Multiple-Phase Energy Detection and Effective Capacity Based Resource Allocation Against Primary User Emulation Attacks in Cognitive Radio Networks

Zongyi Liu[1,3,4], Guomei Zhang[1,2*], Wei Meng[2] , Xiaohui Ma[1,4], Guobing Li[2]
[1] State Key Laboratory of Geo-information Engineering
Xi'an, Shaanxi 710054, China
[e-mail: 8150837@qq.com]
[2] School of Information and Communications Engineering, Xi'an Jiaotong University
Xi'an, Shaanxi 710049, China
[e-mail: zhanggm@mail.xjtu.edu.cn, mengwei0607@stu.xjtu.edu.cn, gbli@mail.xjtu.edu.cn]
[3] School of Information and Electronics, Beijing Institute of Technology
Beijing 100081, China
[4] Xi'an Research Institute of Surveying and Mapping
Xi'an, Shaanxi 710054, China
[e-mail: shellmei.zhang@stu.xjtu.edu.cn]
*Corresponding author: Guomei Zhang

Received July 26, 2018; revised July 13, 2019; accepted October 30, 2019; published March 31, 2020

Abstract

Cognitive radio (CR) is regarded as an effective approach to avoid the inefficient use of spectrum. However, CRNs have more special security problems compared with the traditional wireless communication systems due to its open and dynamic characteristics. Primary user emulation attack (PUEA) is a common method which can hinder secondary users (SUs) from accessing the spectrum by transmitting signals who has the similar characteristics of the primary users' (PUs) signals, and then the SUs' quality of service (QoS) cannot be guaranteed. To handle this issue, we first design a multiple-phase energy detection scheme based on the cooperation of multiple SUs to detect the PUEA more precisely. Second, a joint SUs scheduling and power allocation scheme is proposed to maximize the weighted effective capacity of multiple SUs with a constraint of the average interference to the PU. The simulation results show that the proposed method can effectively improve the effective capacity of the secondary users compared with the traditional overlay scheme which cannot be aware of the existence of PUEA. Also the good delay QoS guarantee for the secondary users is provided.

Keywords: Cognitive radio, Primary user emulation attack, Energy detection, Effective capacity, Power allocation

This research was supported by the National key Research Program of China under Grant No.2016YFB0501900, the State Key Laboratory of Geo-information Engineering of China under Grant No.SKLGIE2018-Z-2-1, the Natural Science Foundation of China (NSFC) under Grant No. 61401350 and the China Scholarship Council (No. 201706285013).

1. Introduction

With the rapid development of wireless communication technology, mobile devices and services become more diverse and the bandwidth demand for wireless networks increases dramatically. The traditional spectrum allocation policy assigns spectrum to the specific authorized users fixedly. The spectrum efficiency of such a static allocation is very low [1]. The survey data of Federal Communication Commission (FCC) show that many authorized bands are underutilized [2]. Cognitive radio is considered to be an efficient solution to overcome the problem of spectrum inefficiency and scarcity by the dynamic and flexible spectrum access. Actually, CR technology has been deemed as a promising approach to address the challenges and requirements on massive capacity of the fifth generation (5G) mobile networks [3], [4]. Spectrum sharing by dynamic spectrum access is the core idea of CR. In order to meet the much higher spectrum requirements of 5G, full spectrum sharing throughout all kinds of spectrum resources is expected, such as low and high frequency bands, licensed and unlicensed frequency bands, and continuous and discontinuous frequency bands [4]. Spectrum sensing and spectrum allocation are two key steps of spectrum sharing in cognitive radio networks (CRNs). The main purpose of spectrum sensing is to find the white spaces so that SUs can obtain more opportunities to access the authorized spectrum without causing harmful interference to PUs. Spectrum allocation aims to achieve the efficient utilization of licensed spectrum to guarantee the QoS requirements for SUs by distributing the spectrum white spaces to SUs optimally.

However, the openness of the wireless communication system makes the CRNs face more specific security issues. PUEA is a common problem. According to the attacking purpose, PUEA could be classified into two categories: a selfish SU and a malicious PUE attacker. A selfish SU would emulate the PU's signal to access a primary channel as the PU does not use it, or broadcast fake information on the available channel in order to empty or pre-occupy a channel for its own transmission. A malicious PUE attacker would induce the denial of service (DoS) to the CRNs by sending the faked PU signal and then decrease the spectrum access opportunity of SUs. The existence of attack signal makes SUs unable to determine whether PUs or MUs occupy channel when channel is busy based on the traditional spectrum sensing methods. Meanwhile, the existing resource allocation schemes will not be suitable for such PUEA scenario either. The power allocation for SUs is also difficult to implement.

The correct detection of PUEA is of great significance for causing the low interference to PUs and maximizing the utilization of spectrum resource. Some works have studied the detection of PUEA. They can be generally divided into two categories namely location-aware methods [5],[6] and location-unaware methods [7]-[12]. Location-aware methods first locate the signal transmitter based on the measurements of received signal strength (RSS)[5] or time difference of arrival (TDOA)[6]. Then, the estimated location of the signal source is compared with the known position of the PU transmitter to determine whether the signal source is a PU or PUEA. However, location based detection schemes need a prior knowledge of the PUs' locations. The location-unaware methods try to identify a PU and a PUEA mainly by using the signals' some characteristics, such as the energy and the cyclic stationarity of signals. Moreover, cooperative spectrum sensing (CSS) technology based on the decisions or measured data fusion of multiple-SUs has been widely used in CRNs to obtain a high detection accuracy in deep fading environment. CSS could be also introduced to improve the PUEA detection performance. In [7], a two-phase PUEA detection algorithm based on multiple SUs

cooperation was proposed toward a CRN with PUs communicating with OFDM signal. In the first phase, the cyclic stationary feature of non-zero autocorrelation property of OFDM signals is utilized to distinguish PUs from PUEAs which do not use OFDM signals. Then the energy based detection is executed in the second phase to further distinguish PUE attacks from the noise, if the first-phase detection reveals that the primary user is absent. However, this method would become invalid when the PUEA can emulate PUs to transmit OFDM signals. In fact, such a scenario would appear very likely for a selfish SU attack or a smart PUE attack. Moreover, hard decision fusion (HDF) detection schemes combining the binary decision of each SU with K-out-N rule at fusion center (FC) were studied to collaboratively detect PU and PUEA in [8],[9]. Concretely, the main parameters involved in cooperative spectrum sensing, such as the number of samples, the detection thresholds for the SU's local decision and the parameter K in voting rule, were optimized to minimize the sensing error probability in the works of [8] and [9]. To retain more information of the local observations at each SU, soft decision fusion (SDF) schemes were studied also to realize the accurate PU detection in the presence of PUEA in [10], [11]. The local measured statistic of each SU rather than the binary decision result is sent to FC and a global decision is made by FU based on the original measurements of multiple SUs. The authors of [10] adopted a weighted combination of energy statistics from SUs at FC to make the global decision. Further, the weights were optimized to maximize the SU's throughput. While, the work in [11] applied minimum Bayes cost criteria to determine the channel status in four cases. In addition, a selfish SU attack was discussed in [12]. In order to find the selfish SU who broadcasts faked available channel lists to its neighboring SUs for pre-occupying the channel, an attack detection method based on information exchanging and comparing among neighboring CR nodes was presented. However, the attack type in [12] is different from our work in this paper. We focus on the malicious PUE attack, where an attacker sends the faked PU signal rather than the false vacant channel lists to prevent legitimate SUs from accessing the available channel.

