IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 24, 2017, accepted December 25, 2017, date of publication January 9, 2018, date of current version March 16, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2791548

Dynamic Spectrum Access With Physical Layer Security: A Game-Based Jamming Approach

YANJUN YAO[1], WUYANG ZHOU[1], (Member, IEEE), BAOHUA KOU[2], AND YAQI WANG[2]
[1]Key Laboratory of Wireless-Optical Communications, Chinese Academy of Sciences, University of Science and Technology of China, Hefei 230026, China
[2]Beijing Space Information Ralay And Transmission Technology Research Center, Beijing 100008, China

Corresponding author: Wuyang Zhou (wyzhou@ustc.edu.cn)

This work was supported by the Key Program of the National Natural Science Foundation of China under Grant 61631018.

ABSTRACT The paper investigates the issue of physical layer security in spectrum overlay networks. First, in order to enhance security performance of the primary system, the secondary users are motivated to act as friendly jamming nodes with the compensation of access to the primary system's spectrum opportunistically. Considering the non-altruistic or rational attribute in practice, we propose a cooperative jamming approach based on Stackelberg game, while primary users acting as the game leader, and secondary users constituting the follower. Under the proposed framework, we design a new mechanism that the secondary users transmit jamming signals according to a pre-determined probability, in order to maximize their own data rate priced by the invested power. To be specific, the more accessible spectrum opportunities, the larger possibility that secondary users would jam. For primary users, their traffic load can be tuned so as to squeeze spectrum holes for secondary access. Therefore, the considered system is dynamic and either primary users or secondary users can operate in the channel. We employ continuous-time Markov chain to explicitly model the system's evolutionary behaviors. Under the proposed scheme, the optimal strategies of primary and secondary users, which are jointly referred to as Stackelberg equilibrium, are analyzed in details. Finally, we demonstrate the performance of the proposed scheme by numerical simulations.

INDEX TERMS Spectrum overlay, physical layer security, game, jamming.

I. INTRODUCTION

With the ever increasing types of new wireless applications, the demand for spectrum resources is becoming insatiable. Under this circumstance, it's universally acknowledged that the advent of cognitive radio has become a promising way to resolve the issue of limited spectrum resources [1]. In a cognitive radio network (CRN), the unauthorized users are granted to access the spectrum dynamically, under the condition that the interference caused by secondary users to primary users should below an acceptable level. A wealth of works can be found in the current literatures focusing on dynamic spectrum access (DSA) [2]–[5]. These works can be summarized as two categories: spectrum underlay and spectrum overlay [6]. The former allows primary and secondary users share the spectrum band simultaneously, while limiting the transmission power of secondary users under interference temperature [7]. On the other hand, the latter is also called Opportunistic Spectrum Access (OSA) [6], which means that secondary users can only share the spectrum band when primary users are idle. To sum up, the band is occupied by primary users continuously in spectrum underlay system, and the related research issue should be constrained to interference temperature which is caused by secondary users. However, in spectrum overlay system, secondary users keep on sensing primary users' activities and access the band if sensed as idle. In essence, restrictions of the two systems are totally different. This paper falls into the second category.

The issue of security in cognitive radio networks has attracted tremendous attention in recent years [8], [9]. Unlike key-based enciphering at the upper layer, physical layer security has hewn out a completely new way to achieve secure communication. The pioneering work can be traced to Wyner from an information-theoretic perspective. He introduced the wiretap channel and revealed that a non-zero secrecy rate can be achieved if the eavesdropper's channel is worse than the legitimate receiver's [10]. Recently, a flurry of works has been emerged concentrating on physical layer security in cognitive radio networks, especially on spectrum underlay

system for licensed band [11]–[14] or spectrum sharing system for common band [15]. Ouyang *et al.* [11], focused on secure transmission with energy efficiency in underlay cognitive radio networks. In [12], the underlay network was also examined, where a secondary user transmitter sends confidential messages to multiple secondary receivers at the presence of primary users. The paper tried to exploit multiuser diversity where the secondary link with best channel condition is scheduled for transmission. Zhang *et al.* [13], considered the physical layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system. Zou *et al.* [14], examined a cognitive radio network that consists of multiple secondary users. The paper proposed a multiuser scheduling method to enhance the security performance of cognitive transmissions with a primary user's quality of service constraint. Zou [15], investigated the physical layer security in a spectrum sharing system, where multiple coequal source-destination pairs access the common spectrum band dynamically.

Anti-jamming attack on secondary users (SUs) in spectrum overlay networks has attracted tremendous attention in recent years [16]–[19]. In [16], the jamming and anti-jamming process has been modeled as a Markov decision process, and SUs are able to avoid the jamming attack launched by malicious users and therefore maximize the payoff function. Wang *et al.* [17] have studied the design of anti-jamming defense mechanism in a cognitive radio network. The interactions between the secondary users and the attackers were modeled as a stochastic zero-sum game. In [18], similar work was done by the same group as [17]. Tan *et al.* [19] considered the anti-jamming issue in IEEE 802.22 networks, where SUs are designed to utilize the unused or underutilized TV bands dynamically. However, few works have focused on traditional security threats in spectrum overlay networks, e.g.,eavesdropping. In [20], interactions between secondary users and eavesdroppers were formulated as a non-cooperative game, in order to improve the security performance of secondary transmissions. The paper considered multiple licensed channels, which can be accessed by SUs when they are idle. Due to primary users' activities, each channel's availability for SUs was simply assumed as a fixed probability.

