IEEE Access

IEEE Access
The journal for rapid open access publishing

IEEE Xplore Digital Library
http://ieeexplore.ieee.org/Xplore

Received December 14, 2017, accepted January 10, 2018, date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Jamming Mitigation via Hierarchical Security Game for IoT Communications

XIAO TANG[1,2],PINYI REN[1,2], AND ZHU HAN[3,4], (Fellow, IEEE)
[1]School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China
[2]Shaanxi Smart Networks and Ubiquitous Access Research Center, Xi'an 710049, China
[3]Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004, USA
[4]Department of Computer Science and Engineering, Kyung Hee University, Seoul 02447, South Korea

Corresponding author: Pinyi Ren (e-mail: pyren@mail.xjtu.edu.cn).

The work of X. Tang and P. Ren was supported in part by the National Natural Science Foundation of China under Grant 61431011, in part by the Key Research and Development Program of Shannxi Province under Grant 2017ZDXM-GY-012, and in part by the National Science and Technology Major Project of China under Grant 2018ZX03001003-004. The work of Z. Han was supported in part by the U.S. National Science Foundation (NSF) under Grant CNS-1717454, Grant CNS-1731424, Grant CNS-1702850, Grant CNS-1646607, Grant ECCS-1547201, Grant CMMI-1434789, Grant CNS-1443917, and Grant ECCS-1405121.

ABSTRACT In the Internet of things (IoT), the malicious node with sensorial capability can smartly launch jamming attacks only when it detects the legitimate transmission, known as the reactive jamming. Compared with the conventional constant jamming model, the reactive nature enables highly efficient and long-lasting attacks with limited energy supply, which thus presents a significant threat upon the secure communications in IoT. In this paper, we investigate the anti-reactive-jamming transmission strategy for IoT by exploiting the inherent weakness of the jammer. Specifically, since the reactive jamming depends on the detection of the legitimate transmission, the legitimate user can elaborately determine its transmit power to trade off between its achieved signal-to-interference-plus-noise ratio (SINR) and the probability to be detected and jammed by its adversary. Meanwhile, the jammer can smartly allocate the jamming power based on its observation of the legitimate transmission. We formulate the rivalry between the legitimate user and jammer as a hierarchical game where the legitimate user takes action first as the leader while the jammer is the follower. We analyze the game equilibrium for both single-channel and multi-channel scenarios and derive the optimal transmission and jamming strategies for the legitimate user and jammer, respectively. Finally, we present the numerical results to evaluate the performance of the secure IoT communications under our proposal.

INDEX TERMS Internet of things, reactive jamming, resource allocation, hierarchical game, equilibrium

I. INTRODUCTION

THE INTERNET of things (IoT) presents a vision that massive devices of different types with sensorial, computing, and communication capabilities work together towards ubiquitous connectivity and efficient information exchange [1]. With massive connections and seamless communications at any time and place, IoT has found its applications in a variability of areas, such as agriculture, industry, transportation, schools, homes, etc., and thus is expected to play a remarkably important role in the near future [2]. Towards this goal, the effective protection of information security under the malicious jamming attack is a fundamental yet challenging issue [3]. In IoT, the wireless communications are usually conducted discontinuously among the power-limited nodes. Consequently, the conventional constant jamming model that conducts jamming attacks all the time is energy-consuming and thus inefficient. Instead, the malicious node can exploit its sensorial capability to sense the surrounding wireless environment and smartly determine its jamming policy to achieve the maximum damage, known as the reactive jamming model [4]. Since the reactive jammer is capable to efficiently deteriorate the secure communications in IoT even with limited energy supply, it is of paramount importance to investigate the jamming mitigation strategy to safeguard the IoT communications [5], [6].

Conventionally, the main research efforts on the anti-jamming strategy concentrate on the constant jamming model [7]. In this respect, there have been the research works regarding the security evaluation [8]–[13] as well as various anti-jamming strategy designs such as frequency hopping [14], [15], power control [16], [17], timing-

Digital Object Identifier: 10.1109/ACCESS.2018.2793280

channel transmissions [18], interference cancellation techniques [19], and so forth. However, the constant jamming is generally energy-hungry and thus may not be feasible for the battery-powered IoT devices [20]. Moreover, as the IoT communications are usually discontinuous, the constant jamming is evidently energy-inefficient. In this respect, the reactive jamming model is a more-threatening alternative that conducts the jamming attack only when it detects the legitimate transmission. The reactive jamming can be easily implemented in IoT with the sensorial and communication capability at the malicious nodes. Meanwhile, it becomes more difficult to detect the reactive jamming attack since it is conducted discontinuously. Moreover, its reactive nature enables long-lasting jamming attacks for more significant deterioration on the legitimate transmissions. Although the reactive jamming presents an unprecedented threat for IoT communications, there have only emerged a few recent results regarding the relevant issues, such as the reactive jamming detection [21], jamming avoidance [22], [23], and other countermeasure designs [24]–[26]. Despite the effectiveness of these proposals, they are not yet able to sufficiently cover the relevant issues in this area, which presents an urgent need for further investigation on the anti-reactive-jamming design for IoT communications.

To defend the secure IoT communications against reactive jamming, we consider this problem from a novel perspective — to exploit the inherent weakness of the reactive jammer as the jammer's detection of the legitimate transmission in practical IoT cannot be perfect. Then, such imperfection further leaves the legitimate side an opportunity to mitigate the jamming attacks. Specifically, as the probability of successful detection of the legitimate transmission at the jammer depends on the legitimate transmit power, the legitimate side can elaborately determine its transmit power to optimize the tradeoff between the achieved signal-to-interference-plus-noise ratio (SINR) and the probability to be detected and jammed. Compared with the proposals such as jamming avoidance techniques in [22], [23] that require relatively rigorous conditions or the complicated mitigation techniques in [24], [25] that requires multiple antennas, our proposal requires rather mild condition and thus can be easily implemented. Moreover, the imperfect detection widely exists in practical wireless systems, which enables our proposal with potentially wider applications in practical IoT communications.

On the other hand, for the existing research works on jamming mitigation techniques, most of them only emphasize on the strategy design for the legitimate side, while ignoring the jammer's reactions [8]–[10], [16], [17], [21]–[26]. However, due to the inherent sensorial and computing capability of the jammer in IoT, it is potentially able to adapt its jamming behavior to the legitimate transmission for the maximum damage. Consequently, we need to consider the behavior at both the legitimate side and its adversary, as well as the interactions between them. In this regard, the game theory provides us an effective tool to track such interest-conflicting scenarios [27]–[29]. However, the existing literature on the game-based jamming analysis mainly focuses on the conventional constant jamming model [18], [30]–[33], where the problem formulation at the jammer only concerns the jamming optimization. In contrast, for the reactive jammer in IoT, it has to jointly consider the detection and jamming strategies, which not only results in a more complicated attacking problem but also induces more intricate interactions between the legitimate side and the jammer. These issues are seldom addressed in the existing research works and thus deserve more research efforts.

Targeting at the issues noted above, in this paper, we address the secure IoT communications under reactive jamming attacks with the game-based analysis. We formulate the rivalry between the legitimate transmission and jamming as a hierarchical game where the legitimate user is the leader to take action first while the jammer is the follower. Within the game, the jamming strategy is jointly considered with detection, while the security enhancement is achieved at the legitimate user through the first-mover advantage. By analyzing the equilibrium, we derive the optimal strategies for both the sides and also reveal the steady states of the security competition. Specifically, the main contribution of this work can be summarized as follows.

- Since the IoT communications are usually discontinuous and the IoT devices are usually energy-sensitive, we consider the reactive jamming model that conducts detection prior to jamming, which makes the attacks purposive and power-efficient. Despite the fact that the reactive jamming is specially challenging for IoT communications, we propose a novel anti-jamming strategy design to effectively protect the legitimate transmission.
- We consider to secure the IoT communications from a novel perspective that exploits the inherent weakness of the reactive mechanism as the detection prior to jamming attacks is not perfect. We formulate the security competition between the legitimate user and jammer as a hierarchical game where the legitimate user takes action first, followed by the jammer. In this respect, the legitimate user can exploit the first-mover advantage to enhance the security.
- For the game under single-channel transmission scenario, we analyze the equilibrium by applying the backward induction method. Then, the optimal jamming strategy is derived with the closed-form expression and the optimal legitimate power allocation is analyzed with effective calculation.
- We further extend the security game to the multi-channel transmission scenario. Since there potentially lacks the closed-form solution for the lower problem at the jammer, we reformulate the game as a mathematical program with equilibrium constraints (MPEC) to solve for the game equilibrium, along with the strategy designs for both the legitimate user and jammer.

The rest of the paper is organized as follows. In Sec. II, we review the related works. The system model is introduced in Sec. III. The jamming game is analyzed, respectively, for the single-channel transmission scenario and multi-channel transmission scenario in Sec. IV and Sec. V. We evaluate the security performance with simulation results in Sec. VI and conclude this paper in Sec. VII.

II. RELATED WORKS

The anti-jamming transmission strategy for wireless security has long been a hot topic for wireless researches. In the literature, most research works have been focused on the constant jamming. In [8], the authors consider the jamming attack in the wireless networks and evaluate the performance with stochastic geometry based analysis. The distributed security estimation is evaluated in [9] for the wireless sensor networks by adopting the Markov chain theory. In [10], the authors specialize on the jamming attacks on the frequency offset estimation in orthogonal frequency division multiplexing (OFDM) system. The authors of [11] investigate the jamming attacks over the vehicular ad hoc network with experimental results. In [12], the authors consider the hybrid jamming issue with eavesdropping threats. In [14], the authors adopt the frequency hopping technique to mitigate jamming attacks and employ the multi-arm bandit theory to model the rivalry. In [15], the anti-jamming transmission strategy is investigated by jointly optimizing the frequency hopping and rate adaptation techniques. In [16], the authors propose to mitigate the jamming attacks to improve the legitimate transmissions by exploiting the subcarrier agility in the OFDM system. The joint optimization over power control and scheduling is explored in [17] to defend against the jamming attacks. In [19], the dual antennas are exploited to cancel the hostile jamming signals to protect the legitimate transmissions.