The purpose of accurate detection is to improve QoS of SUs as well as avoid any deleterious interference to the PU. Specifically, the real-time performance is one of important evaluation indexes of communication quality. Compared with conventional wireless networks, delay QoS guarantee is a more challenging issue for CRNs. Effective capacity [13] has been introduced as a powerful tool to describe the ability that a system provides real-time services. Thus, enhancing the effective capacity is a feasible way to ensure the delay QoS of SUs. Furthermore, different users may have different delay requirements. For example, the voice traffic may have stricter delay QoS constraint than the data traffic. Hence, it is meaningful to study on the discrepant delay QoS provision for different SUs. There exist some works considering the resource allocation for the PUEA scenarios. The authors of [14] proposed a power allocation to maximize the transmission rate of SUs for an OFDM CRNs with PUEA. Here, the secondary users only transmit signals when the primary channel is sensed to be idle. In order to improve the spectrum utilization, the scheme in [15] allowed the SUs to access the spectrum when it is idle or occupied by MUs. It also took the maximization of the SU's rate as the design object. Furthermore, the works in [16], [17] investigated the energy efficiency (EE) maximization problem by SU selection, power allocation and sensing time assignment in the presence of PUEA. However, the above works did not consider the delay QoS requirement of the SU's practical traffic. While, such a requirement is more difficult to be satisfied when the malicious attacker exists.

In order to provide better delay QoS for different secondary users, we first propose a multiple-phase energy detection scheme to detect the PUEA more accurately through fusing the energy statistics of multiple secondary users. Further, the weights in the fused statistic are

determined and the decision thresholds are obtained based on the analyzed detection probabilities for three decision cases. Second, a joint SUs scheduling and power allocation scheme is proposed to maximize the weighted effective capacity of the SUs. Here, the secondary users will access the spectrum when it is sensed to be idle or occupied by the malicious users. Further, an iterative process, which includes an exhaustive search based user scheduling and a CVX based power allocation, is adopted to solve the joint optimization problem. The simulation results demonstrate that the proposed PUEA detector can recognize the primary users and malicious users efficiently. The delay QoS guarantee for SUs can be realized better by the proposed joint user scheduling and power allocation scheme.

The rest of the paper is organized as follows: In section 2, a system model with multiple SUs and several MUs is described and the transmission model is given. The multiple-phases energy detection scheme based on the cooperation of multiple SUs is presented in section 3. Section 4 introduces the joint user scheduling and power allocation method based on effective capacity in detail. Section 5 presents and analyzes the simulation results. Section 6 concludes the paper.

2. System Model

Consider a cognitive radio network shown in **Fig. 1**, which includes one primary channel, M secondary users and several malicious users. Assume the MUs occupy the primary channel with a certain probability when the PU is inactive. Multiple SUs can cooperatively sense the occupancy state of the primary channel and then access the channel legitimately based on the sensing result. The overlay mode is adopted. SUs will not access the channel when it is sensed to be occupied by PU in order to reduce interference to the PU as much as possible.

Assume the licensed spectrum bandwidth is B and the small-scale fading of wireless channel follows the independent and identically distributed (i.i.d.) Rayleigh block fading. The length of a frame is T seconds. The SUs perform spectrum sensing to detect the status of channel during the preceding T_0 seconds of a frame. Then, one SU is scheduled to transmit signal in the remaining $T-T_0$ seconds if the decision result is the PU being absent. The other main assumptions similar as the ones given in [18] are listed as followings:

1) The primary transmitter (PT) sends the signal with constant power and the SUs' positions remain unchanged. While, MUs' power and positions would change randomly.

2) The received signals from PT and MUs are both assumed to be independent and identically distributed (i.i.d.) random variables following cyclo-stationary complex Gaussian distribution with zero mean. The variances are σ_{Ps}^2 and σ_{Ms}^2, respectively, where $s=1,2,...,M$ is the index of SU.

3) The noise is the i.i.d. cyclo-stationary complex Gaussian distributed random variables with mean zero and the variance σ_{Ns}^2.

There are three actual states for the primary channel. H_0 indicates idleness. H_1 and H_2 indicate that the channel is occupied by PU and MUs, respectively. Assume that MUs can sense the status of the primary channel correctly. MUs will not attack when the channel is used by the PU in order to prevent being detected by the conservation strategies of the PU. Moreover, MUs cannot occupy the idle channel continuously due to the power restriction. Then, the Priori probability of each status $P(H_i)$ would be larger than 0.

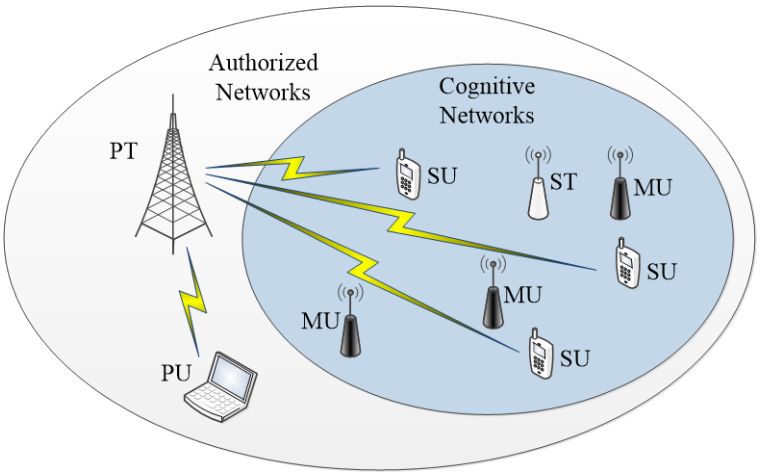

Fig. 1. System model of a CRN with PUEA

3. Multiple-Phase Energy Detection for PUEA

In the system given above, the spectrum sensing problem could be modeled as a hypothesis testing problem with three actual states. Further, D_0, D_1 and D_2 are used to represent the three channel states sensed, namely being idle, being used by PU and being attacked by MUs. Then, the detection results have nine possible cases and the corresponding probabilities are denoted by $\{P_{ij} = P(H_i) \cdot P(D_j / H_i), i, j \in \{0,1,2\}\}$.