Since in cognitive radio networks, primary and secondary users usually belong to two different entities, it is reasonable to assume they are rational or selfish in nature. Therefore, game-based theoretic method is becoming prevalent because it's suitable to analyze non-altruistic behaviors. In [21], the interference channel which allows primary and secondary users transmit simultaneously was considered. The authors employed Stackelberg game to model the interaction between primary users and secondary users. Zhang *et al.* [22], considered a spectrum underlay system, where multiple device-to-device links can access the licensed resource blocks. A coalitional game was formulated in order to motivate the cooperation among cellular communication links and device-to-device pairs. In [23], via spectrum leasing, the unlicensed users are inspired to act as jamming node to improve the secrecy rate of primary system. Stackelberg game was also adopted to investigate the cooperation. In [24], a multilevel Stackelberg game was used for cooperation between the primary user and the secondary user so as to facilitate physical layer security.

In the before-mentioned literatures, either spectrum underlay or spectrum leasing system was considered. A general assumption in these works is that the primary users are always filled with packets to transmit. In fact, when considering security issue in cognitive radio networks, the pursuits of primary and secondary users may be different. As authorized group, the primary users tend to concern its secrecy rate, rather than transmission rate. On the other hand, due to the valuable spectrum opportunity, it's reasonable to assume that secondary users are more interested in maximizing their data rate. Stimulated by this thought, this paper designs a cooperation framework, in which the primary users can adjust their service load, so that the spectrum band can be vacated for secondary access opportunistically. In reward for the access, secondary users act as jamming nodes during primary user's transmission. The contributions of this paper are summarized as follows:

Firstly, quite distinct from the literatures above, we endeavor to improve security performance against eavesdropping in spectrum overlay networks. It is primary user's service characteristics that should be concerned in spectrum overlay system, which is one contribution of the paper that is not considered in related literatures. Specifically, we assume that primary system's traffic load can be tuned so as to squeeze spectrum holes for secondary users. Taking into account of primary user's service activities, we develop a dynamic spectrum access scheme based on continuous-time Markov chain, by which the system's evolutionary behavior can be thoroughly captured.

Secondly, considering the non-altruistic or rational attribute in practice, we propose a cooperative jamming approach based on Stackelberg game, with the primary users acting as the game leader, and the secondary users constituting the follower.

Thirdly, we apply artificial noise (AN) based jamming scheme for secondary users. The AN-based method does not require the channel state information (CSI) of eavesdroppers, which is different from [23]. Moreover, a new idea is put forward that the secondary users transmit jamming signals according to a pre-determined probability, in order to maximize their own data rate priced by the invest power. To be specific, the more spectrum accessible opportunities, the larger possibility that secondary users would jam.

The remainder of this paper is organized as follows. In Sec. II, the system model is introduced. In Sec. III, game-based jamming scheme is presented with theoretical analysis. In Sec.IV, numerical results are presented to evaluate the performance of the proposed scheme. Sec.V concludes this paper.

II. SYSTEM SCENARIO AND DSA SCHEME BASED ON MARKOV THEORY

In this section, we introduce the considered scenario and system assumptions in Sec.II-A, dynamic spectrum access scheme based on CTMC in Sec.II-B and performance metrics in Sec.II-C.

A. SYSTEM SCENARIO AND NOTATIONS

We consider a dynamic spectrum access network, which consists of one primary user pair and two secondary users. Specifically, we denote the primary transmitter and receiver as PUt and PUr, respectively. The two secondary users, which are denoted as A and B, transmit their packets to a cognitive base station (CBS). The configuration can be extended to multi-secondary users, which is not the focus of this paper. In addition, there is one eavesdropper, denoted as E, endeavors to intercept primary transmission. It's assumed that each node is equipped with one omni-antenna. The system scenario is shown as Fig.1.

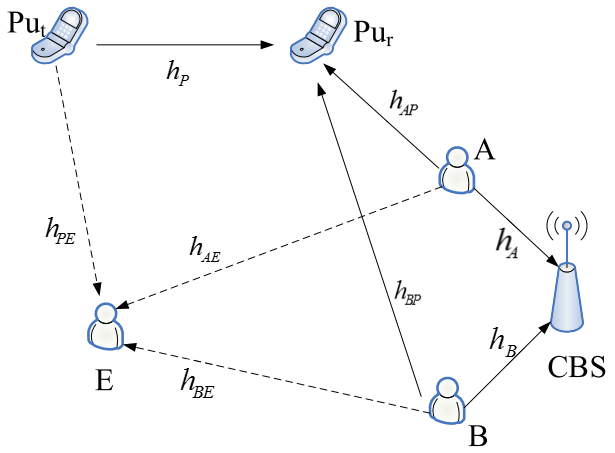

FIGURE 1. System scenario.

The channel gains between nodes are modeled as independent complex Gaussian random variables. To be more specific, the instantaneous channel coefficients of the links $PUt-PUr, PUt-E, A-E, B-E, B-PUr, A-PUr, B-CBS$, $A-CBS$ are denoted as $h_p, h_{PE}, h_{AE}, h_{BE}, h_{BP}, h_{AP}, h_B, h_A$, respectively. Independent additive white Gaussian noise at PUr, E, CBS for A and B are denoted as n_p, n_e, n_A, n_B, with variance σ_p^2, σ_e^2, σ_A^2, σ_B^2, respectively. We denoted transmit power for user P, A (or B) as P_{pu} and P_{su}, respectively. With the same priority, it's reasonable to assume that secondary users A and B have the same transmission ability.