The reactive jamming issue has recently attracted an increasing research interest. In [21], the authors consider the detection of reactive jamming in the direct sequence spread spectrum wireless system by exploring the distinguished statistics of the jamming as compared with the jamming-free transmissions. In [22], the authors propose to improve the legitimate transmission under reactive jamming attacks by harnessing the reaction time at the jammer. In [23], the authors propose to elaborately determine the active transmission nodes to smartly avoid invoking the reactive jammer. In [24], the multiple-input multiple-output (MIMO) transmissions are exploited to cancel the jamming signals to improve the legitimate transmissions. The similar technique is employed in [25] to improve the channel estimation under reactive jamming attacks. The authors of [26] propose an interesting scheme where the reactive jammer is piggybacked as an unwitting relay node by elaborately designing the frequency-shift keying waveform.

Game theory provides us a powerful mathematical tool to evaluate the security performance in the presence of jamming attacks. In [18], the authors consider the timing-channel transmission strategy under jamming attacks with game-based formulation. In [30], the authors investigate the optimal power allocation strategy under constant jamming attacks. In [31], the stochastic game model is applied to study the jamming issue for the secure transmission over time series. In [32], the prospect theory, as a variation of game theory, is applied to investigate the jamming problem when the jammer and legitimate user potentially have biased evaluation regarding their rewards. In [33], the authors investigate the security game by jointly consider the jamming and eavesdropping attacks.

III. SYSTEM MODEL

We consider one active legitimate transmission pair in the IoT in the presence of a reactive jammer. The legitimate pair may correspond to a radio frequency identification (RFID) tag and the reader, or the sensorial node and the fusion center, etc., which are currently active with the ongoing transmissions. The legitimate source node intends for reliable and high-speed transmissions with the legitimate destination node, while the jammer aims at interrupting the legitimate transmissions by launching jamming attacks. The system is shown in Fig. 1. For the legitimate transmissions, we assume the transmit power is p_S, which is constrained by the maximum allowed power denoted by $p_S^{\max}$. The channel gain from the legitimate source node to the destination node is h_S. Meanwhile, the legitimate transmission is detected by the jammer, for which the channel gain from the legitimate source node to the jammer is h_R. Based on the results of detection, the jammer determines the power allocation for jamming attacks, denoted by p_J, which is constrained by the maximum power given by $p_J^{\max}$. Also, the channel gain from the jammer to the legitimate destination node for the jamming attack is denoted by h_J.

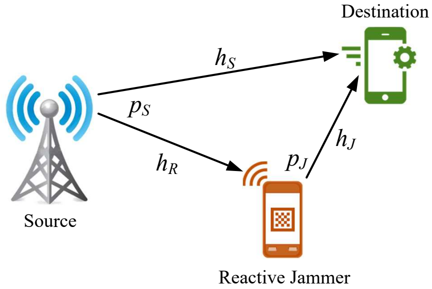


FIGURE 1. System model.

For a variety of applications in IoT, such as the sensor network, RFID tags, etc., the wireless transmissions are usually conducted discontinuously. To model such discontinuity, we assume that the legitimate transmission is performed with the probability of α, $(0 \leq \alpha \leq 1)$, while with the probability of $1-\alpha$ to stay idle. The transmission probability is determined by the inherent nature of the actual IoT application, and we here assume it is a predefined constant. Since the legitimate transmissions are discontinuous, the jammer node will correspondingly abandon the constant jamming policy, as it is evidently energy-consuming and ineffective. Instead, it adopts the reactive jamming strategy that detects the legitimate transmission before conducting the jamming attacks. However, for the practical IoT system, since the wireless environment and network topology may vary with time, the detection cannot be perfect. To rigorously track such imperfection, we introduce the probability of detection and false alarm for the detection. In particular, the probability of detection, denoted by $\mathcal{P}_D$, corresponds to the case that the jammer successfully detects the ongoing legitimate transmission. The probability of false alarm, denoted by $\mathcal{P}_F$, is the probability that the jammer mistakenly detects the legitimate transmission while the the legitimate user is actually idle. We here assume that the jammer adopts the classical energy detection, which can be conveniently implemented in practice [34]. Then, the probability of detection and false alarm can be given as

$$\mathcal{P}_D\left(p_S\right) = \mathcal{Q}\left(\left(\frac{\epsilon}{\sigma_0^2} - \gamma - 1\right)\sqrt{\frac{\tau f_s}{2\gamma + 1}}\right), \tag{1}$$

and

$$\mathcal{P}_F = \mathcal{Q}\left(\left(\frac{\epsilon}{\sigma_0^2} - 1\right)\sqrt{\tau f_s}\right), \tag{2}$$

respectively, where $\gamma = \frac{p_S h_R}{\sigma_0^2}$ is the signal-to-noise ratio for the detection with σ_0^2 being the power of background noise, and ϵ is the predefined threshold for the detection, τ is the detection time, f_s is the sampling frequency for detection, and $\mathcal{Q}$ is the complementary distribution function of Gaussian specified as

$$\mathcal{Q}\left(x\right) = \frac{1}{\sqrt{2\pi}}\int_x^\infty \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t. \tag{3}$$

Note that the probabilities of detection and false alarm depend the contributing factors such as the detection threshold, power of background noise, specific configuration of detection, etc. In this paper, we mainly focus on the power allocation strategies at the legitimate user and jammer. In this respect, The probability of detection only concerns the legitimate power allocation through the detection link. While the probability of false alarm is immune to the legitimate transmission and jamming strategies. As such, we explicitly denote probability of detection as a function of the legitimate power allocation, given as $\mathcal{P}_D\left(p_S\right)$ in (1), and the probability of false alarm is presented without arguments in (2).

Considering the jamming-affected legitimate transmission, the actually achieved SINR can be obtained as $\frac{p_S h_S}{p_J h_J + \sigma_0^2}$. Here we assume the background noise power over all links are identical as σ_0^2, since it is dominated by the jamming signal. The obtained SINR can be regarded as the reward for the legitimate transmissions, which is a crucial metric that further determines the transmission rate, error rate, etc. Towards such a reward, the legitimate user has to consume its limited energy supply, and thus we consider the allocated power as the corresponding cost. As such, we can combine the reward and cost as the basic utility function for the legitimate user, given as

$$u_S = \frac{p_S h_S}{p_J h_J + \sigma_0^2} - c_S p_S, \tag{4}$$

where c_S is the linear coefficient for the power price. The basic utility function here actually provides a tradeoff between the reward and the cost, where the price coefficient can be utilized to tune the tradeoff quantitively based on the sensitivity of power consumption at the legitimate user. On the other hand, for the jammer, whose objective is to deteriorate the legitimate transmission, its achieved reward can be considered as the opposite of legitimate user. Meanwhile, the power consumption is also need for the jammer to conduct the jamming attack. As such, the basic utility function for the jammer can be given as

$$u_J = -\frac{p_S h_S}{p_J h_J + \sigma_0^2} - c_J p_J, \tag{5}$$

where c_J is the coefficient for the power price at the jammer. Consider the potential case of the missed detection of the legitimate transmission and thus the jamming attack is not launched, then the basic utility functions at the legitimate user and the jammer are reduced to $u_S|_{p_J=0} = \frac{p_S h_S}{\sigma_0^2} - c_S p_S$ and $u_J|_{p_J=0} = -\frac{p_S h_S}{\sigma_0^2}$, respectively. On the contrary, for the case of false alarm, the basic utility functions can be obtained as $u_S|_{p_S=0} = 0$ and $u_J|_{p_S=0} = -c_J p_J$, respectively, for the legitimate user and jammer. Therefore, considering all the potential cases regarding whether the legitimate transmission or the jamming is conducted, the achieved basic utility function can summarized in Table 1, where $\{T, NT\}$ denotes whether there is the legitimate transmission, and $\{J, NJ\}$ specifies whether the jamming attack is launched.

TABLE 1. The basic utility functions for the legitimate user and jammer in different cases.

	T	NT
J	$\frac{p_S h_S}{p_J h_J + \sigma_0^2} - c_S p_S, -\frac{p_S h_S}{p_J h_J + \sigma_0^2} - c_J p_J$	$0, -c_J p_J$
NJ	$\frac{p_S h_S}{\sigma_0^2} - c_S p_S, -\frac{p_S h_S}{\sigma_0^2}$	$0, 0$

Note that the cases summarized in Table 1 actually correspond to the scenarios for the rivals being in the states of correct detection, false alarm, missed detection, and both staying idle. Since the performance of detection can be fully characterized by the probability of detection and false alarm specified in (1) and (2), the expected utility function can be obtained as (6) and (7) for the legitimate user and jammer, respectively, by considering all the cases listed in Table 1.

IV. SINGLE-CHANNEL GAME

In this section, we consider the secure IoT communication for the single-channel scenario. We formulate the competi-

$$U_S = \alpha\mathcal{P}_D(p_S)\left(\frac{p_S h_S}{p_J h_J + \sigma_0^2} - c_S p_S\right) + \alpha\left(1 - \mathcal{P}_D(p_S)\right)\left(\frac{p_S h_S}{\sigma_0^2} - c_S p_S\right) \tag{6}$$

$$U_J = \alpha\mathcal{P}_D(p_S)\left(-\frac{p_S h_S}{p_J h_J + \sigma_0^2} - c_J p_J\right) + \alpha\left(1 - \mathcal{P}_D(p_S)\right)\left(-\frac{p_S h_S}{\sigma_0^2}\right) + (1-\alpha)\mathcal{P}_F(-c_J p_J) \tag{7}$$

tion between the legitimate user and jammer as a game. The optimal strategies for both sides are derived by analyzing the game equilibrium.