3.1 Multiple Detection Statistics

Energy detection is a simple method for spectrum sensing in the traditional CRNs with two actual states, whose hypothesis testing problem for the *s*-th SU could be expressed as

$$Y_s = \frac{1}{N}\sum_{i=1}^{N}\left|y_s(i)\right|^2 \underset{H_0}{\overset{H_1}{\gtrless}} \lambda \tag{1}$$

where we have

$$y_s(i) = \begin{cases} n_s(i), & H_0 \\ h_s(i)x_{\mathrm{P}}(i) + n_s(i), & H_1 \end{cases} \tag{2}$$

Here, h_s is the primary channel coefficient and n_s is an additive noise. x_{P} is the signal sent by the PU's transmitter. N is the number of samples for sensing. λ is the decision threshold to detect the presence of the signal x_{P}.The energy statistic Y_s in Eq. (1) follows the Chi-square distribution with a degree of freedom of N. However, according to the Central Limit Theorem (CLT), Y_s can be approximated by a Gaussian distribution with a long enough *N*. Actually, CLT has been usually applied to simplify the analysis and design in the spectrum sensing, such as in [9], [11] and [19]. Further, the authors of [9] and [11] considered that CLT could be used when N >10. This condition is commonly satisfied in a practical system.

However, the traditional binary hypothesis testing is unsuitable for the scenario with PUEA. As the primary channel is occupied by a MU, the received signal of the *s*-th SU is $y_s(i) = g_s(i)x_{\mathrm{M}}(i) + n_s(i)$, where g_s is the channel coefficient from the MU to the *s*-th SU

and x_{M} is the signal sent by the MU. Then, Y_s may still be larger than the threshold λ and the SU cannot distinguish whether the channel is occupied by PU or MUs. Therefore, combing the idea of multiple thresholds based scheme in [20] with the CSS methods in [10] and [11], we present a modified energy based PUEA detection method, called multiple-phase energy detection based on multiple users' cooperation. Its main idea is to extract multiple detection statistics based on the energy statistics from *M* SUs to detect the presence of PU and MUs more accurately.

In this scheme, the key parameters of σ_{Ps}^2 and σ_{Ns}^2 for each SU are assumed to be known by fusion center, but there is no information about σ_{Ms}^2. The detection statistic used in the *i*-th phase is $V_i = \mathbf{W}_i^T \mathbf{Y} = \sum_{s=1}^{M} w_{i\_s} Y_s$, where $\mathbf{W}_i = [w_{i\_1}, w_{i\_2}, ..., w_{i\_M}]^T$ and $\mathbf{Y} = [Y_1, Y_2, ..., Y_M]^T$. Furthermore, $i \in \{1, 2, ..., L\}$ and we take $L = M$ in order to make full use of the energy statistics provided by all SUs. From observation, we can find that it is more difficult for MUs to emulate PU's signals to make all of *L* detection statistics built by *M* SU's measurements similar to the case of PU exiting, except that the location of MU is same as PU. For example, consider a simple case of two SUs, which corresponds to a two-phase energy detection. The two detection statistics can be simply built as $V_1 = (Y_1 + Y_2)/2$ and $V_1 = (Y_1 - Y_2)/2$, respectively. Under the scenario assumption that PU's signal has constant power and SUs' positions are fixed, V_1 and V_2 would be stable around two certain values, denoted by ε_1 and ε_2, when PU is present. Because the dynamic nature of PUEA's behaviors, Y_1 and Y_2 would change randomly. Then, even though the PUEA could make V_1 near to ε_1, it is still difficult to keep V_2 close to ε_2 simultaneously. From this point of view, we can think that the given multi-phase scheme has stronger robustness to PUEA.

3.2 Decision Procedure

The decision procedure of the proposed multiple phase energy detection for PUEA is presented in **Fig. 2**. There are $2L+1$ thresholds for L detection statistics. The first detection statistic V_1 is mainly used to distinguish whether the primary channel is idle or busy. All the other V_i are used to distinguish whether the channel is used by PU or by MUs. When V_1 is less than the threshold of λ_0, the channel is deemed to be idle. Because the transmitting power of PU is constant, all of the detection statistics should keep stable under H_1 state. Therefore, only when all the V_i locate during the corresponding range of (λ_{i1}, λ_{i2}), the detection result is D_1. In other situations, the channel would be deemed to be occupied by MUs based on the instability assumption of the MUs' power and locations.

3.3 Determination of the Weights and Detection Thresholds

A. Determination of the weight vector $\mathbf{W}_i$

Since V_1 is mainly used to decide whether the channel is occupied, the average received energy of all the SUs are taken as V_1 simply and then we have $w_{1\_s} = 1/M, \forall s \in \{1, ..., M\}$.

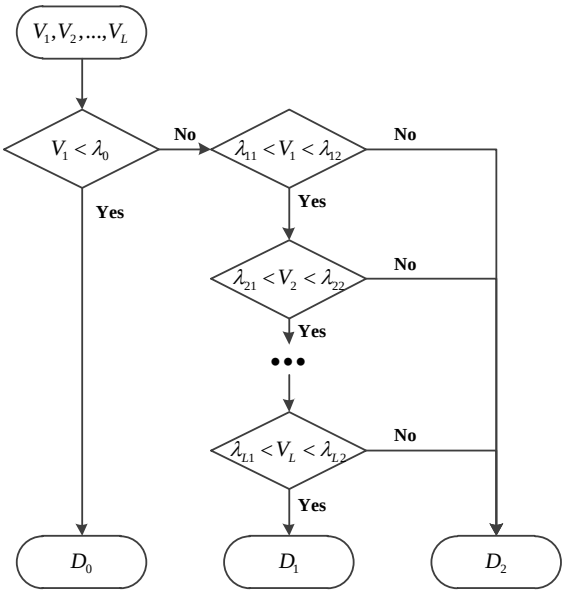

Fig. 2. Decision Procedure of Multiple-Phase Energy Detection

In order to obtain the other weight vectors $\mathbf{W}_i$, $i = 2,..,L$, an intuitive and heuristic method is given. We set $|w_{i\_1}|(\sigma_{\mathrm{N1}}^2 + \sigma_{\mathrm{P2}}^2) = |w_{i\_2}|(\sigma_{\mathrm{N2}}^2 + \sigma_{\mathrm{P2}}^2) = ... = |w_{i\_M}|(\sigma_{\mathrm{N}M}^2 + \sigma_{\mathrm{P}M}^2)$ and then combine it with the constraints of $0 < |w_{i\_s}| < 1$ and $\sum_{s=1}^{M} |w_{i\_s}| = 1$ to obtain

$$|w_{i\_s}| = \frac{\prod_{k=1,k\neq s}^{M} (\sigma_{\mathrm{N}k}^2 + \sigma_{\mathrm{P}k}^2)}{\sum_{l=1}^{M} \prod_{k=1,k\neq l}^{M} (\sigma_{\mathrm{N}k}^2 + \sigma_{\mathrm{P}k}^2)} \tag{3}$$