B. DYNAMIC SPECTRUM ACCESS SCHEME BASED ON CTMC

1) SERVICE DESCRIPTION

For the primary user, we model the arrival traffic as a Poisson process with rate λ_p [25]. The service duration is negative-exponentially distributed with mean time $1/\mu_p$. Therefore, the departure of primary user's traffic is another Poisson process with rate μ_p. In addition, the traffic load of primary user, namely λ_p/μ_p, can be tuned such that spectrum opportunities can be squeezed for secondary users.

As discussed in previous section, it is assumed that the secondary users are always hunger for data transmission. Therefore, once the channel is sensed as idle, the CBS will schedule the user (A or B) with the best signal to noise ratio (SNR) for spectrum access. It should be noted that other scheduling methods, such as proportional fair criterion, decentralized competitive method, can also be adopted in the DSA scheme. The scheduling method itself is not the main focus of this paper.

2) AN-BASED JAMMING

When primary user's service arrives, secondary users should stop their own data transmissions and switch to jamming mode. We apply the conventional artificial noise interference into the cooperation. The reason for choosing the AN method mainly lies in the fact that AN can be designed only to interfere with the eavesdropper if the antenna number of the legitimate user is more than that of eavesdropper [26]. Therefore, it's not indispensable to achieve the CSI of eavesdropper, which is practical in passive eavesdropping.

During the phase of primary transmission, we denote the desired signal as x_p, which will be sent from PUt to PUr. Meanwhile, the artificial noise vector is denoted as $\boldsymbol{\omega} = [\omega_A, \omega_B]$, where $\omega_i (i = A, B)$, is to be transmitted by A and B. Hence, the received signal at PUr can be expressed as:

$$y_p = \sqrt{P_{pu}} h_P x_p + \sqrt{P_{su}} h_{AP} \omega_A + \sqrt{P_{su}} h_{BP} \omega_B + n_p. \quad (1)$$

Furthermore, the AN vector $\boldsymbol{\omega}$ should be designed only to interfere with the eavesdropper, which implies:

$$h_{AP}\omega_A + h_{BP}\omega_B = 0, \quad (2)$$

for $\boldsymbol{\omega} \neq 0$. The constraint specified in Eq. 2 can be easily satisfied when there are more than two secondary users.

Meanwhile, the received signal at the eavesdropper can be expressed as:

$$y_e = \sqrt{P_{pu}} h_{PE} x_p + \sqrt{P_{su}} h_{AE} \omega_A + \sqrt{P_{su}} h_{BE} \omega_B + n_e. \quad (3)$$

Due to the fact that the channel coefficients h_{AE}, h_{BE}, are independent of h_{AP} and h_{BP}, the AN vector $\boldsymbol{\omega}$ will produce harmful interference for eavesdropper E, i.e. $h_{AE}\omega_A + h_{BE}\omega_B \neq 0$.

Therefore, with cooperative jamming, the achievable secrecy rate of primary user can obtained as:

$$R_1 = \left[\log_2\left(1 + \frac{P_{pu}|h_P|^2}{\sigma_p^2}\right) - \log_2\left(1 + \frac{P_{pu}|h_{PE}|^2}{P_{su}|h_{AE}|^2 + P_{su}|h_{BE}|^2 + \sigma_e^2}\right) \right]^+, \quad (4)$$

where $[x]^+$ denotes $\max\{0, x\}$. On the other hand, if secondary users are idle during primary transmission,

the achievable secrecy rate can obtained as:

$$R_2 = \left[\log_2(1+\frac{P_{pu}|h_P|^2}{\sigma_p^2}) - \log_2(1+\frac{P_{pu}|h_{PE}|^2}{\sigma_e^2})\right]^+. \quad (5)$$

3) DSA SCHEME WITH CTMC MODELING

The DSA scheme is developed with CTMC modeling, which exists three states according to different channel occupations, as illustrated in Fig.2. State 1 means secondary user (A or B) transmits its own information in the channel, state 2 indicates the channel is occupied by primary user P without friendly jamming, while state 3 means the channel is occupied by P with secondary users transmitting jamming signals.

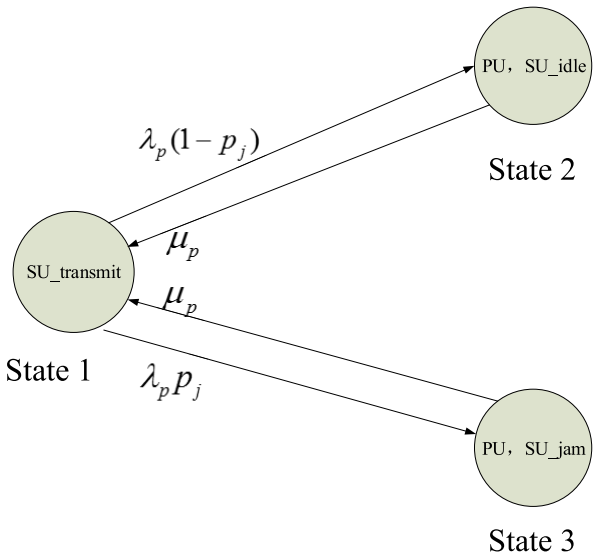

FIGURE 2. System state transition for DSA.

