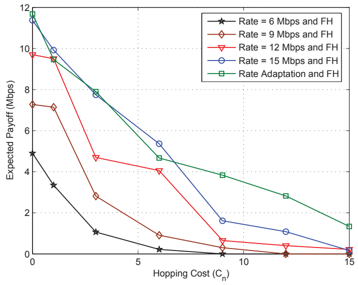

Fig. 4. Variation of expected/average payoff vs. hopping cost.

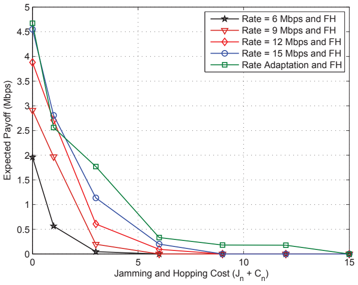

Fig. 5. Variation of expected/average payoff vs. jamming and hopping cost.

First, we plotted the variation of an average payoff for different number of channel slots as shown in Fig. 3. For increasing rate, payoff is increasing for a given number of channel slots. For combined frequency hopping and rate[3] adaptation strategy, the average payoff is highest when there is only one channel and always higher other than 15 Mbps rate as shown in Fig. 3.

Average payoff could be lower even though there are more channels slots. For instance, average payoff for 15 Mbps and FH when $N = 4$ is lower than that when $N = 3$ as shown in Fig. 3. The decrease in payoff happens when the jammer and legitimate user hop into the same channel slot, and the legitimate user would have to hop into another channel to avoid the jammer or it communicates in high interference caused by

[3] Rate and power are related by (2) and (3) as in Fig. 2

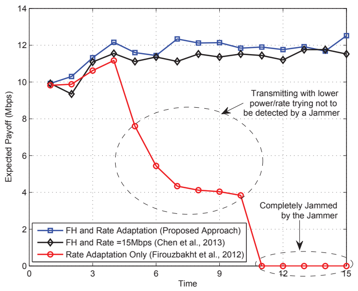

Fig. 6. Comparison of the proposed approach with others.

the jammer.

Next, we plotted the variation of average payoff for different values of hopping cost in Fig. 4. With the increasing hopping cost, average payoff decreases for given rate and FH as shown in Fig. 4. We also note that, the joint rate/power adaption and FH has highest average payoff when hopping cost is greater than 7 Mbps. Then, we plotted expected/average payoff variation for different values of combined hopping and jamming cost as shown in Fig. 5. Because of the joint jamming and hopping cost, average payoff decreases sharply. As expected joint FH and rate adaptation gives better results than the method with fixed rate with FH as shown in Fig. 5.

Finally, we compare the performance of the proposed approach with other methods in the literature as shown in Fig. 6. To compare different approaches in an identical scenario, we consider that the maximum value of hopping and jamming cost is 3 Mbps. Note that the rate adaptation approach in [16] lowers its transmission power (rate) trying not to be detected by the jammer until Time $= 10$. However, when jammer's power reaches above certain threshold, the legitimate link cannot decode the information sent from its transmitter resulting in zero payoff after Time $= 10$ as shown in Fig. 6. Furthermore, the FH and fixed rate method in [9] does not consider that transmitter-receiver pair and jammer hop to a same channel and the effect of detection performance of the jammer which results in payoff as in Fig. 6. Note that the proposed (FH and power/rate adaptation) approach takes account of these issues and thus outperforms the existing methods in terms of expected payoff as shown in Fig. 6.

We conclude that the joint FH and rate (equivalently power) adaptation achieves better expected payoff when there is high hopping and jamming cost than that using FH for a given rate (power) or only rate/power adaptation.

## V. Conclusion

In this paper, we have presented an anti-jamming game that uses frequency hopping and rate/power adaptation to mitigate the jamming effect introduced by a reactive cognitive jammer in the context of space communication systems. Jamming and anti-jamming process is formulated as a game where anti-jamming approach maximizes the expected payoff (throughput) of legitimate satellite link whereas the jammer tries to minimize that. We have observed that the proposed approach with joint frequency hopping and rate/power adaptation outperforms the other existing methods in terms of expected payoff. Furthermore, the proposed approach achieves better expected payoff when there is high hopping and jamming cost and/or there are few channel slots.