Because it is reasonable to deem that the SU with higher received power from the PU transmitter may not contribute more for detecting the MU, we set a smaller $|w_{i\_s}|$ for a SU with a larger $(\sigma_{\mathrm{Ns}}^2 + \sigma_{\mathrm{Ps}}^2)$.

As for the sign of w_{i-s}, some optimization criterion could be used. For example, $D_w = \sum_{i=2}^{M} \sum_{j=i+1}^{M} \left\| \mathbf{W}_i - \mathbf{W}_j \right\|^2$ maximization which is adopted in this paper. In the simulation, a greedy search is used to find the signs of w_{i_s}.

B. Calculating Probability Density Function (PDF) of V_i

The probability density function of the detection statistics V_i under three Prior states could be easily obtained as

$$\begin{cases} H_0 : V_i \sim \mathrm{N}(\sum_{s=1}^{M} w_{i\_s} \sigma_{\mathrm{Ns}}^2, 1/N \sum_{s=1}^{M} w_{i\_s}^2 \sigma_{\mathrm{Ns}}^4) = \mathrm{N}(\beta_{i0}, \delta_{i0}^2) \\ H_1 : V_i \sim \mathrm{N}(\sum_{s=1}^{M} w_{i\_s} (\sigma_{\mathrm{Ns}}^2 + \sigma_{\mathrm{Ps}}^2), 1/N \sum_{s=1}^{M} w_{i\_s}^2 (\sigma_{\mathrm{Ns}}^2 + \sigma_{\mathrm{Ps}}^2)^2) = \mathrm{N}(\beta_{i\mathrm{P}}, \delta_{i\mathrm{P}}^2) \\ H_2 : V_i \sim \mathrm{N}(\sum_{s=1}^{M} w_{i\_s} (\sigma_{\mathrm{Ns}}^2 + \sigma_{\mathrm{Ms}}^2), 1/N \sum_{s=1}^{M} w_{i\_s}^2 (\sigma_{\mathrm{Ns}}^2 + \sigma_{\mathrm{Ms}}^2)^2) = \mathrm{N}(\beta_{i\mathrm{M}}, \delta_{i\mathrm{M}}^2) \end{cases} \tag{4}$$

C. Setting the constraints for the probabilities of correction detection

Two constraints for the probabilities of correct detection under the cases of H_0 and H_1 are preset as $P(D_0 / H_0) \geq a$ and $P(D_1 / H_1) \geq b$.

D. Calculating the threshold λ_0 for V_1

One threshold λ_0 is used to distinguish H_0 from the other two states and it can be derived by selecting the equality sign in $P(D_0 / H_0) \geq a$. The detail is given by

$$\begin{aligned} P(D_0 / H_0) &= P(V_1|_{H_0} \leq \lambda_0) = 1 - Q\left((\lambda_0 - \beta_{10}) \Big/ \sqrt{\delta_{10}^2}\right) = a \\ \Rightarrow \lambda_0 &= Q^{-1}(1-a)\delta_{10} + \beta_{10} \end{aligned} \tag{5}$$

E. Calculating the rest thresholds λ_{i1} and λ_{i2}

The rest thresholds λ_{i1} and λ_{i2}, $\forall i \in \{1,...,L\}$, are obtained by using the constraint $P(D_1 / H_1) = b$. In order to derive $2L$ thresholds from only one equalization determinately, we deem that V_i is independent with each other approximately, then it can be achieved that

$$P(D_1 | H_1) = \prod_{i=1}^{L} P(D_1 | H_1, V_i) = b, \ i = 1,...,L \tag{6}$$

Furthermore, we simply set

$$P(D_1 | H_1, V_i) = P(D_1 | H_1, V_j) \quad \forall i, j \in \{1,...,L\} \tag{7}$$

Thus, we have

$$P(\lambda_{i1} \leq V_i|_{H_1} \leq \lambda_{i2}) = Q\left((\lambda_{i1} - \beta_{iP}) \Big/ \sqrt{\delta_{iP}^2}\right) - Q\left((\lambda_{i2} - \beta_{iP}) \Big/ \sqrt{\delta_{iP}^2}\right) = \sqrt[L]{b} \tag{8}$$

Further, let λ_{i1} and λ_{i2} be symmetrical about β_{iP} and it can be easily obtained

$$\begin{cases} \lambda_{i1} = \beta_{iP} - Q^{-1}\left((1 - \sqrt[L]{b})/2\right)\delta_{iP} \\ \lambda_{i2} = \beta_{iP} + Q^{-1}\left((1 - \sqrt[L]{b})/2\right)\delta_{iP} \end{cases}, \quad i = 1,2,...,L \tag{9}$$

It is worth noting that there is a special case for setting λ_0 and λ_{11}. From Eq.(5) and Eq.(9), we can see that λ_{11} may be smaller than λ_0 when σ_{Pk}^2 is small. For such a case, we will set them identical with the average value of them.

4. Effective Capacity Based Joint SUs Scheduling and Power Allocation under PUEA Scenario

Consider the case that multiple secondary users will share the primary channel after coordinate spectrum sensing. Furthermore, suppose that different SUs have different delay QoS requirements because different traffics usually have different delay constraints in practical communications. In order to address the resource allocation issue in the above scenario, an effective capacity based joint SUs scheduling and power allocation is proposed to guarantee the differential delay QoS requirements of multiple SUs who share one idle primary channel.