CBS keeps on sensing the spectrum band and schedules secondary user with the best SNR. Due to user P's priority, secondary user's traffic should be promptly discarded once user P's service arrives. The probabilistic jamming scheme is proposed, which implies that secondary users transmit jamming signals according to a pre-determined probability. As a result, secondary users have more freedom in negotiating with primary system. The jamming signal is controlled by probability p_j , therefore, the rate that the chain transits from state 1 to state 3 can be obtained as $\lambda_p p_j$. On the other hand, the system transition rate from state 1 to state 2 can be calculated as $\lambda_p(1-p_j)$. Once user P's service is completed, the CBS would promptly schedule the best user to utilize the band. As a result, both state 2 and 3 transit to state 1 with the rate of μ_p.

C. PERFORMANCE METRICS

The "flow-balance" (the rate transitions out of state S equals to the rate transitions into state S) and the normalization equations governing the above system are given below [5]:

$$H\prod^T = 0, \quad (6)$$

$$\pi_1 + \pi_2 + \pi_3 = 1. \quad (7)$$

In the above equations, $\boldsymbol{H}$ is the matrix that characterizes the transition states of the Markov chain. $\prod = [\pi_1, \pi_2, \pi_3]$ is the steady state probability vector, where π_i means that system is in state $i(i = 1, 2, 3)$. Through solving Eq. 6 and Eq. 7, π_i is given by

$$\pi_1 = \frac{\mu_p}{\mu_p + \lambda_p}, \quad (8)$$

$$\pi_2 = \frac{\lambda_p(1-p_j)}{\mu_p + \lambda_p}, \quad (9)$$

$$\pi_3 = \frac{\lambda_p p_j}{\mu_p + \lambda_p}. \quad (10)$$

The primary user aims to maximize its average secrecy rate, which is expressed as follows:

$$U_p = \pi_2 R_2 + \pi_3 R_1. \quad (11)$$

From the secondary users' point of view, their utility is defined as the achievable data rate during the spectrum opportunities, priced by the total invested power in the cooperative jamming [23]:

$$U_s = \pi_1 R_{su} - 2cP_{su}\pi_3. \quad (12)$$

In the above equation, c is the cost per unit transmission power, and according to the best SNR rule, the secondary communication rate is given by

$$R_{su} = \max_{i\in(A,B)} \log_2(1+\frac{P_{su}|h_i|^2}{\sigma_i^2}). \quad (13)$$

III. STACKELBERG GAME MODEL

Considering the formulated utilities of primary and secondary parties, the Stackelberg game model is proposed, where primary user acts as the leader and secondary users act as the follower. Then, Stackelberg equilibrium is analyzed.

A. STACKELBERG GAME MODEL

Throughout this work, the nodes are defined as selfish and rational to mimic a non-altruistic behavior. An appropriate framework for analyzing the interaction between such nodes is Stackelberg game [23]. Because primary user is authorized to operates in the spectrum band, it's reasonable to assume that the game leader and follower are the primary user and secondary users. In the defined setting, the follower acts in regards to the strategy chosen by the leader, which affects the leader's choice in return.

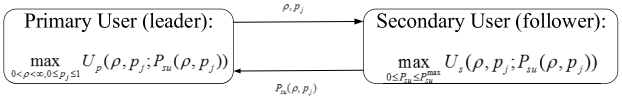

FIGURE 3. Interaction of the game.

The interaction between primary and secondary users is illustrated in Fig. 3. The primary user's strategy is denoted as (ρ, p_j), where ρ is load factor termed as λ_p/μ_p. The secondary system is aware of (ρ, p_j), and optimizes its

transmission power towards the goal of maximizing its own utility, given by Eq. 12.

B. SOLUTION TO THE GAME

1) SECONDARY USER's STRATEGY

The secondary users calculate the transmission power, so that their utility can be maximized.

$$\max_{0\le P_{su}\le P_{su}^{\max}} U_s(\rho, p_j; P_{su}(\rho, p_j)). \tag{14}$$

Lemma 1: U_s in Eq. 14 is convex in terms of P_{su}.

Proof: To determine the concavity, we derive the second derivative of U_s with respect to P_{su} as follows:

$$\frac{\partial^2 U_s}{\partial^2 P_{su}} = \frac{-\gamma^2}{\ln 2 \cdot (1+\rho)(1+P_{su}\gamma)^2}, \tag{15}$$

where $\gamma = \max_{i\in(A,B)} \frac{|h_i|^2}{\sigma_i^2}$. Obviously, the derivative of U_s in Eq. 15 is negative. Therefore, U_s in Eq. 14 is convex in terms of P_{su}.

According to Lem. 1, we can get the optimal P_{su}^* by solving the following equation:

$$\frac{\partial U_s}{\partial P_{su}} = \frac{1}{\ln 2(1+\rho)} \cdot \frac{\gamma}{1+P_{su}\gamma} - 2cp_j\frac{\rho}{1+\rho} = 0. \tag{16}$$

As a result, the optimal P_{su}^* can be obtained as:

$$P_{su}^* = \frac{1}{2\ln 2c\rho p_j} - \frac{1}{\gamma}. \tag{17}$$

It's obvious that the condition $2\ln 2c\rho p_j \le \gamma$ should be satisfied for jamming participation. ■

2) PRIMARY USER's STRATEGY

According to Stackelberg game theory, primary user is able to predict secondary system's choice of P_{su}^*. In response, it tries to find its optimal strategy (ρ^*, p_j^*), by maximizing its own utility which can be expressed as follows:

$$\max_{0<\rho<\infty, 0\le p_j\le 1} U_p(\rho, p_j; P_{su}^*(\rho, p_j)). \tag{18}$$