A. GAME FORMULATION

In (6) and (7), we have derived the expected utility functions[1], and they represent the averaged performance the legitimate user and jammer can achieve. Then, the legitimate user and jammer will seek for the maximization of their respective utility function. Consequently, the problem formulation at legitimate user can be specified as

$$\max_{p_S} \quad U_S \tag{8a}$$

$$s.t. \quad 0 \le p_S \le p_S^{\max}. \tag{8b}$$

Similarly, the problem as the jammer can be given as

$$\max_{p_J} \quad U_J \tag{9a}$$

$$s.t. \quad 0 \le p_J \le p_J^{\max}. \tag{9b}$$

Although the problems given by (8) and (9) appear to be rather simple, they are actually coupled with each other and thus difficult to be solved. In particular, the utility functions for both the legitimate user and jammer concern the strategies of its own and its adversary, yet they can only control the behavior of their own. Furthermore, we know that the explicit jamming action will be conducted after its detection, which suggests that the legitimate transmission actually starts before the jamming attacks. Consequently, we need to model and analyze a sequential decision-making process.

Considering the conflicting interest between the legitimate user and jammer as well as the sequential decision-making process, we exploit the hierarchical game model [29] to formulate their competition. In particular, as the legitimate user takes action first, it is the leader in the game, and thus the jammer is the follower. For such a game model, the follower only needs to react to the leader's strategy, while the leader will jointly consider its own strategy and potential reaction of the follower to reach its own target. In this respect, the leader can exploit the so-called first-mover advantage to have a favorable position in the competition and thus improve the security.

B. EQUILIBRIUM ANALYSIS

As we have introduced before, the game playing is sequential as the legitimate user takes action first, followed by the jammer. To derive the game equilibrium, we resort to the backward induction method to tackle the lower problem at the jammer first, followed by the upper problem solving at the legitimate user.

Based on the backward induction method, we first solve the lower problem at the jammer given in (9) while assuming fixed upper strategy at the legitimate user. In this respect, we can easily very that utility function U_J is concave with respect to the jamming power p_J. Then, we can derive the optimal jamming power by nulling the first-order derivative of the utility function, given as

$$p_J^\star = \begin{cases} \frac{1}{h_J}\left[\sqrt{\frac{\alpha\mathcal{P}_D(p_S)h_S h_J p_S}{c_J[\alpha\mathcal{P}_D(p_S)+(1-\alpha)\mathcal{P}_F]}} - \sigma_0^2\right], & \\ \qquad\qquad \text{if } \frac{\alpha\mathcal{P}_D(p_S)p_S}{\alpha\mathcal{P}_D(p_S)+(1-\alpha)\mathcal{P}_F} \ge \frac{\sigma_0^4 c_J}{h_S h_J}, & \\ 0, \qquad\qquad \text{otherwise.} & \end{cases} \tag{10}$$

For the jamming power specified in (10), we can see that it only conducts the jamming attack when $\frac{\alpha\mathcal{P}_D(p_S)p_S}{\alpha\mathcal{P}_D(p_S)+(1-\alpha)\mathcal{P}_F} \ge \frac{\sigma_0^4 c_J}{h_S h_J}$ holds. For this condition, we can readily observe that the left-hand side is a function of the legitimate transmit power p_S which can be defined as

$$f(p_S) = \frac{\alpha\mathcal{P}_D(p_S)p_S}{\alpha\mathcal{P}_D(p_S) + (1-\alpha)\mathcal{P}_F}. \tag{11}$$

For $f(p_S)$, we can obtain its first-order derivative as

$$\frac{\partial f}{\partial p_S} = \frac{\alpha(1-\alpha)\mathcal{P}_D'(p_S)\mathcal{P}_F p_S}{[\alpha\mathcal{P}_D(p_S) + (1-\alpha)\mathcal{P}_F]^2} + \frac{\alpha\mathcal{P}_D(p_S)}{\alpha\mathcal{P}_D(p_S) + (1-\alpha)\mathcal{P}_F}, \tag{12}$$

where $\mathcal{P}_D'(p_S)$ is the partial derivative of $\mathcal{P}_D$ with respect to p_S given as

$$\mathcal{P}_D'(p_S) = \frac{1}{\sqrt{2\pi}}\exp\left(-\frac{\left(\epsilon/\sigma_0^2 - \gamma - 1\right)^2}{2(2\gamma+1)}\right) \cdot \frac{1}{\sqrt{2\gamma+1}} \cdot \frac{\epsilon/\sigma_0^2 + \gamma}{2\gamma+1} \cdot \frac{h_R}{\sigma_0^2}. \tag{13}$$

We can easily observe that $\mathcal{P}_D'(p_S)$ is always positive and thus $\partial f/\partial p_S$ is positive, which indicates that f is monotonously increasing with respect to p_S. Consequently, we know that the jammer conducts the jamming attack only when the legitimate transmit power is sufficiently high. Here we denote the threshold for this condition as $\hat{p}_S$ such that

$$f(\hat{p}_S) = \frac{\sigma_0^4 c_J}{h_S h_J}. \tag{14}$$

[1] For the following discussions, we will refer to the expected utility function as utility function for brevity.

$$\frac{\partial U_S^C}{\partial p_S} = \frac{a_1\left\{\mathcal{P}_D(p_S)\left[\alpha\mathcal{P}_D(p_S)+(1-\alpha)\mathcal{P}_F\right]+p_S\mathcal{P}_D'(p_S)\left[\alpha\mathcal{P}_D(p_S)+(1-\alpha)\mathcal{P}_F\right]+\alpha p_S\mathcal{P}_D(p_S)\mathcal{P}_D'(p_S)\right\}}{2\sqrt{p_S\mathcal{P}_D(p_S)\left[\alpha\mathcal{P}_D(p_S)+(1-\alpha)\mathcal{P}_F\right]}} + a_2\left(1-\mathcal{P}_D(p_S)\right)-a_2p_S\mathcal{P}_D'(p_S)-a_3, \tag{19}$$

Then, the condition for jamming attack is equivalently to require that $p_S \geq \hat{p}_S$.

Now that we have obtained the optimal jamming strategy for the lower problem with respect to the fixed legitimate transmit power, we can then substitute the obtained results to the upper problem at the legitimate user. As such, the utility function of the legitimate user can be updated as

$$U_S = \begin{cases} U_S^L, & \text{if } 0 \leq p_S < \hat{p}_S, \\ U_S^C, & \text{otherwise,} \end{cases} \tag{15}$$

where

$$U_S^L = \alpha\left(\frac{p_S h_S}{\sigma_0^2} - c_S p_S\right), \tag{16}$$

and

$$U_S^C = a_1\sqrt{p_S\mathcal{P}_D(p_S)\left[\alpha\mathcal{P}_D(p_S)+(1-\alpha)\mathcal{P}_F\right]} + a_2p_S\left(1-\mathcal{P}_D(p_S)\right)-a_3p_S, \tag{17}$$

with

$$a_1 = \sqrt{\frac{\alpha h_S c_J}{h_J}}, \quad a_2 = \frac{\alpha h_S}{\sigma_0^2}, \quad a_3 = \alpha c_S. \tag{18}$$

For the utility function, we can readily notice that, when the legitimate transmit power is low and there is no jamming attack, the utility function U_S in the form of U_S^L is linear with respect to its transmit power. In this case, the maximum allowed transmit power, i.e., $\hat{p}_S$, can be used. On the other hand, when the legitimate transmit power becomes high enough to trigger the jamming attack, the utility function U_S becomes in the form of U_S^C. To investigate its properties, we can obtain its first-order derivative as (19) at the top of the next page, where $\mathcal{P}_D'(p_S)$ is given in (13). Then, we can obtain that[2]

$$\lim_{p_S\to 0} U_S^C = 0, \qquad \lim_{p_S\to\infty} U_S^C = -\infty,$$
$$\lim_{p_S\to 0} \frac{\partial U_S^C}{\partial p_S} = +\infty, \qquad \lim_{p_S\to\infty} \frac{\partial U_S^C}{\partial p_S} < 0. \tag{20}$$

With the conclusions in (20), we can assure the existence of the extreme point for the utility function U_S^C, though the more desired property such as concavity is still missing. To facilitate our discussion, we denote the extreme point as $\tilde{p}_S$. On the other hand, we can prove that

$$U_S^C(\hat{p}_S) = \alpha\left(\frac{\hat{p}_S h_S}{\sigma_0^2} - c_S\hat{p}_S\right) = \lim_{p_S\uparrow\hat{p}_S} U_S^L(p_S). \tag{21}$$

Then, we know that the utility function U_S in (15), although piece-wise, is continuous in the region $\left[0, p_S^{\max}\right]$. By summarizing the discussions above, we know that the maximization of the utility function U_S can be obtained based on the extremes of U_S^L and U_S^C, given as

$$p_S^\star = \max\left\{\hat{p}_S, \tilde{p}_S\right\}, \tag{22}$$

where $\hat{p}_S$ is obtained through (14) and $\tilde{p}_S$ is the extreme point of U_S^C. Note for $\hat{p}_S$ and $\tilde{p}_S$, although we cannot derive the closed-form expression for them, we can resort to the numeric method such as bi-directional search, which allows us to calculate them efficiently.

Now we have obtained the optimal legitimate transmission strategy and jamming strategy for the legitimate user and jammer, respectively. Based on the previous discussions, we have the following conclusion regarding the game equilibrium.