4.1 Effective Capacity of Secondary Users

Effective capacity can be used to describe the ability to provide real-time services. It is defined as the maximum constant arrival rate that a given service process can support under an appointed statistical QoS constraint [21],[22]. Effective capacity can be expressed as

$$E_C(\theta) = -[1/\theta(T-T_0)]\log \mathrm{E}\left[e^{-\theta S(T-T_0)}\right] \tag{10}$$

where θ is QoS parameter and defined as the exponential decay rate of the buffer overflow probability when the buffer threshold increases to infinity[21]. Here, θ can be considered as the delay QoS constraint and a higher θ means a more strict delay QoS requirement. $\mathrm{E}\{\bullet\}$ indicates calculating the mean value over $S(T-T_0)$ in the time period $[T_0, T]$. $S(T-T_0)$ is the cumulative service process, namely the number of bits sent to the users from the buffer during the time period$[T_0, T]$.

As for the transmission of the secondary user in the considered scenario, the secondary transmitter (ST) will send signals to the scheduled SU over the primary channel when it is sensed to be idle or occupied by MUs. While the primary channel is sensed to be used by PU, ST will keep silent to avoid interfering the PU's communication. Moreover, the transmission power of ST will depend on both the sensing result of the primary channel and the channel state information from ST to the scheduled SU. Then, a transmission power factor $\eta\left(z, D_i\right)$ is introduced in, which satisfies the constraint of $\mathrm{E}_{z,\mathrm{D}_i}\left[\eta\left(z,\mathrm{D}_i\right)\right] \le 1$. Here, $i \in \{0,1,2\}$ and z is the power gain of the scheduled secondary user's channel. Especially, we have $\eta\left(z, D_1\right) = 0$ no matter what the secondary user's channel is. Thus, the instantaneous transmission rate of the scheduled SU can be written as

$$R\left(\eta\left(z, D_i\right)\right) = B\log_2\left(1+\eta\left(z, D_i\right) z\bar{P}/\left(\sigma_{\mathrm{N}}^2+\sigma_{\mathrm{M}}^2 \cdot i/2\right)\right) \tag{11}$$

where B is the frequency bandwidth of the primary channel and $\bar{P}$ is the average transmission power of ST. σ_{N}^2 is the variance of the white noise at the scheduled SU and and σ_{M}^2 is the power of the interference from MUs to the scheduled SU. After spectrum sensing, the fusion center can obtain a rough estimation of σ_{M}^2 based on the received detection statistic from each SU with PUEA detection result being D_2. Moreover, the spectrum sensing is assumed completely correct in calculating the instantaneous rate shown in Eq. (11). Such an assumption is acceptable when Eq. (11) is only applied to optimize the scheduling and power allocation strategies.

Substituting Eq. (11) into Eq. (10), we can obtain the effective capacity of the scheduled SU given by

$$E_C(\theta) = -(1/\theta T^{'})\log \mathrm{E}_{z,D_i}\left\{e^{-\theta T^{'} R(\eta(z,D_i))}\right\} \tag{12}$$

where $T^{'} = T - T_0$. Let's consider the expectation in Eq.(12) over D_i firstly. From Section 3, we can see that the sensed state of the primary channel has nine possibilities. Moreover, for the case of M=2, the corresponding probabilities for nine cases are listed in Appendix. Then, it can be easily achieved that Eq.(12) could be rewritten as

$$E_C(\theta) = -\frac{1}{\theta T'} \log \mathrm{E}_z \left[\sum_{j=0}^{2} P(H_j) \sum_{i=0}^{2} P(D_i | H_j) e^{-\theta T' R(\eta(z, D_i))} \right] \tag{13}$$

As for the expectation over the channel gain in Eq. (13), the useful finite state channel model [23], [24] is adopted to enhance the algorithm's operability. Assume the channel from ST to SU over the licensed frequency band follows Rayleigh block fading. Further, it is assumed to be i.i.d from frame to frame and among different SUs. Here, the secondary user's channel is discretized to a *K*-state model $M_{\mathrm{CH}} = \{m_1, m_1, ..., m_K\}$ based on the received instantaneous signal to interference plus noise ratio (SINR) γ. Specifically, the entire SINR region is divided into *K* non-overlapping intervals according to the boundary points of $\{\alpha_0, \alpha_1, ..., \alpha_K\}$. When γ locates in the range $[\alpha_{k-1}, \alpha_k)$, $k = 1, 2, ..., K$, the channel is considered to be the state m_k. Furthermore, the probabilities of the secondary channel lying in all the states are denoted as $\boldsymbol{\pi}^{s,j} = \{\pi_1^{s,j}, \pi_2^{s,j}, ..., \pi_K^{s,j}\}$, $j \in \{0, 1, 2\}$ and $s \in \{1, 2, ..., M\}$. $\boldsymbol{\pi}^{s,0}$, $\boldsymbol{\pi}^{s,1}$ and $\boldsymbol{\pi}^{s,2}$ correspond to the cases under three occupancy states of the licensed channel H_0, H_1 and H_2 for *s*-th SU, respectively. For the Rayleigh fading channel, we have $\pi_k^{s,j} = \int_{\alpha_k}^{\alpha_{k+1}} f_{H_j}^s(\gamma) d\gamma$, where $f_{H_j}^s(\gamma) = \left(1/\overline{\gamma}_{H_j}^s\right) e^{-\left(\gamma/\overline{\gamma}_{H_j}^s\right)}$. Moreover, $\overline{\gamma}_{H_0}^s = z_s \overline{P} / \sigma_{\mathrm{Ns}}^2$, $\overline{\gamma}_{H_1}^s = z_s \overline{P} / (\sigma_{\mathrm{Ns}}^2 + \sigma_{\mathrm{Ps}}^2)$ and $\overline{\gamma}_{H_2}^s = z_s \overline{P} / (\sigma_{\mathrm{Ns}}^2 + \sigma_{\mathrm{Ms}}^2)$. Here, $z_s = \left| h_{ST\_SU\_s} \right|^2$ is the power gain of the channel between ST and the *s*-th SU.

Based on the finite state channel model, Eq.(13) can be expressed as

$$E_C^s(\theta) = -\frac{1}{\theta_s T'} \log \left[\sum_{j=0}^{2} P(H_j) \sum_{i=0}^{2} P(D_i | H_j) \sum_{k=1}^{K} \pi_k^{s,j} e^{-\theta_s T' R(\eta(m_k, D_i))} \right] \tag{14}$$

where the *s*-th SU is assumed to be scheduled always.