U_p in Eq. 18 can be transformed into the following expression:

$$U_p(\rho, p_j) = \frac{\rho(1-p_j)}{1+\rho}R_2 + \frac{\rho p_j}{1+\rho}\left[\log_2(1+\frac{P_{pu}|h_P|^2}{\sigma_p^2}) - \log_2(1+\frac{P_{pu}|h_{PE}|^2}{P_{su}|h_{AE}|^2 + P_{su}|h_{BE}|^2 + \sigma_e^2})\right]. \tag{19}$$

For mathematical convenience, we denote the following variables:

$$\begin{aligned} U_p(\rho, p_j) &\triangleq f(x, y), \\ x &\triangleq \rho, \\ y &\triangleq p_j, \end{aligned}$$

$$\begin{aligned} M &= \frac{P_{pu}|h_P|^2}{\sigma_p^2}, \\ N &= P_{pu}|h_{PE}|^2, \\ L &= \frac{2c\ln 2}{|h_{AE}|^2 + |h_{BE}|^2}, \\ Q &= \frac{|h_{AE}|^2 + |h_{BE}|^2}{\gamma}, \\ G &= \sigma_e^2, \end{aligned}$$

where $x \in (0, \infty)$, $y \in [0, 1]$, $\frac{1}{Lxy} - Q \ge 0$.

Therefore, we get the following expression:

$$f(x, y) = \frac{x(1-y)}{1+x}R_2 + \frac{xy}{1+x}u(x, y), \tag{20}$$

where $u(x, y) = log_2(1+M) - log_2(1+\frac{N}{(\frac{1}{Lxy}-Q)+G})$.

Let $z = xy$, the following expression can be obtained:

$$f(x, z) = \frac{R_2 x}{1+x} - \frac{R_2 z}{1+x} + \frac{z}{1+x}u(z), \tag{21}$$

where $u(z) = m - \log_2\frac{1+bz}{1+az}$, $m = log_2(1+M)$, $a = LG - LQ$, $b = LG - LQ + LN$, and $0 \le z \le \frac{1}{LQ}$, $z \le x < \infty$.

Lemma 2: $f(x, z)$ is convex and has unique maximum value in terms of z.

Proof: See in Appendix.

The closed form of maximization can't be easily obtained. However, the problem can be solved efficiently by numerical analysis, such as gradient descent algorithm [27]. We denote the optimum solution as z_0.

The following step is to find optimal x, such that $f(x, z_0)$ is maximized.

$$\frac{\partial f}{\partial x}\Big|_{z=z_0} = \frac{R_2 + R_2 z_0 - z_0 u(z_0)}{(1+x)^2}. \tag{22}$$

If $\frac{\partial f}{\partial x}\Big|_{z=z_0} > 0$, $f(x, z_0)$ is monotone increasing in terms of x. Then x should be infinite and $y = 0$, which means load factor ρ is infinite and $p_j = 0$. In other words, no cooperation between primary and secondary users becomes the best strategy.

If $\frac{\partial f}{\partial x}\Big|_{z=z_0} \le 0$, $f(x, z_0)$ is monotone decreasing in terms of x. Then x should be equal to z_0 and $y = 1$, which means load factor ρ is z_0 and $p_j = 1$.

IV. NUMERICAL RESULTS

In this section, we evaluate the performance of the proposed scheme with computer simulations. Unless otherwise stated, the parameters used are: $|h_P|^2 = |h_{PE}|^2 = |h_A|^2 = |h_B|^2 = |h_{AE}|^2 = |h_{BE}|^2 = 0.5$, $|h_{AP}|^2 = |h_{BP}|^2 = 0.1$, $\sigma_A^2 = \sigma_B^2 = \sigma_P^2 = 0.1$, $\sigma_E^2 = 0.6$, $P_{pu} = 4$ [mw], $c = 0.25$ [bit/sec/Hz/mW]. The simulations consist of two steps as follows: Firstly, the optimal strategies of the game participators are depicted in terms of different factors. Following that, the performance of the proposed scheme is evaluated through comparison with Power-control scheme in [23] through numerical simulations.

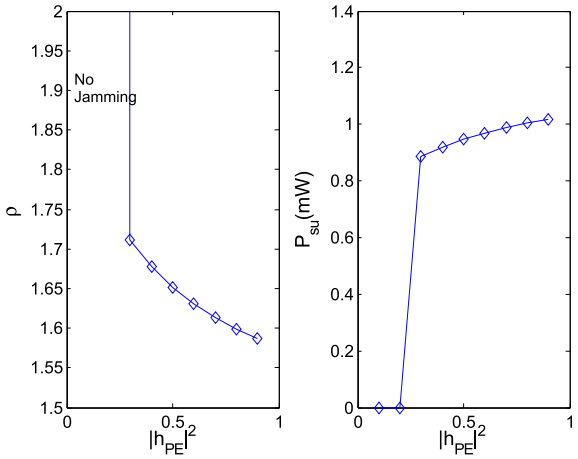

FIGURE 4. Load factor ρ and secondary power P_{su} vs. $|h_{PE}|^2$.