Proposition 1. *The hierarchical security competition game between the legitimate user and reactive jammer under the single-channel scenario always admits the equilibrium.*

Proof: Based on the analysis presented before, we know that the jammer's best-response strategy in (10) is always unique, regardless of the transmit power at the legitimate user. According to [35], the existence of equilibrium for the one-leader-follower game can be confirmed when the follower's optimum is unique. Then we know that our game satisfies this condition, and thus the equilibrium always exists. ■

With confirmed existence of the game equilibrium, we can follow the procedure detailed below to obtain the equilibrium as the solution to the game. Specifically, we first solve for the leader's optimum through (22), denoted by $p_S^\star$. Then, we substitute the leader's strategy into the follower's best response given in (10) to obtain the jammer's optimal strategy as $p_J^\star\left(p_S^\star\right)$. Finally, the strategy profile at both sides, denoted by $\left(p_S^\star, p_J^\star\left(p_S^\star\right)\right)$, constitutes the equilibrium of the game.

V. MULTI-CHANNEL GAME

In this section, we extend our discussion to the multi-channel scenario with the hierarchical game formulation. However, different from the single-channel case where the lower problem admits a closed-form solution, the lower problem under multi-channel transmission is more complicated, and thus the closed-form solution is potentially unavailable. As such, we adopt the MPEC [36] formulation to solve the game equilibrium, for which the detailed discussions are presented below.

[2] Although the utility function U_S^C is currently defined for $p_S \geq \hat{p}_S$, we temparorily extend its definition over the interval $[0, \hat{p}_S)$ for the derivations in (20).

A. GAME FORMULATION

As we consider the multi-channel scenario, we assume that there are N orthogonal channels available, denoted as $\mathcal{N} = \{1, 2, \cdots, N\}$. To be in consistence with the discussions in the preceding sections, we here use the same notations and add the argument-n to specify the variables corresponding to the channel-n. As such, the utility functions for channel-n are denoted as $U_S(n)$ and $U_J(n)$ for the legitimate user and jammer, respectively. Then, the overall utility for the legitimate user and jammer can be defined as the corresponding sum over all channels, i.e., $\mathcal{U}_S = \sum_{n\in\mathcal{N}} U_S(n)$ and $\mathcal{U}_J = \sum_{n\in\mathcal{N}} U_J(n)$.

In accordance with the problem formulation for the single-channel case, the problem for the legitimate user under multi-channel can be specified as

$$\max_{\boldsymbol{p}_S} \quad \mathcal{U}_S = \sum_{n\in\mathcal{N}} U_S(n) \tag{23a}$$

$$s.t. \quad \sum_{n\in\mathcal{N}} p_S(n) \le p_S^{\max}, \tag{23b}$$

$$p_S(n) \ge 0, \quad \forall\, n \in \mathcal{N}, \tag{23c}$$

where $\boldsymbol{p}_S = [p_S(n)]_{n\in\mathcal{N}}$. Similarly, we can denote the problem for the jammer as

$$\max_{\boldsymbol{p}_J} \quad \mathcal{U}_J = \sum_{n\in\mathcal{N}} U_J(n) \tag{24a}$$

$$s.t. \quad \sum_{n\in\mathcal{N}} p_J(n) \le p_J^{\max}, \tag{24b}$$

$$p_J(n) \ge 0, \quad \forall\, n \in \mathcal{N}, \tag{24c}$$

where $\boldsymbol{p}_J = [p_J(n)]_{n\in\mathcal{N}}$. The problems in (23) and (24) are coupled with each other, for which we introduce the hierarchical game to tackle the security competition.

B. EQUILIBRIUM ANALYSIS

Due to the hierarchical structure of the game model, we solve for the game equilibrium by following the idea of backward induction. First, we assume that the strategy of the leader is fixed and solve the lower problem at the jammer. For the jamming problem specified in (24), we can readily have the following observations. In particular, based on the analysis for the single-channel game in the previous section, we know that the utility function at each single channel is a concave function with respect to the jamming power. Then the utility function for the multi-channel game, as the sum utility over all channels, is also concave with respect to the jamming power allocation. Meanwhile, the feasible region of the jamming power is a convex set. Therefore, we know that the jammer's problem in (24) is a concave optimization problem. Then, we can adopt the Lagrange multiplier method, for which the Karush-Kuhn-Tucker (KKT) condition can be given as

$$\begin{cases} 0 \le p_J(n) \;\perp\; \lambda - \dfrac{\partial \mathcal{U}_J}{\partial p_J(n)} \ge 0, \quad \forall\, n \in \mathcal{N}, \\ 0 \le \lambda \;\perp\; p_J^{\max} - \displaystyle\sum_{n\in\mathcal{N}} p_J(n) \ge 0, \end{cases} \tag{25}$$

where λ is the Lagrange multiplier associated with the maximum power constraint, and $0 \le x \perp y \ge 0$ indicates that $x, y \ge 0$ and $x \cdot y = 0$. Then, we can solve the equation set in (25) for the optimal jamming power. To this end, we need to discuss the following two cases depending on whether the maximum jamming power is applied.

Case 1: $\sum\limits_{n\in\mathcal{N}} p_J(n) < p_J^{\max}$, and thus $\lambda = 0$.

In this case, we can apply $\lambda = 0$ to solve (25) and obtain the optimal jamming power for each channel-n as[3]

$$p_J^{\star}(n) = \begin{cases} \frac{1}{h_J(n)} \left[\sqrt{\frac{\alpha \mathcal{P}_D(n) h_S(n) h_J(n) p_S(n)}{c_J[\alpha \mathcal{P}_D(n) + (1-\alpha)\mathcal{P}_F(n)]}} - \sigma_0^2 \right], & \text{if } n \in \mathcal{N}', \\ 0, & \text{otherwise.} \end{cases} \tag{26}$$

where $\mathcal{N}'$ is defined as the channel set such that

$$\mathcal{N}' = \{ n \in \mathcal{N} \,|\, p_S(n) \ge \hat{p}_S(n) \} \tag{27}$$

with $\hat{p}_S(n)$ calculated on each individual channel such that

$$f(\hat{p}_S(n)) = \frac{\sigma_0^4 c_J}{h_S(n)\, h_J(n)}. \tag{28}$$

As we can readily notice, $\mathcal{N}'$ denotes the channels on which the legitimate transmit power is sufficiently high. On these channels, the jammer believes that its jamming power allocation is worth the cost and thus launches jamming attacks. With (26), we have obtained the closed-form expression for the jamming power allocation, which can be regarded as a simple extension of the single-channel game and can be calculated directly.

Case 2: $\sum\limits_{n\in\mathcal{N}} p_J(n) = p_J^{\max}$, and thus $\lambda > 0$.

In this case, we can solve the equation set in (25) and obtain that

$$p_J^{\star}(n) = \begin{cases} \frac{1}{h_J(n)} \left[\sqrt{\frac{\alpha \mathcal{P}_D(n) h_S(n) h_J(n) p_S(n)}{\lambda + c_J[\alpha \mathcal{P}_D(n) + (1-\alpha)\mathcal{P}_F(n)]}} - \sigma_0^2 \right], & \text{if } n \in \mathcal{N}', \\ 0, & \text{otherwise.} \end{cases} \tag{29}$$

where $\mathcal{N}'$ is similarly defined as (27). Note here the jamming power calculation in (29) is parameterized by the Lagrange multiplier λ, for which we can resort to the complementary slackness condition and find that λ satisfies

$$\sum_{n\in\mathcal{N}} p_J^{\star}(n) = p_J^{\max}. \tag{30}$$

Here we can see that although the jamming power allocation in this case has the similar structure with that of *Case 1*, we cannot calculate them directly, because we cannot calculate the Lagrange multiplier with the closed-form expression. However, as we can readily notice that the jamming power allocation in each channel is monotonously decreasing with the Lagrange multiplier according to (29),

[3] As we in this section consider the multi-channel scenario with argument-n to specify the channel, for the probability of detection $\mathcal{P}_D$, we omit the argument of legitimate power allocation to simplify the notation.

we can resort to the numeric method of bi-directional search for the efficient calculation of the Lagrange multiplier through (30). Then, with the obtained Lagrange multiplier, we can calculate the jamming power allocation for each channel based on (29).

Now that we have obtained the optimal jamming policy on condition of the fixed legitimate transmit power, we then consider the strategy design for the legitimate user in the upper problem. In this respect, we need to substitute the jammer's policy as a function of the legitimate power allocation into the problem of the legitimate user. However, as we have shown before, the closed-form solution for the jammer's policy is not always guaranteed. Consequently, we will address the legitimate user's problem for different cases regarding the solution form of the jammer's problem.

Case 1: The lower problem has the closed-form solution.

We can readily know that it corresponds to *Case 1* as we discuss the lower problem before. In this case, the jammer's solution is given in (26) with closed-form expressions. We can substitute the solution given in (26) into the utility function of the legitimate user. Then, the utility function on each channel can be obtained as (15) which is similar to those in the single-channel case. Consequently, we know that the overall utility function for the legitimate user can be obtained as

$$\mathcal{U}_S = \sum_{n\in\mathcal{N}'} U_S^C(n) + \sum_{n\in\mathcal{N}\backslash\mathcal{N}'} U_S^L(n), \tag{31}$$

where $\mathcal{N}'$ is given in (27), and $U_S^L(n)$ and $U_S^C(n)$ are similarly defined as (16) and (17), respectively, specified for each single channel. Then, the upper problem at the legitimate user can be reformulated as

$$\begin{aligned} \max_{\boldsymbol{p}_S} \quad & \mathcal{U}_S = \sum_{n\in\mathcal{N}'} U_S^C(n) + \sum_{n\in\mathcal{N}\backslash\mathcal{N}'} U_S^L(n) & \text{(32a)}\\ s.t. \quad & \sum_{n\in\mathcal{N}} p_S(n) \le p_S^{\max}, & \text{(32b)}\\ & p_S(n) \ge 0, \quad \forall\, n \in \mathcal{N}. & \text{(32c)} \end{aligned}$$

For the problem in (32), we can see that it is the sum of piece-wise functions over all channels. Thus, it may be non-differential over the feasible region, which impedes us to solve it efficiently. To solve the problem in (32), we first consider the problem at each individual channel, and we can calculate $\hat{p}_S(n)$ and $\tilde{p}_S(n)$ that correspond to the threshold legitimate transmit power to trigger the jamming attack and the extreme point for $U_S^C(n)$ for each channel, respectively. Then we can discuss the solution to this problem for the following two subcases.