## Acknowledgment

The research of Danda B. Rawat is supported by U.S. NSF grant CNS-1405670. The research of Min Song is supported by U.S. NSF IPA Independent Research and Development (IR/D) Program.

## References

[1] Y. Tan, S. Sengupta, and K. Subbalakshmi, "Analysis of coordinated denial-of-service attacks in ieee 802.22 networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 890–902, 2011.

[2] W. Xu, W. Trappe, and Y. Zhang, "Channel surfing: defending wireless sensor networks from interference," in *Proc. of the 6th int'l conference on information processing in sensor networks*, 2007, pp. 499–508.

[3] S. Khattab, D. Mosse, and R. Melhem, "Jamming mitigation in multi-radio wireless networks: reactive or proactive?" in *Proc. of the 4th int'l conference on security & privacy in com. networks*, 2008, p. 27.

[4] R. Pickholtz, D. Schilling, and L. Milstein, "Theory of spread-spectrum communications–a tutorial," *IEEE Transactions on Communications*, vol. 30, no. 5, pp. 855–884, 1982.

[5] L. Zhang and T. Li, "Anti-Jamming Message-Driven Frequency HoppingPart II: Capacity Analysis Under Disguised Jamming," *IEEE Transactions on Wireless Communications*, vol. 12, pp. 80 – 88, 2013.

[6] B. Wang, Y. Wu, K. R. Liu, and T. C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 877–889, 2011.

[7] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service," in *Proc. of the 3rd ACM workshop on Wireless security*, 2004, pp. 80–89.

[8] M. J. Abdel-Rahman, H. Rahbari, M. Krunz, and P. Nain, "Fast and secure rendezvous protocols for mitigating control channel dos attacks," in *Pro. of IEEE INFOCOM'13*, 2013, pp. 370–374.

[9] C. Chen, M. Song, C. Xin, and J. Backens, "A game-theoretical anti-jamming scheme for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 22 – 27, 2013.

[10] H. Li and Z. Han, "Dogfight in spectrum: jamming and anti-jamming in multichannel cognitive radio systems," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, 2009, pp. 1–6.

[11] Y. Wu, B. Wang, K. R. Liu, and T. C. Clancy, "Anti-jamming games in multi-channel cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 1, pp. 4–15, 2012.

[12] M. Hanawal, M. Abdel-Rahman, D. Nguyen, and M. Krunz, "Game theoretic anti-jamming dynamic frequency hopping and rate adaptation in wireless systems," 2013.

[13] X. Tian, Z. Tian, K. Pham, E. Blasch, and D. Shen, "Jamming/anti-jamming game with a cognitive jammer in space communication," in *International Society for Optics and Photonics Defense, Security, and Sensing*, 2012.

[14] M. Takai, J. Martin, and R. Bagrodia, "Effects of wireless physical layer modeling in mobile ad hoc networks," in *Proc. of 2nd ACM int'l symposium on mobile ad hoc networking & computing*, 2001, pp. 87–94.

[15] Y.-C. Liang, Y. Zeng, E. C. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1326–1337, 2008.

[16] K. Firouzbakht, G. Noubir, and M. Salehi, "On the capacity of rate-adaptive packetized wireless communication links under jamming," in *Proc. of the 5th ACM Conference on Security & Privacy in Wireless & Mobile Networks*, 2012, pp. 3–14.

[17] C. Xin, M. Song, L. Ma, and C. Shen, "ROP: Near-Optimal Rendezvous for Dynamic Spectrum Access Networks," *IEEE Transactions on Vehicular Technology*, vol. 24, no. 7, pp. 3383 – 3391, 2013.

[18] W.-S. Luk and T.-T. Wong, "Two new quorum based algorithms for distributed mutual exclusion," in *Proc. of the 17th International Conference on Distributed Computing Systems, 1997*, 1997, pp. 100–106.

[19] S. P. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[20] M. Sullivan and T. Spring, "Early IPTV uses only a little of its fat pipe," *PC World*, pp. 26–28, 2007.