4.2 Joint Optimization for SU Scheduling and Power Allocation

A. Optimization variables

When the primary channel is sensed to be idle or occupied by MUs, the ST will schedule one of the *M* secondary users for communication with an optimized transmission power. Define a scheduling matrix $\mathbf{S}$ with size of $\underbrace{K \times K \times ... \times K}_{M}$ according to the *K*-state channel model of each SU. Here, $\mathbf{S}(k_1, k_2, ..., k_M)$ is the scheduling result for the case that the channel state of the *s*-th SU is m_{k_s} ($\forall s \in \{1, ..., M\}$). $\mathbf{S}(k_1, k_2, ..., k_M) = s$ means that the *s*-th SU is served.

According to the K-state finite channel model, the power allocation strategy could be defined as

$$\boldsymbol{\Gamma} = \begin{bmatrix} \eta(m_1, D_0) & \eta(m_2, D_0) & \cdots & \eta(m_K, D_0) \\ 0 & 0 & \cdots & 0 \\ \eta(m_1, D_2) & \eta(m_2, D_2) & \cdots & \eta(m_K, D_2) \end{bmatrix} \tag{15}$$

where $\eta(m_k, D_i)$ indicates the transmission power factor when the secondary channel condition is the state m_k and the sensing result is D_i. Based on the analysis in Section 4.1, the transmission power factor is set as zero if the detection result is PU occupying the channel, i.e. D_1. Therefore, the elements in the second line of $\mathbf{\Gamma}$ are all set as 0. It should be noted that $\eta(m_k, D_i)$ is independent on which SU is scheduled and it is only related with the scheduled SU's SINR level and the sensing result about the primary channel.

The scheduling matrix $\mathbf{S}$ and the power allocation strategy $\mathbf{\Gamma}$ just are our optimization variables in the following optimization problem.

B. Optimization objective function

Considering that *M* SUs would sharing the vacant primary channel, the weighted summation of *M* SUs' effective capacity is adopted as the optimization objective function. Define $\boldsymbol{\beta} = [\beta_1, \beta_2, ..., \beta_M]$ as the weights vector. Here β_s represents the proportion of the effective capacity of the *s*-th SU in the overall objective function. Thus, the weights have to satisfy the conditions of $0 \le \beta_s \le 1$ and $\sum_{s=1}^{M} \beta_s = 1$. Then, the optimization objective function can be written as

$$F(\mathbf{S}, \mathbf{\Gamma}, \boldsymbol{\beta}) = \sum_{s=1}^{M} \beta_s E_C^s(\theta_s) \tag{16}$$

where the effective capacity of the *s*-th SU could be expressed as

$$E_C^s(\theta) = -\frac{1}{\theta_s T} \log\left[\sum_{j=0}^{2} P(H_j) \sum_{i=0}^{2} P(D_i | H_j) \sum_{k_1=1}^{K} \cdots \sum_{k_M=1}^{K} \pi_{k_1}^{1,j} \cdots \pi_{k_M}^{M,j} e^{-\theta_s [\mathbf{S}(k_1,...,k_M)==s] T R(\eta(m_{k_s}, D_i))} \right] \tag{17}$$

Eq.(17) is obtained by considering the effect of the SU scheduling scheme based on Eq.(14) . Moreover, the use of $\boldsymbol{\beta}$ makes the scheme more flexible when different SUs have different priorities. If necessary, it could be involved as another optimization variable in the joint optimization problem for some scenarios and objectives.

C. Constraint condition

In practice, the sensing result for the licensed channel is possibly false. For instance, the channel is sensed to be idle or occupied by MUs, but actually it is occupied by PU. In this case, the transmission of SU would cause interference to the PU. Therefore, in order to limit the interference to the PU caused by the ST, the following interference power constraint on the SUs is introduced in the joint optimization [18].

$$I = \left(P(D_0, H_1) \cdot \mathrm{E}_z \left\{ \eta(z, D_0) \,|\, H_1 \right\} + P(D_2, H_1) \cdot \mathrm{E}_z \left\{ \eta(z, D_2) \,|\, H_1 \right\} \right) \overline{P} \le P_{up} \tag{18}$$

where P_{up} represents the maximum interference power tolerated by PU. And, we have

$$\mathrm{E}_z \left\{ \eta(z, D_i) \middle| H_1 \right\} = \sum_{k_1=1}^{K} \cdots \sum_{k_M=1}^{K} \sum_{s=1}^{M} \pi_{k_1}^{1,1} \cdots \pi_{k_M}^{M,1} [\mathbf{S}(k_1,...,k_M) == s] \eta(m_{k_s}, D_i), \; i = 0, 2 \tag{19}$$

Except the above interference power constraint of Eq.(18), the power allocation strategy should also satisfy the total power constraint of $\mathrm{E}_{z,\mathrm{D}_i} \left[\eta(z, \mathrm{D}_i) \right] \le 1$ given in Section 4.1.

Further, combing the *K*-state channel model for SUs with detection of the primary channel, we have

$$\mathrm{E}_{z,\mathrm{D}_i}\left[\eta\left(z,\mathrm{D}_i\right)\right]= \sum_{j=0}^{2}P\left(H_j\right)\sum_{i=0}^{2}P\left(D_i\middle|H_j\right)\sum_{k_1=1}^{K}\cdots\sum_{k_M=1}^{K}\sum_{s=1}^{M}\pi_{k_1}^{1,j}\cdots\pi_{k_M}^{M,j}[\mathbf{S}(k_1,...,k_M)==\mathrm{s}]\eta(m_{k_s},D_i) \tag{20}$$

D. Optimization problem

Based on the above description, we can finally establish the following optimization problem:

$$\begin{aligned}\underset{\mathbf{S},\boldsymbol{\Gamma}}{\text{maximize}}\ & F\left(\mathbf{S},\boldsymbol{\Gamma},\boldsymbol{\beta}\right)=\sum_{s=1}^{M}\beta_s E_C^s\left(\theta_s\right)\\ \text{s.t.}\quad & \mathrm{E}_{z,\mathrm{D}_i}\left[\eta\left(\mathrm{z},\mathrm{D}_i\right)\right]\le 1\\ & I\le P_{up}\end{aligned} \tag{21}$$

where the first constraint is the sum power constraint and the second constraint corresponds to the interference constraint to the PU.

4.3. The solution of optimization problem

To solve the problem of Eq. (21), the alternating iterative optimization is used over the scheduling matrix $\mathbf{S}$ and the power allocation strategy $\boldsymbol{\Gamma}$ under a fixed $\boldsymbol{\beta}$, which is shown as follows:

Specify the parameters of $\boldsymbol{\beta}$, $\theta_1,...,\theta_M$ and ε. Initialize $F_{\max}=0$.

Step 1): Select one $\mathbf{S}$ in the set of $[1,...,M]^{K^M}$ randomly.