Subcase 1-1: $\sum_{n\in\mathcal{N}} p_S(n) < p_S^{\max}$.

In this case, the maximum transmit power is not used, and thus we can consider the problem for each channel individually. Based on the discussion for the single-channel case, we can obtain the legitimate transmit power for each channel as

$$p_S^\star(n) = \max\left\{\hat{p}_S(n), \tilde{p}_S(n)\right\}. \tag{33}$$

Note in this subcase, the condition can be equivalently interpreted as

$$\sum_{n\in\mathcal{N}'} \tilde{p}_S(n) + \sum_{n\in\mathcal{N}\backslash\mathcal{N}'} \hat{p}_S(n) < p_S^{\max}. \tag{34}$$

Subcase 1-2: $\sum_{n\in\mathcal{N}} p_S(n) = p_S^{\max}$.

In this subcase, the legitimate user will use the maximum power for the secure transmission. In this regard, we have to jointly consider the power allocation over all the channels. As we can readily notice, for the channels in $\mathcal{N}\backslash\mathcal{N}'$, the corresponding utility function, $U_S^L(n)$, is a linear function. As such, the legitimate user will always adopt the maximum allowable power, i.e., $\hat{p}_S(n)$. Then, the remaining power budget, i.e. $p_S^{\max} - \sum_{n\in\mathcal{N}\backslash\mathcal{N}'} \hat{p}_S(n)$ is used for the channel set $\mathcal{N}'$. Based on the discussions above, we can reformulate problem (32) in this subcase as

$$\begin{aligned} \max_{\boldsymbol{p}_S} \quad & \mathcal{U}_S = \sum_{n\in\mathcal{N}'} U_S^C(n) & \text{(35a)}\\ s.t. \quad & \sum_{n\in\mathcal{N}'} p_S(n) = p_S^{\max} - \sum_{n\in\mathcal{N}\backslash\mathcal{N}'} \hat{p}_S(n), & \text{(35b)}\\ & p_S(n) \ge 0, \quad \forall\, n \in \mathcal{N}'. & \text{(35c)} \end{aligned}$$

For the problem in (35), we can see that the utility function is a continuous and differentiable function, though the concavity cannot be proved. Meanwhile, the feasible region is convex. For this problem, although the classical Lagrange multiplier method cannot be directly used, we can resort to the primal-dual interior point (PDIP) to solve for the optimum effectively. For the detailed discussion of the PDIP method, the readers can refer to a similar discussion presented in [37], [38]. We omit the detailed discussion here as the PDIP procedure is beyond the technical scope of this paper.

Case 2: The lower problem lacks the closed-form solution.

This corresponds to *Case 2* when we discuss the lower problem. In this case, we can only employ the numerical method to calculate optimal jamming power allocation based on (29) and (30). Consequently, we cannot substitute the lower solution into the upper problem directly. To tackle the problem in this case, we resort to the MPEC based analysis. In particular, the MPEC model deals with the optimization problem for which part of its constraints appear in the form of the solution to another optimization. In this regard, we can see that MPEC perfectly fits the hierarchical game as the leader needs to consider the lower optimal for its own strategy design, i.e., dealing with the lower optimal as part of the constraints within its own problem. Specifically, due to the concavity of the lower problem, the KKT condition is equivalent to the optimality of the original problem. As such, we can reformulate the upper problem by exploiting the lower KKT condition as

$$\max_{\boldsymbol{p}_S,\boldsymbol{p}_J} \quad \mathcal{U}_S = \sum_{n\in\mathcal{N}} U_S(n) \tag{36a}$$

$$s.t. \quad \sum_{n\in\mathcal{N}} p_S(n) \le p_S^{\max}, \tag{36b}$$

$$p_S(n) \ge 0, \quad \forall\, n \in \mathcal{N}, \tag{36c}$$

$$\sum_{n\in\mathcal{N}} p_J(n) \le p_J^{\max}, \tag{36d}$$

$$p_J(n) \ge 0, \quad \forall\, n \in \mathcal{N}, \tag{36e}$$

$$0 \le p_J(n) \perp \lambda - \frac{\partial \mathcal{U}_J}{\partial p_J(n)} \ge 0, \quad \forall\, n \in \mathcal{N}, \tag{36f}$$

$$0 \le \lambda \perp p_J^{\max} - \sum_{n\in\mathcal{N}} p_J(n) \ge 0. \tag{36g}$$

Note in problem (36), the upper strategy $\boldsymbol{p}_S$ and lower strategy $\boldsymbol{p}_J$ are both the optimization variables. The channel-specified utility function $U_S(n)$ in the objective adopts its original definition as (6). For the constraints in (36f) and (36g), they represent the lower optimality of the jammer, and thus the problem in (36) is a MPEC problem.

The MPEC problem is inherently difficult to be solved [36]. For the problem in (36), we can see that from the perspective of optimization, it violates the constraint qualification, as the constraints in (36d) and (36g) are linearly dependent. However, as we here consider the case that the jammer adopts the full-power jamming attack, we use the results of $\sum_{n\in\mathcal{N}} p_J(n) = p_J^{\max}$ and $\lambda > 0$ to simplify the MPEC problem. Then, the problem in (36) can be equivalently reformulated as

$$\max_{\boldsymbol{p}_S,\boldsymbol{p}_J} \quad \mathcal{U}_S = \sum_{n\in\mathcal{N}} U_S(n) \tag{37a}$$

$$s.t. \quad \sum_{n\in\mathcal{N}} p_S(n) \le p_S^{\max}, \tag{37b}$$

$$p_S(n) \ge 0, \quad \forall\, n \in \mathcal{N}, \tag{37c}$$

$$\sum_{n\in\mathcal{N}} p_J(n) = p_J^{\max}, \tag{37d}$$

$$p_J(n) \ge 0, \quad \forall\, n \in \mathcal{N}, \tag{37e}$$

$$\frac{\partial \mathcal{U}_J}{\partial p_J(n)} = \lambda, \quad \forall\, n \in \mathcal{N}, \tag{37f}$$

For the optimization in (37), we can see that it satisfies the constraint qualification, as all the constraints are linearly independent. However, for this problem, the objective function is non-concave with respect to the optimization variables and the feasible region is complexly defined by a set of equalities and inequalities. Consequently, we cannot derive the optimal solution with the classical Lagrange method. In this regard, we can resort to the PDIP approach to obtain the optimal solution efficiently. Since the PDIP procedure has little relevance with the technical content in this paper, we omit the details and the readers can refer to [37], [38] for relevant discussions.

Based on the preceding discussions on solving for the optimal strategies at the legitimate user and jammer, we can prove the following conclusion regarding the equilibrium of the multi-channel game.

Proposition 2. *The hierarchical security competition game between the legitimate user and reactive jammer under the multi-channel scenario always admits the equilibrium.*

Proof: This conclusion can be similarly proved as Proposition 1, as we can observe from the previous derivations that the lower problem at the jammer always has the unique solution, which further guarantees the existence of the equilibrium of the game. ■

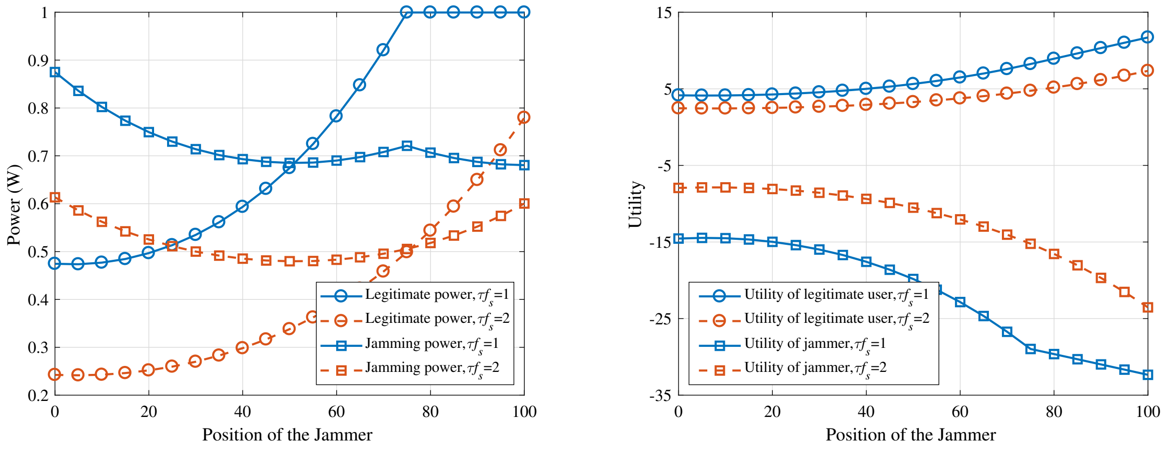
From the previous discussions, we can see that the solution to the optimization problem in (37) is exactly the equilibrium for the hierarchical game. However, this is only the single-sided knowledge at the legitimate user as (37) corresponds the problem at the legitimate user. From the perspective of the actual game playing between the legitimate user and jammer, the legitimate user will first obtain its own optimal transmission strategy through (37), denoted by $\boldsymbol{p}_S^\star$. Then, the jammer will observe the transmission behavior of the legitimate user and apply the results in (26) or (29) to obtain its optimal jamming policy, denoted by $\boldsymbol{p}_J^\star\left(\boldsymbol{p}_S^\star\right)$. Finally, the strategy pair $\left(\boldsymbol{p}_S^\star, \boldsymbol{p}_J^\star\left(\boldsymbol{p}_S^\star\right)\right)$ at both players constitute the equilibrium of the multi-channel hierarchical security game.