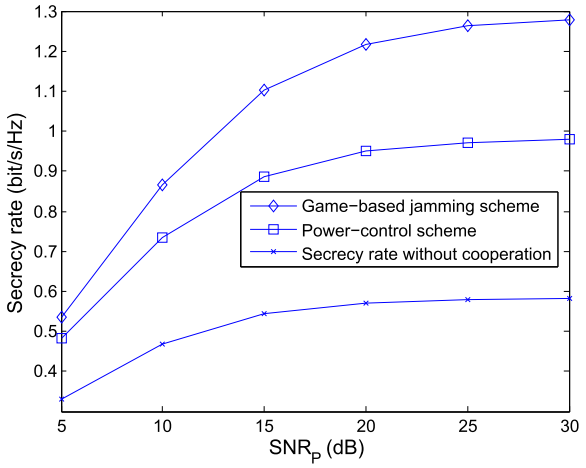

FIGURE 6. Primary user's secrecy rate vs. its SNR.

Fig. 4 shows load factor ρ and secondary transmission power P_{su} with different $|h_{PE}|^2$. As can be observed from the figure, there is no cooperation when $|h_{PE}|^2$ is less than 0.2. This is attributed to the fact that no jamming is favorable for both of primary and secondary users, which has been discussed in Sec. III. As $|h_{PE}|^2$ grows lager, it's better for user P to allocate more spectrum opportunities for secondary users, so that secondary users are stimulated to transmit more jamming power, and thus, leading to the decrease of ρ and increase of P_{su}. For the same reason, ρ decreases as user P's SNR increases, while secondary jamming power P_{su} increases as the SNR increases, which is illustrated in Fig. 5.

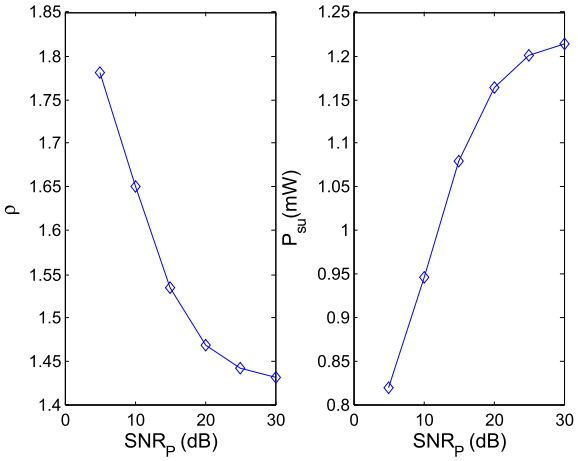

FIGURE 5. Load factor ρ and secondary power P_{su} vs. SNR of P.

We evaluate the performance of the proposed method by comparing it with Power-control scheme in [23]. In the reference, multiple cooperative jammers are employed and competition between them is formulated as a non-cooperative power control game. Besides, the interaction between source and jammer is also formulated as Stackelberg game. The reason why we choose Power-control scheme as benchmark lies in the fact that the method is representative, and furthermore, the studied system is similar to ours which justifies the comparison. For fairness, the setting for Power-control scheme is the same as the configuration described before.

Fig. 6 shows secrecy rate with different user P's SNR under different schemes. It's nature to see that as the SNR increases, primary user's secrecy rate also increases. In addition, it also shows that our proposed game-based jamming method outperforms the Power-control scheme significantly because the interference is removed at the receiver under AN jamming. It also can be observed that both of the two schemes outperform the one without cooperation. Fig. 7 shows secrecy rate with different $|h_{PE}|^2$. As can be seen from the figure that secrecy rate decreases as eavesdropper's channel becomes better. It also can be seen that secrecy rate under our proposed scheme is higher than that under Power-control scheme for the same reason as Fig. 6's observation.

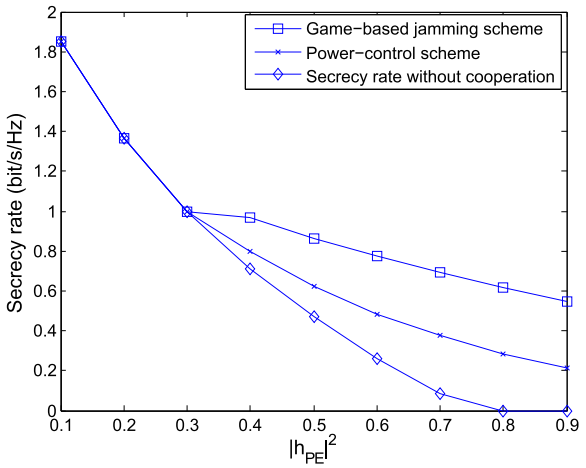

FIGURE 7. Primary user's secrecy rate vs. $|h_{PE}|^2$.

Fig. 8 depicts secondary users' utility with different primary user P's SNR. P would lower its load factor as SNR increases, which had been demonstrated in Fig. 5. As a

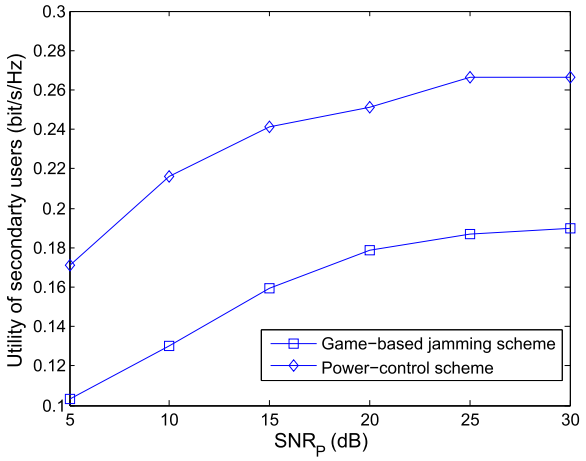

FIGURE 8. Secondary users' utility vs. primary user's SNR.