Step 2): Optimize $\boldsymbol{\Gamma}$ with the CVX toolbox in that $F\left(.\right)$ is a monotonically increasing function with respect to $\boldsymbol{\Gamma}$. Next, calculate F_{op} based on the expression of $F\left(\mathbf{S},\boldsymbol{\Gamma},\boldsymbol{\beta}\right)$.

Step 3): Search an optimized $\mathbf{S}$ in the set of $[1,...,M]^{K^M}$ exhaustively to maximize $F\left(\mathbf{S},\boldsymbol{\Gamma},\boldsymbol{\beta}\right)$ under the case of $\boldsymbol{\Gamma}$ obtained in Step 2). Then, update F_{op}.

Step 4): Comparing F_{op} and $F_{\max}$, if $\left|F_{\max}-F_{op}\right|<\varepsilon$, the iteration is ended. Otherwise, if $\left|F_{\max}-F_{op}\right|>\varepsilon$ and $F_{op}>F_{\max}$, then set $F_{\max}=F_{op}$ and skip to Step 2). If $\left|F_{\max}-F_{op}\right|>\varepsilon$ and $F_{op}<F_{\max}$, then directly skip to Step 2).

From the above iterative optimization process, it can be obtained that the computation complexity of our algorithm is mainly dependent on three factors, namely the number of iteration, the complexity to compute $\boldsymbol{\Gamma}$ by CVX toolbox and the computational cost of exhaustively searching S. These three parameters are denoted by I_{ITE}, C_{CVX} and C_{SE}, respectively. Then, the complexity of our optimization algorithm can be expressed as $I_{\mathrm{ITE}}\cdot(C_{\mathrm{CVX}}+C_{\mathrm{SE}})$ approximately. According to our simulation, the iteration process could reach convergence after about 4 iterations. As to C_{CVX}, it would be decided by the convex optimization algorithms utilized by CVX toolbox and the user usually has no the exact

information about them. Therefore, it is difficult to analyze C_{CVX} quantitatively. Thus, the runtime of CVX toolbox over a specific computer and software can be used to evaluate its running efficiency, just as done in [25]. The concrete runtime under our specific simulation scenario and configuration will be presented in Section 5. Moreover, an exhaustive search is executed in step 3) to find the optimized S in a set with size of M^{K^M}. Hence, C_{SE} is proportional to M^{K^M} and it increases extremely fast with K and M. In fact, for small K and M, the overall complexity is mainly decided by the running cost of CVX toolbox. However, for large K and M, the complexity of exhaustive search is dominant.

Although the alternating iterative optimization is complex and has a high computational overhead, it is only executed offline and independent on the instantaneous channel state information. For the specific M, SINR quantization and channel model, the above iterative optimization is carried out only once to obtain S and $\mathbf{\Gamma}$. In practical operation, how to schedule SU and allocate the transmit power could be easily obtained by looking up S and $\mathbf{\Gamma}$ according to the SUs' quantized SINR.

5. Simulation Results and Discussions

To evaluate the proposed multiple-phase detection scheme in Section 3 and the effective capacity based resource allocation algorithm in Section 4, a simulation system is built by using MATLAB 2018a. The simulation system includes one PU and two SUs. The number of MUs is one or two. For convenience, we put all users into a two-dimensional Cartesian coordinate system. The default unit of power is Watt, and the default unit of distance is Km. The primary simulation parameters are shown in **Table 1**.

Table 1. Primary Simulation Parameters

Parameters	Assumptions
the Priori probabilities $P(H_0), P(H_1), P(H_2)$	0.25,0.5,0.25
Constraints for correct detection probabilities	$a = 0.99$ (Except **Fig. 6**) $b = 0.9$ (Except **Fig. 6** ~ **Fig. 8**)
PU's position	(0,0)
PU's transmit power	$P_{\mathrm{PU}} = 100$
Noise variance	$\sigma_{\mathrm{N1}}^2 = \sigma_{\mathrm{N2}}^2 = 1$
Number of samples	N=100 (Except **Fig. 8**)

5.1 Performance of Multiple-Phase Energy Detection for PUEA

In this section, the performance of the proposed multiple-phase energy detection scheme for PUEA is evaluated. Under each of three Prior states, we carried out 10,000 Monte Carlo simulations to test the performance. To simplify the expression, we define that $\gamma_{\mathrm{Xs}} = 10\log_{10}(\sigma_{\mathrm{Xs}}^2 / \sigma_{\mathrm{Ns}}^2)$, where $s = 1, 2$ and X is P or M. Dis_s^{X} denote the distances of the s-th SU from the PU or MU. The received power of each SU can be calculated by $\sigma_{\mathrm{Ps}}^2 = z_{\mathrm{Ps}} P_{\mathrm{PU}} = P_{\mathrm{PU}} / (Dis_s^{\mathrm{P}})^2$ and $\sigma_{\mathrm{Ms}}^2 = z_{\mathrm{Ms}} P_{\mathrm{MU}} = P_{\mathrm{MU}} / (Dis_s^{\mathrm{M}})^2$.