VI. SIMULATION RESULTS

In this section, we present the simulation results to evaluate the security performance under our proposal. We assume that the legitimate source node locates at the origin, and the legitimate destination node is with the coordinates $(100, 0)$ (distance in meters). For the jammer, it locates at $(50, -100)$, unless otherwise noted. For the legitimate transmission and jamming, we assume the path loss follows the model $127.1 + 37.6\log_{10}(d[\text{km}])$ (in dB). Also, the wireless communications experience Rayleigh flat fading and the background noise power is -110 dBm. The maximum transmit power for the legitimate user and jamming power for the jammer are both 30 dBm. The probability of active legitimate transmission is 0.8. For the detection at the jammer, we can easily derivate that the probabilities of detection and false alarm satisfy

$$\mathcal{P}_D(p_S) = \mathcal{Q}\left(\sqrt{\frac{1}{2\gamma+1}}\left(\mathcal{Q}^{-1}(\mathcal{P}_F) - \sqrt{\tau f_S \gamma}\right)\right). \tag{38}$$

Then, instead of explicitly setting the detection threshold ϵ, we fix the probability of false alarm as $\mathcal{P}_F = 0.1$. Also, unless otherwise noted, we assume the product of detection time and sampling frequency is 1, i.e., $\tau f_s = 1$. The other relevant simulation parameters will then be introduced for the individual simulation result below.



(a)

(b)

FIGURE 2. The security performance with respect to the position of the reactive jammer. (a) The power allocation at the equilibrium against the position of the jammer. (b) The achieved utility at the equilibrium against the position of the jammer.

A. PERFORMANCE UNDER SINGLE-CHANNEL GAME

We here provide the results under the single-channel security game, which helps reveal the properties of the game equilibrium. First, we inspect the equilibrium strategies for the legitimate user and jammer when the jammer locates at different positions. Specifically, we consider the jammer moves from the coordinates $(0, -100)$ to $(100, -100)$ for the jamming attacks. We assume the power price coefficients at the legitimate user and jammer are 10 and 2, respectively, i.e., $c_S = 10$ and $c_J = 2$. Also, we consider the different detection performance at the jammer, i.e., the cases that $\tau f_s = 1$ and $\tau f_s = 2$, where the latter case corresponds to better detection performance. With the parameters specified above, we obtain the equilibrium of the game and show the results in Fig. 2.

As we can readily infer, when the jammer moves from the coordinates $(0, -100)$ to $(100, -100)$, the detection performance is degraded while the effectiveness of jamming attack is improved, as it locates farther from the legitimate source node while closer to the destination node. Thus, there exists a tradeoff for the jammer's performance to balance between the detection and jamming attacks. Correspondingly, in Fig. 2(a), we can see that the jamming power first decreases and then increases. However, as we can see in Fig. 2(b), the utility of the jammer keeps decreasing as it moves from left to right. This indicates that when the jammer moves rightwards, the improvement in jamming attacks may not be able to compensate the loss due to the degraded detection performance. As such, we can see that the detection prior to jamming attack is critical for the performance of the reactive jammer. For the legitimate user, we can see that the legitimate transmit power keeps increasing in Fig. 2(a), so does its utility as shown in Fig. 2(b). This is because, as the jammer's performance is worsened, the legitimate user can more aggressively exploit the resources to improve its security performance. Besides, we compare the performance for the cases with $\tau f_s = 1$ and $\tau f_s = 2$, for which we know that the detection at the jammer is improved when $\tau f_s = 2$. Then, from the results in Figs. 2(a) and 2(b), we can see that the improved detection allows the jammer to achieve higher utility with less power consumption. Meanwhile, the enhanced jamming performance degrades the secure transmission at the legitimate user. Therefore, we can also observe that the transit power as well as the achieved utility of the legitimate user are lower with improved detection performance at the jammer.

Then, we consider the security performance with respect to different price coefficients of the legitimate transmit power and jamming power. In this respect, we fix the position of the reactive jammer at $(50, -100)$. The results are shown in Figs. 3 and 4. As we can see in Fig. 3, generally, the higher coefficients for legitimate transmit power and jamming power will decrease the corresponding power allocation. This is as expected since the power price is a negative factor for the utility function at both the legitimate user and the jammer. Also, when the price coefficients are sufficiently low, the legitimate user and jammer will adopt the full-power transmission and jamming attack, respectively. To be more specific, for the legitimate transmit power shown in Fig. 3(b), the power price at its own more effectively controls its behavior, while the influence of the jamming power price is not as evident. In contrast, for the jamming power, we can see in Fig. 3(a) that it is significantly affected by power price coefficients at both itself and the legitimate user. This can be explained by the first-mover advantage for the hierarchical game. In particular, as the leader to take action first in the game, the legitimate user can always choose an advantageous position in the security competition. Consequently, although the jamming power price affects the jammer, the legitimate user can compensate its influence by adapting its behavior with the first-mover advantage.

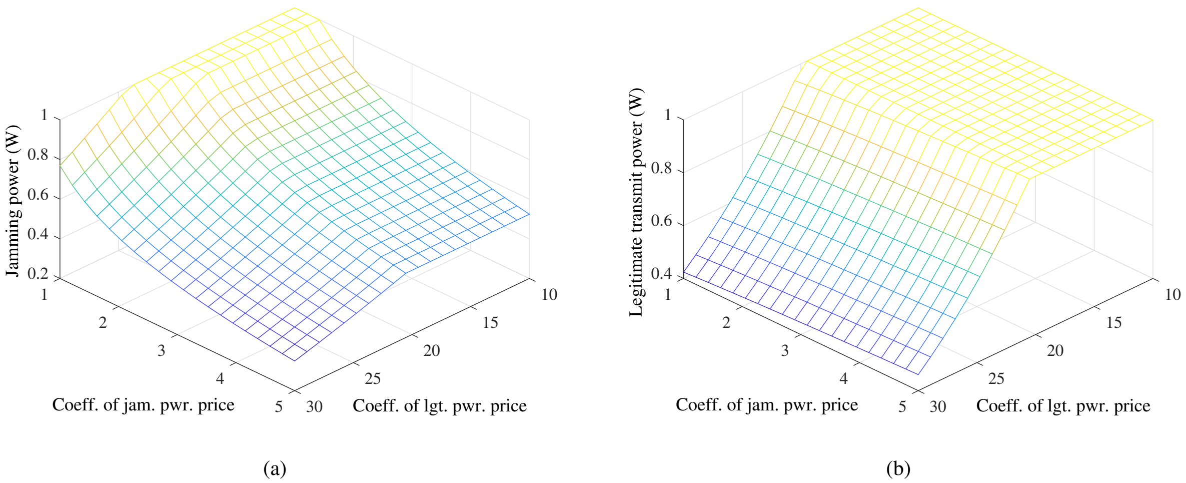


FIGURE 3. The power allocation at the game equilibrium with respect to the price coefficients of legitimate transmit power and jamming power. (a) Jamming power allocation against the price coefficients. (b) Legitimate power allocation against the price coefficients.

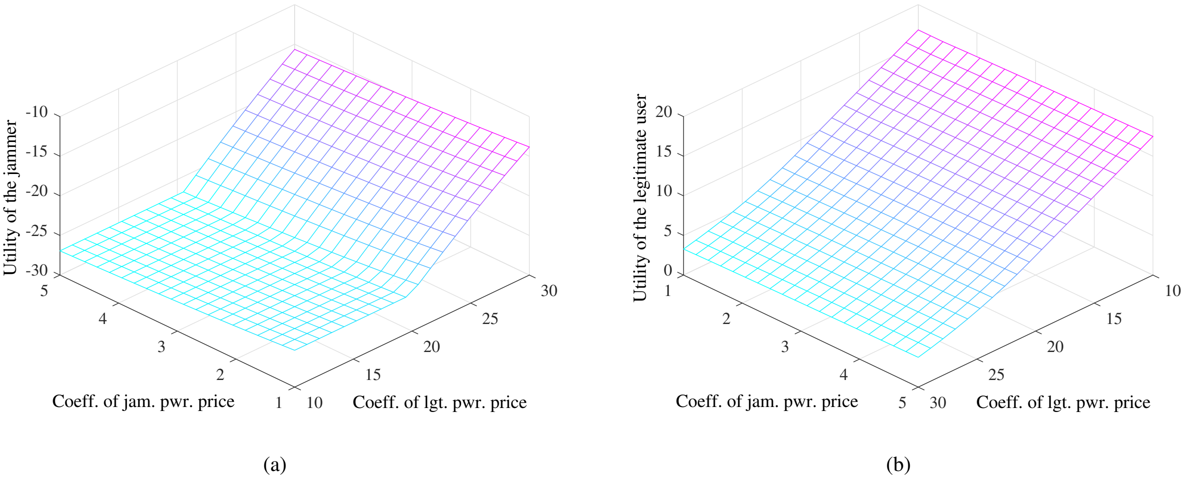
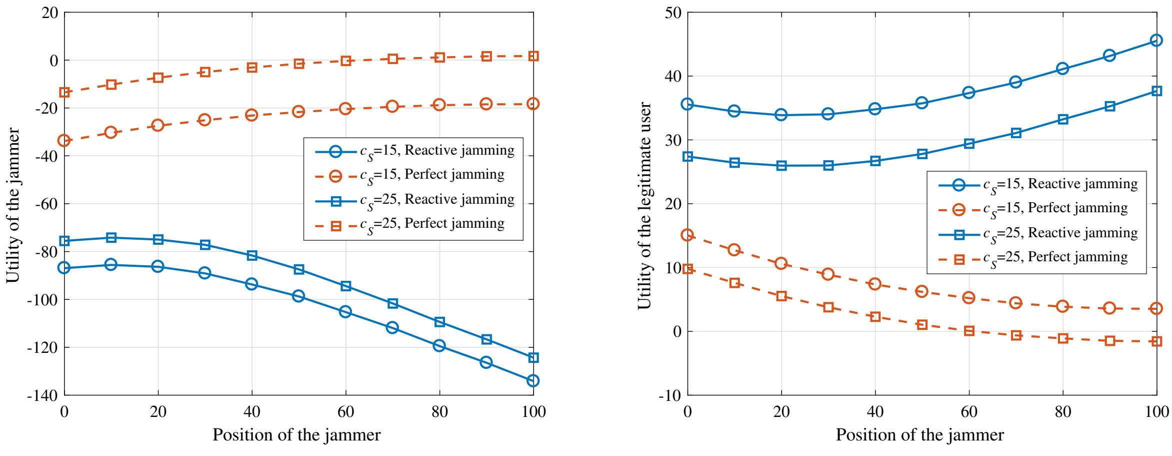


FIGURE 4. The achieved utility at the game equilibrium with respect to the price coefficients of legitimate transmit power and jamming power. (a) Achieved utility of the jammer against the price coefficients. (b) Achieved utility of the legitimate user against the price coefficients.