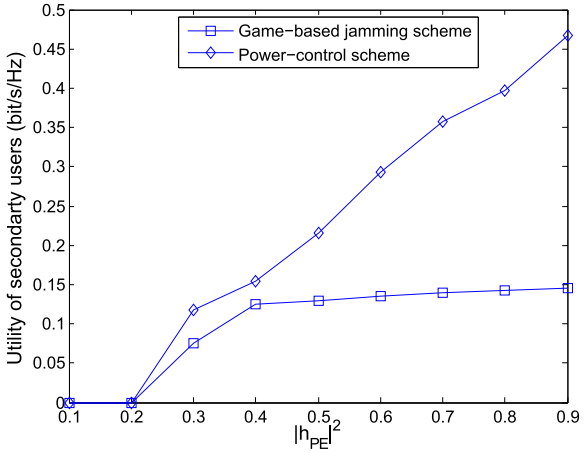

FIGURE 9. Utility of secondary users vs. $|h_{PE}|^2$.

result, more jamming power will be invested in the cooperation, which in turn favors secondary users themselves. Hence, utility of secondary users increases as user P's SNR increases. Because multiple simultaneous jamming transmissions and negligible interference is assumed in Power-control scheme [23], its performance is better than our proposed scheme in terms of secondary users' utility.

Fig. 9 shows secondary users' utility with different $|h_{PE}|^2$. Without cooperation, the utility is zero when $|h_{PE}|^2$ is less than 0.2. As $|h_{PE}|^2$grows larger, more spectrum opportunities will be allocated to secondary users, therefore, the utility increases with $|h_{PE}|^2$. For the same reason, the performance of our proposed scheme is inferior to that of Power-control scheme in terms of secondary users' utility.

V. CONCLUSION

In this paper, we have proposed a game-based jamming approach for physical layer security in spectrum overlay system. To thoroughly capture the characteristics of primary user's service, continuous-time Markov chain is employed and thus channel state transition is clearly built. The incentive for secondary system's jamming cooperation is tuning primary user's load factor. The AN-based jamming method is applied and information about CSI of eavesdroppers is not necessary. In addition, the probabilistic jamming mechanism is designed, such that more degree of freedom can be granted for the game participators. We have analyzed the detailed Stackelberg equilibrium, which gives the conditions for game cooperation. Simulation results show that the secrecy performance of primary users outperforms the power control scheme in [23] because the interference is removed at the receiver under AN jamming.

It is worth mentioning that in this paper, we have not considered user's fairness in the scheduling. Hence, it is of high interest for us to extend the scope of the paper to more than just two secondary users, and to introduce competitive mechanism regarding fairness and other factors. Therefore, a more complicated Markov chain will be established, which remains as the interesting issue for our future research work.

APPENDIX
PROOF OF LEMMA 2

We derive the second derivative of $f(x, z)$ with respect to z as follows:

$$\frac{\partial^2 f}{\partial^2 z} = -\frac{1}{\ln 2(1+x)} \cdot \frac{(b-a)(2+az+bz+a^2b^2z)}{(1+az)^2(1+bz)^2}. \quad (23)$$

Obviously, the above value is negative and $f(x, z)$ is convex in terms of z.

Next, we analyze the monotonicity $f(x, z)$ of in terms of z via solving the first derivative of $f(x, z)$:

$$\frac{\partial f}{\partial z} = \frac{zu^{'}(z) + u(z) - R_2}{1+x} = \frac{h(z)}{1+x}. \quad (24)$$

By substituting $u^{'}(z)$ and $u(z)$ into Eq. 23, we get:

$$h(z) = m - R_2 - \log_2 \frac{1+bz}{1+az} - \frac{z}{\ln 2} \frac{b-a}{(1+az)(1+bz)}. \quad (25)$$

We define $g(z) = \log_2 \frac{1+bz}{1+az} + \frac{z}{\ln 2} \frac{b-a}{(1+az)(1+bz)}$, $h(z)$ can be simplified as:

$$h(z) = m - R_2 - g(z). \quad (26)$$

The first derivative of $g(z)$ can be obtained as:

$$g'(z) = \frac{b-a}{\ln 2} \cdot \frac{2+(a+b)z}{(1+az)^2(1+bz)^2}. \quad (27)$$

$$\because 0 < z \leq \frac{1}{LQ}$$

$$\therefore 2+(a+b)z \in [2, \frac{2G}{Q} + \frac{N}{Q}] \quad if\ a+b \geq 0$$

$$2+(a+b)z \in [\frac{2G}{Q} + \frac{N}{Q}, 2] \quad if\ a+b < 0$$

$$\therefore 2+(a+b)z > 0$$

$$\therefore g'(z) > 0$$

Therefore, $g(z)$ is monotone increasing, and reaches the peak when

$$z = \frac{1}{LQ} = \frac{\gamma}{2c \ln 2}. \quad (28)$$

Because $h(z) = m - R_2 - g(z)$, it's monotone decreasing.

$$h(\frac{1}{LQ}) = -\frac{z}{\ln 2}\frac{b-a}{(1+az)(1+bz)}\Big|_{z=\frac{1}{LQ}} < 0. \quad (29)$$

$$h(0) = m - R_2 > 0. \quad (30)$$

Combining Eq. 24, Eq. 29 and Eq. 30, we can conclude that $f(x, z)$ is increasing and then monotone decreasing in terms of z $z \in [0, \frac{1}{LQ}]$. Therefore, $f(x, z)$ has unique maximum value in terms of z. ■

REFERENCES

[1] J. Mitola, "Cognitive radio: An integrated agent architecture for software defined radio," Ph.D. dissertation, KTH Royal Inst. Technol., Stockholm, Sweden, 2000.