We show the achieved utilities for both the legitimate user and jammer in Fig. 4, where Fig. 4(a) corresponds the utility of the jammer while Fig. 4(b) is for the utility of the legitimate user. Generally, we can see in Fig. 4(a) that the utility function of the jammer increases with the decreasing price coefficient of jamming power and the increasing price coefficient of the legitimate transmit power. Fig. 4(b) depicts the opposite results in terms of the utility of the legitimate user. This is as expected since the pricing mechanism at any game player has a negative influence at its own while induces positive results if applied at the adversary. Moreover, we can see from Figs. 4(a) and 4(b) that generally, the price coefficient of the legitimate transmit power has more significant influence on the utilities of the legitimate user and jammer as compared with the price coefficient of the jamming power. This can also be explained with the first-mover advantage, similar as the results in Fig. 3. As the leader in the game, the legitimate user is able to affect the game playing directly and more effectively while the jammer as the follower can only passively react to it. Moreover, the leader is able to foresee the potential reaction of the follower, and thus elaborately determines an advantageous action at the first stage of game playing. Additionally, revisit the results in Fig. 3, we can see that when the price coefficient of legitimate power is smaller than 20, the legitimate transmit power saturates as shown in Fig. 3(b). In the meantime, we can see that the jammer has the chance to achieve higher utility by adapting the jamming power. Otherwise, when the price coefficient of legitimate power is higher than 20 and the legitimate transmit power adapts to the jamming strategy, the utility of the jammer is always low.



(a)

(b)

FIGURE 5. The security performance with respect to the position of the jammer and price coefficient of the legitimate transmit power. (a) The utility of the jammer against its position. (b) The utility of the legitimate user against the jammer's position.

B. PERFORMANCE UNDER MULTI-CHANNEL GAME

We extend the performance evaluation to the multi-channel transmission scenario. The basic simulation parameters are identical with those in the previous discussions on the single-channel game while we here assume that there are 5 channels available, i.e., $N = 5$. As we have shown before, the detection performance has significant influence on the reactive jamming. To better evaluate the security performance, we consider the jammer with perfect detection for comparison. In this regard, we have $\mathcal{P}_D(n) = 1$ and $\mathcal{P}_F(n) = 0$, $\forall\, n \in \mathcal{N}$. Correspondingly, the utility functions of the legitimate user and jammer given in (6) and (7) are reduced as

$$U_S = \alpha\left(\frac{p_S h_S}{p_J h_J + \sigma_0^2} - c_S p_S\right), \tag{39}$$

and

$$U_J = \alpha\left(-\frac{p_S h_S}{p_J h_J + \sigma_0^2} - c_J p_J\right), \tag{40}$$

respectively. Then the utility functions $\mathcal{U}_S$ and $\mathcal{U}_J$ under multi-channel transmissions can be similarly defined as the sum utility over all channels. For the game under perfect detection, we can also adopt the hierarchical game formulation and analyze the game equilibrium by following the same procedure as we have presented in the previous sections. The details are omitted here for space limitation.

In Fig. 5, we show the achieved utilities for the legitimate user and jammer when the jammer moves from $(0, -100)$ to $(100, -100)$. Also, we fix the price coefficient of the jamming power at 3, i.e., $c_J = 3$, and consider the cases with the price coefficient of legitimate power being 15 and 25, i.e., $c_S = 15$ and $c_S = 25$. As we can see, for both reactive jamming and the perfect jamming, as the price for legitimate transmit power increases, the utility of the legitimate user is degraded and the utility of the jammer is improved. This is as expected since the legitimate user and jammer have conflicting interest. Meanwhile, as the perfect jamming can be regarded as the extreme case for reactive jamming, we can see that the utility of the jammer under perfect jamming is higher than that under reactive jamming. Correspondingly, the utility of legitimate user under perfect jamming is, as expected, lower than that under reactive jamming. On the other hand, we can see that in Fig. 5(a), as the jammer moves rightwards and thus becomes farther from the legitimate source node while closer to the legitimate destination node, the utility of the jammer under reactive jamming first increases and then decreases. In contrast, the jammer's utility under perfect jamming keeps increasing. The reason is that, as the jammer moves rightwards, the performance of detection is degraded yet the performance of jamming is improved, and thus a tradeoff exists. For a reactive jammer, when it locates too far away from the legitimate source node, the degradation in detection cannot be compensated by the jamming attacks, and thus the overall performance is downgraded. In contrast, for a perfect jammer who is free from the detection error, when it moves rightwards, the jamming link quality is improved, and thus its performance is improved. Fig. 5(b) demonstrates the similar phenomenon that as the jammer moves rightwards, the utility of the legitimate user under reactive jamming first decreases and then increases, while its utility under perfect jamming monotonously decreases.

In Fig. 6, we show the security performance when the jammer moves from the coordinates $(0, -100)$ to $(100, -100)$ with different coefficients of jamming power price, where we fix the price coefficient of the legitimate power as 20, i.e., $c_S = 20$, and consider the cases with the price coefficient of jamming power being 2 and 4, i.e., $c_J = 2$ and $c_J = 4$. As expected, we can see that the utility of the jammer is decreased and the utility of the legitimate user is increased as the jamming power price becomes higher, for both the

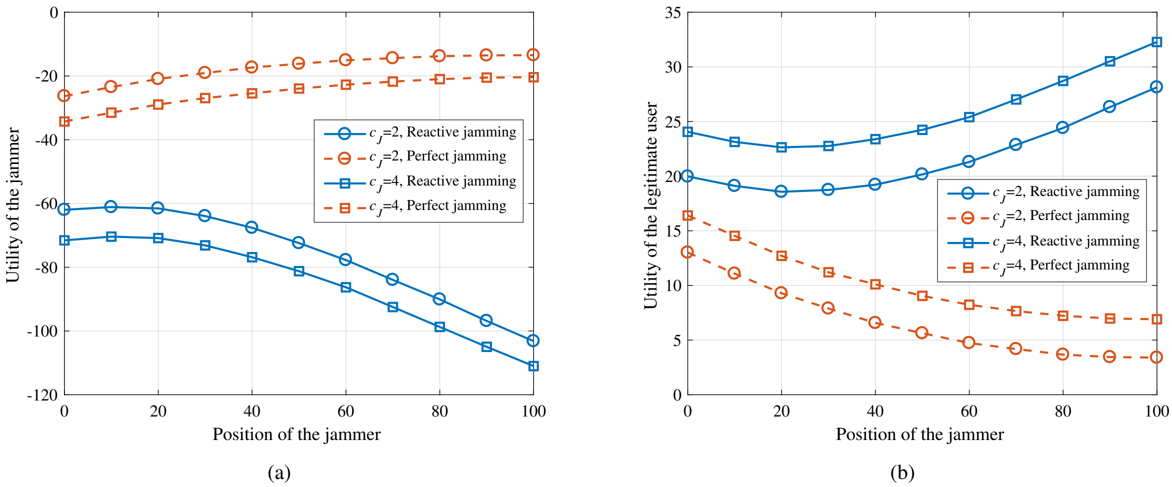


FIGURE 6. The security performance with respect to the position of the jammer and price coefficient of the jamming power. (a) The utility of the jammer against its position. (b) The utility of the legitimate user against the jammer's position.

cases of reactive jamming and perfect jamming. Moreover, similar to the results in Fig. 5, we can see that the utility of the jammer first increases and then decreases as the jammer moves rightwards, as the jammer has to achieve the tradeoff between the detection and jamming to optimize its performance under the reactive jamming strategy. In accordance, the utility of the legitimate user first decreases and then increases as the jammer moves rightwards. While in contrast, the utilities of the legitimate user and jammer are both monotonous as the jammer moves from left to right. Consequently, we can see the paramount importance of detection prior to jamming under the reactive jamming scheme.

VII. CONCLUSIONS

In this paper, we investigate the secure wireless communications for IoT under jamming attacks. In particular, we consider the malicious node in IoT exploits its sensorial capability to perform detection prior to jamming towards more efficient attacks, known as the reactive jamming. To defend against the jamming attack, the legitimate user elaborately determines its transmit power to trade off between the achieved SINR and the probability to be detected and jammed. Meanwhile, the jammer needs to jointly optimize the detection and jamming for the maximum deterioration. The security competition is formulated as a hierarchical game that the legitimate user is the leader and the jammer is the follower. The strategy designs for both sides are proposed based on the analysis on the game equilibrium. With the simulation results, we can observe that the detection at the jammer has a significant influence over the performance of the reactive jamming. Moreover, the legitimate user can exploit the first-mover advantage in the hierarchical game to enhance the secure communications.

REFERENCES

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of things: architecture, enabling technologies, security and privacy, and applications," IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, 4th quart. 2015.

[3] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," Proc. IEEE, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[4] X. Tang, P. Ren, Y. Wang, Q. Du, and L. Sun, "Securing wireless transmission against reactive jamming: a Stackelberg game framework," in Proc. IEEE Global Commun. Conf. (GLOBECOM). San Diego, CA, USA, Dec. 2015.

[5] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of things: a survey of existing protocols and open research issues," IEEE Commun. Surveys Tuts., vol. 17, no. 3, pp. 1294–1312, 3rd quart. 2015.

[6] L. Sun, P. Ren, Q. Du, and Y. Wang, "Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks," IEEE Trans. Ind. Informat., vol. 12, no. 1, pp. 291–300, Feb. 2016.

[7] J. T. J. Penttinen, Wireless Communications Security: Solutions for the Internet of Things. Chichester, UK: John Wiley & Sons, 2016.

[8] S. Amuru, H. S. Dhillon, and R. M. Buehrer, "On jamming against wireless networks," IEEE Trans. Wireless Commun., vol. 16, no. 1, pp. 412–428, Jan. 2017.

[9] Y. Guan and X. Ge, "Distributed secure estimation over wireless sensor networks against random multichannel jamming attacks," IEEE Access, vol. 5, pp. 10 858–10 870, 2017.

[10] H. Rahbari, M. Krunz, and L. Lazos, "Swift jamming attack on frequency offset estimation: the Achilles' heel of OFDM systems," IEEE Trans. Mobile Comput., vol. 15, no. 5, pp. 1264–1278, May 2016.

[11] Ó. Puñal, C. Pereira, A. Aguiar, and J. Gross, "Experimental characterization and modeling of RF jamming attacks on VANETs," IEEE Trans. Veh. Technol., vol. 64, no. 2, pp. 524–540, Feb. 2015.

[12] X. Tang, P. Ren, Y. Wang, and Z. Han, "Combating full-duplex active eavesdropper: a hierarchical game perspective," IEEE Trans. Commun., vol. 65, no. 3, pp. 1379–1395, Mar. 2017.

[13] W. Wang, K. C. Teh, K. H. Li, and S. Luo, "On the impact of adaptive eavesdroppers in multi-antenna cellular networks," IEEE Trans. Inf. Forensics Sec., vol. 13, no. 2, pp. 269–279, Feb. 2018.

[14] Q. Wang, P. Xu, K. Ren, and X. Y. Li, "Towards optimal adaptive UFH-based anti-jamming wireless communication," IEEE J. Sel. Areas Commun., vol. 30, no. 1, pp. 16–30, Jan. 2012.

[15] M. K. Hanawal, M. J. Abdel-Rahman, and M. Krunz, "Joint adaptation of frequency hopping and transmission rate for anti-jamming wireless

systems," IEEE Trans. Mobile Comput., vol. 15, no. 9, pp. 2247–2259, Sep. 2016.

[16] A. O. F. Atya, A. Aqil, S. Singh, I. Broustis, K. Sundaresan, and S. V. Krishnamurthy, "Exploiting subcarrier agility to alleviate active jamming attacks in wireless networks," IEEE Trans. Mobile Comput., vol. 14, no. 12, pp. 2488–2501, Dec. 2015.

[17] S. D'Oro, E. Ekici, and S. Palazzo, "Optimal power allocation and scheduling under jamming attacks," IEEE/ACM Trans. Netw., vol. 25, no. 3, pp. 1310–1323, Jun. 2017.

[18] 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 Trans. Wireless Commun., vol. 14, no. 5, pp. 2337–2352, May 2015.

[19] J. Zhang, H. Zhang, and Z. Cui, "Dual-antenna-based blind joint hostile jamming cancellation and multi-user detection for uplink of asynchronous direct-sequence code-division multiple access systems," IET Commun., vol. 7, no. 10, pp. 911–921, Jul. 2013.

[20] U. Fiore, A. Castiglione, A. D. Santis, and F. Palmieri, "Exploiting battery-drain vulnerabilities in mobile smart devices," IEEE Trans. Sust. Comput., vol. 2, no. 2, pp. 90–99, Apr. 2017.

[21] M. Spuhler, D. Giustiniano, V. Lenders, M. Wilhelm, and J. B. Schmitt, "Detection of reactive jamming in DSSS-based wireless communications," IEEE Trans. Wireless Commun., vol. 13, no. 3, pp. 1593–1603, Mar. 2014.

[22] S. Fang, Y. Liu, and P. Ning, "Wireless communications under broadband reactive jamming attacks," IEEE Trans. Depend. Sec. Comput., vol. 13, no. 3, pp. 394–408, May 2016.

[23] Y. Xuan, Y. Shen, N. P. Nguyen, and M. T. Thai, "A trigger identification service for defending reactive jammers in WSN," IEEE Trans. Mobible Comput., vol. 11, no. 5, pp. 793–806, May 2012.

[24] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "Jamming resilient communication using MIMO interference cancellation," IEEE Trans. Inf. Forensics Sec., vol. 11, no. 7, pp. 1486–1499, Jul. 2016.

[25] M. C. Mah, H. S. Lim, and A. W. C. Tan, "Improved channel estimation for MIMO interference cancellation," IEEE Commun. Letts., vol. 19, no. 8, pp. 1355–1357, Aug. 2015.

[26] M. Lichtman, T. C. Clancy, and J. H. Reed, "FSK-based reactive jammer piggybacking," IEEE Commun. Letts., vol. 21, no. 1, pp. 68–71, Jan. 2017.

[27] X. Liang and Y. Xiao, "Game theory for network security," IEEE Commun. Surveys Tuts., vol. 15, no. 1, pp. 472–486, 1st quart. 2013.

[28] H. Fang, L. Xu, and K.-K. R. Choo, "Stackelberg game based relay selection for physical layer security and energy efficiency enhancement in cognitive radio networks," Appl. Math. Comput., vol. 296, pp. 153–167, 2017.

[29] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, Game Theory in Wireless and Communication Networks. Cambridge, UK: Cambridge University Press, 2011.

[30] D. Yang, G. Xue, J. Zhang, A. Richa, and X. Fang, "Coping with a smart jammer in wireless networks: a Stackelberg game approach," IEEE Trans. Wireless Commun., vol. 12, no. 8, pp. 4038–4047, Aug. 2013.

[31] Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, "Anti-jamming games in multi-channel cognitive radio networks," IEEE J. Sel. Areas Commun., vol. 30, no. 1, pp. 4–15, Jan. 2012.

[32] L. Xiao, J. Liu, Q. Li, N. B. Mandayam, and H. V. Poor, "User-centric view of jamming games in cognitive radio networks," IEEE Trans. Inf. Forensics Sec., vol. 10, no. 12, pp. 2578–2590, Dec. 2015.

[33] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," IEEE Trans. Signal Process., vol. 61, no. 1, pp. 82–91, Jan. 2013.

[34] S. Atapattu, C. Tellambura, and H. Jiang, "Energy detection based cooperative spectrum sensing in cognitive radio networks," IEEE Trans. Wireless Commun., vol. 10, no. 4, pp. 1232–1241, Apr. 2011.

[35] R. Lucchetti, F. Mignanego, and G. Pieri, "Existence theorems of equilibrium points in Stackelberg," Optimization, vol. 18, no. 6, pp. 857–866, 1987.

[36] Z. Luo, J. Pang, and D. Ralph, Mathematical Programs with Equilibrium Constraints. Cambridge, UK: Cambridge University Press, 1996.

[37] R. H. Byrd, M. E. Hribar, and J. Nocedal, "An interior point algorithm for large-scale nonlinear programming," SIAM J. Optim., vol. 9, no. 4, pp. 877–900, 1999.

[38] R. Waltz, J. Morales, J. Nocedal, and D. Orban, "An interior algorithm for nonlinear optimization that combines line search and trust region steps," Math. Program., vol. 107, no. 3, pp. 391–408, 2006.

XIAO TANG (S'14) received his B.S. degree in Information Engineering (Elite Class Named After Tsien Hsue-shen) from Xi'an Jiaotong University, in 2011. He is currently working towards his Ph.D. degree in Information and Communications Engineering at the same university. From September 1, 2015 to August 31, 2016, he worked as a visiting student at the Department of Electrical and Computer Engineering in University of Houston. His research interests include wireless communications and networking, game theory, and physical layer security.

PINYI REN (M'10) received the Ph.D. degree in Electronic and Communications System, the M.S. degree in Information and Communications Engineering, the B.S. degree in Information and Control Engineering, in 2001, 1997, and 1994, respectively, all from Xi'an Jiaotong University, China. He is currently a Professor of Information and Communications Engineering Department, Xi'an Jiaotong University, China. He has published over 100 technical papers on international journals and conferences. He received the Best Letter Award of IEICE Communications Society 2010. He has over 15 Patents (First Inventor) authorized by Chinese Government.

Dr. Pinyi Ren serves as an Editor for the Journal of Xi'an Jiaotong University, and has served as the Leading Guest Editor for the Special Issue of Mobile Networks and Applications on "Distributed Wireless Networks and Services" and the Leading Guest Editor for the Special Issues of Journal of Electronics on "Cognitive Radio". He has served as the General Chair of ICST WICON 2011, and frequently serves as the Technical Program Committee members of IEEE GLOBECOM, IEEE ICC, IEEE CCNC, etc. Dr. Pinyi Ren is a Member of IEEE and IEEE Communications Society.

ZHU HAN (S'01–M'04–SM'09–F'14) received the B.S. degree in electronic engineering from Tsinghua University, in 1997, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, in 1999 and 2003, respectively.

From 2000 to 2002, he was an R&D Engineer of JDSU, Germantown, Maryland. From 2003 to 2006, he was a Research Associate at the University of Maryland. From 2006 to 2008, he was an assistant professor at Boise State University, Idaho. Currently, he is a Professor in the Electrical and Computer Engineering Department as well as in the Computer Science Department at the University of Houston, Texas. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grid. Dr. Han received an NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the Journal on Advances in Signal Processing in 2015, IEEE Leonard G. Abraham Prize in the field of Communications Systems (best paper award in IEEE JSAC) in 2016, and several best paper awards in IEEE conferences. Currently, Dr. Han is an IEEE Communications Society Distinguished Lecturer.