[2] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Comput. Netw.*, vol. 50, pp. 2127–2159, Sep. 2006.

[3] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[4] V. Le, Z. Feng, D. Bourse, and P. Zhang, "A cell based dynamic spectrum management scheme with interference mitigation for cognitive networks," *Wireless Pers. Commun.*, vol. 49, no. 2, pp. 275–293, Apr. 2009.

[5] Y. Yao, Z. Feng, W. Li, and Y. Qian, "Dynamic spectrum access with QoS guarantee for wireless networks: A Markov approach," in *Proc. IEEE Globecom*, Dec. 2010, pp. 1–5.

[6] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE Signal Process. Mag.*, vol. 24, no. 3, pp. 79–89, May 2007.

[7] Y. Xing, C. Mathur, M. Haleem, R. Chandramouli, and K. Subbalakshmi, "Dynamic spectrum access with QoS and interference temperature constraints," *IEEE Trans. Mobile Comput.*, vol. 6, no. 4, pp. 423–433, Apr. 2007.

[8] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Commun. Surv. Tuts.*, vol. 17, no. 2, pp. 1023–1043, 2nd Quart., 2015.

[9] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Netw.*, vol. 27, no. 3, pp. 28–33, May/Jun. 2013.

[10] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[11] J. Ouyang, W.-P. Zhu, D. Massicotte, and M. Lin, "Energy efficient optimization for physical layer security in cognitive relay networks," in *Proc. IEE ICC*, May 2016, pp. 1–6.

[12] L. Sibomana, H. Tran, and H.-J. Zepernick, "On physical layer security for cognitive radio networks with primary user interference," in *Proc. IEEE Milcom*, Oct. 2015, pp. 281–286.

[13] J. Zhang, G. Pan, and H.-M. Wang, "On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system," *IEEE Access*, vol. 4, pp. 3887–3893, Jul. 2016.

[14] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103–5113, Dec. 2013.

[15] Y. Zou, "Physical-layer security for spectrum sharing systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1319–1329, Feb. 2017.

[16] C. Chen, M. Song, C. Xin, and J. Backens, "A game-theoretical antijamming scheme for cognitive radio networks," *IEEE Netw.*, vol. 27, no. 3, pp. 22–27, May/Jun. 2013.

[17] B. Wang, Y. Wu, K. J. R. Liu, and T. C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 877–889, Apr. 2011.

[18] 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.

[19] Y. Tan, S. Sengupta, and K. P. Subbalakshmi, "Analysis of coordinated denial-of-service attacks in IEEE 802.22 networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 890–902, Apr. 2011.

[20] A. Houjeij, W. Saad, and T. Bascar, "A game-theoretic view on the physical layer security of cognitive radio networks," in *Proc. IEEE ICC*, Jun. 2013, pp. 2095–2099.

[21] Y. Wu and K. J. R. Liu, "An information secrecy game in cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 831–842, Sep. 2011.

[22] R. Zhang, X. Cheng, and L. Yang, "Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks," *IEEE Trans. Wireless Commun*, vol. 15, no. 8, pp. 5651–5663, Aug. 2016.

[23] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134–145, Jan. 2013.

[24] A. Al-Talabani, Y. Deng, A. Nallanathan, and H. X. Nguyen, "Enhancing secrecy rate in cognitive radio networks via multilevel Stackelberg game," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1112–1115, Jun. 2016.

[25] Y. Xing, R. Chanddramouli, S. Mangold, and S. S. N, "Dynamic spectrum access in open spectrum wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 3, pp. 626–636, Mar. 2006.

[26] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[27] R. L. Burden, *Numercial Analysis*. Mount Pearl, NL, Canada: Cole Int., 2006.

YANJUN YAO was born in Hefei, China, in 1986. He received the bachelor's and master's degrees in electrical engineering from the Beijing University of Posts and Telecommunications, in 2008 and 2011 respectively. He was with the research institute, as a satellite communication system designer. He is currently pursuing the Ph.D. degree with the Key Laboratory of Wireless-Optimal Communications, University of Science and Technology of China. His research interests include wireless channel security, cognitive radio networks, and satellite communication networks.

WUYANG ZHOU received the B.S. and M.S. degrees from Xidian University, Xi'an, China, in 1993 and 1996, respectively, and the Ph.D. degree from the University of Science and Technology of China, Hefei, China, in 2000. He is currently a Professor with the Department of Electronic Engineering and Information Science, University of Science and Technology of China. His research interests include cooperative communication, radio resource management, and wireless networking.

BAOHUA KOU received the B.S. degree from Xi'an Jiaotong University and the Ph.D. degree from the National University of Defence Technology, Changsha, China, in 2007. He is currently a Senior Engineer with the Beijing Space Information Relay and Transmission Technology Center. His research interests include space tracking, satellite communication, and mobile communication.

YAQI WANG received the B.S. degree from Northwestern Polytechnical University, Xi'an, China, in 2013, and the M.S. degree from the Equipment Academy of China, Beijing, China, in 2015. He is currently an Engineer with the Beijing Space Information Relay and Transmission Technology Center. His research interests include satellite communication and system engineering.