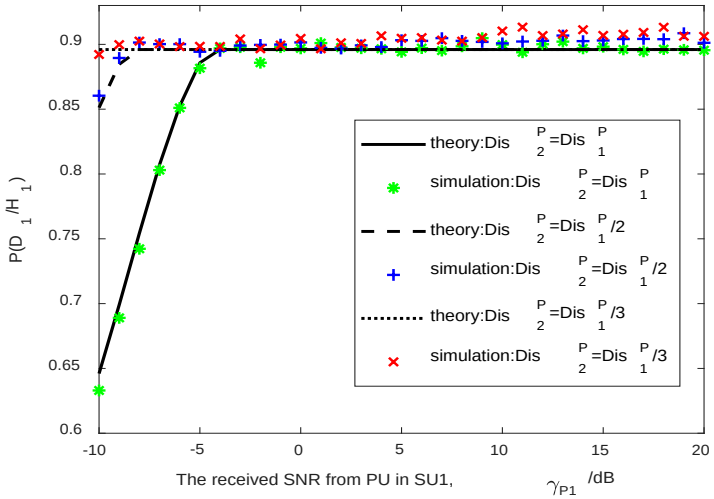

Fig. 3. $P(D_1 / H_1)$ where the distances of two SUs from the PT are varied

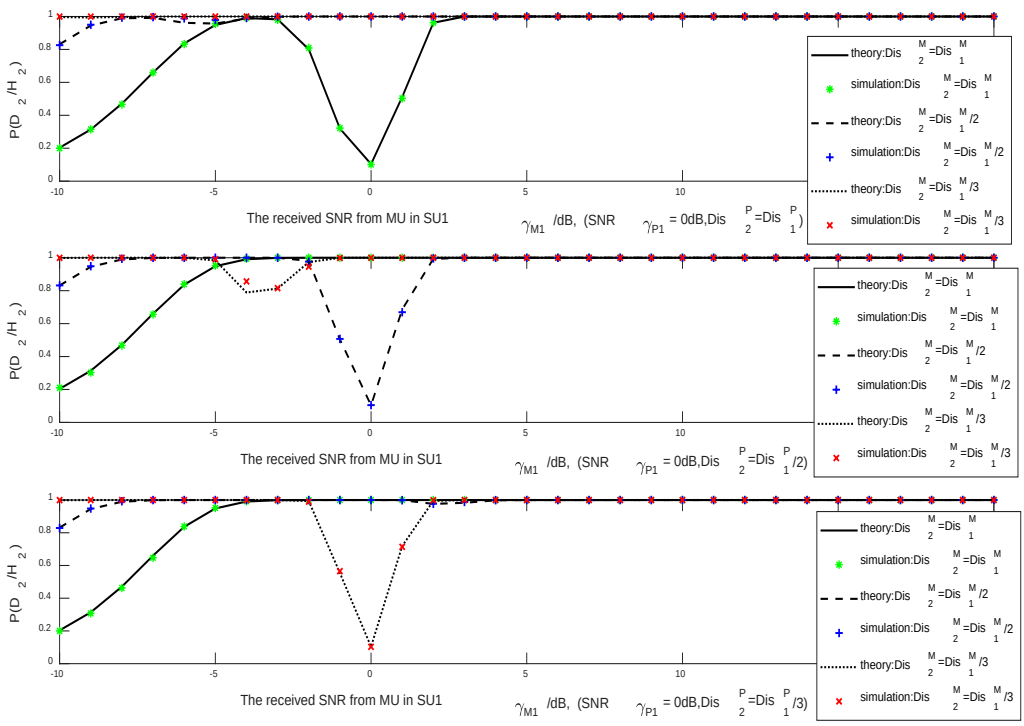

Fig. 4. $P(D_2 / H_2)$ where the distances of two SUs from the PT and the MU are varied

Fig. 3 and **Fig. 4** give the detection probabilities under H_1 and H_2 states for various distances of two SUs from the PT or the MU, respectively. Here, only one MU is considered. Since the correct detection probability under actual state H_1 is concerned in **Fig. 3**, PU is always existing and then MU keeps silent in this simulation. This is according to the

assumption that MUs only attack in the absence of PU. From **Fig. 3**, we can see that all the simulation results are roughly located in the theory lines. Here, the theory results are corresponding to the analysis results given in Appendix. It can be seen that the practical probabilities of correction detection under H_1 basically satisfy the constraints preset. When the distances between the two users and the PT are different, the simulation value is slightly higher than the theoretical value which is induced by the approximate assumptions used in calculating the thresholds. However, such a little bias of the simulation result from the analytical result indicates that the independence assumption among different detection statistics is feasible. In **Fig. 4**, different PU's locations are considered, but the PU does not transmit signal during the whole simulation, for the detection of PUEA being focused on. From **Fig. 4**, it can be seen clearly that the probability of detecting PUEA will decrease as σ^2_{Mk} approaches σ^2_{Pk} and it will reach the minimum value when the distance feature of two SUs from the MU are same as that from the PT. Moreover, it can be seen from the cases of low SNR in **Fig. 3** and **Fig. 4** that the larger difference of the distances between two SUs from the PT or MU is, the higher detection probability is. This means that different power features of various SUs contribute more to detect PUEA.

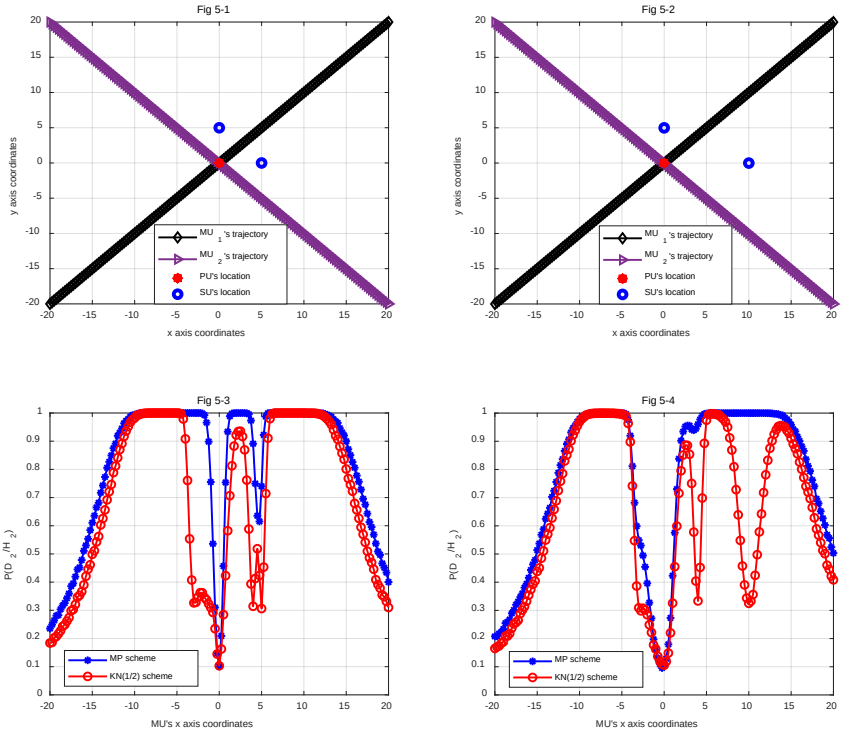

Fig. 5. The PUEA detection probability with two moving Mus

Next, we would compare the proposed detection scheme with a CSS scheme which uses the K/N guideline [26]. Here, $P(D_0 / H_0)$ and $P(D_1 / H_1)$ of two schemes are kept same so that only $P(D_2 / H_2)$ curves are compared. Because there are two SUs, the 1/2 rule with detection priority $D_1 > D_2 > D_0$ is included for the baseline scheme. In **Fig. 5**, two MUs move along

two different straights lines synchronously. Moreover, they have different transmitting powers, i.e, $P_{\mathrm{M1}}=60$ and $P_{\mathrm{M2}}=40$. Two cases of $Dis_2^{\mathrm{P}}=Dis_1^{\mathrm{P}}$ and $Dis_2^{\mathrm{P}}\neq Dis_1^{\mathrm{P}}$ are simulated. It can be seen that the proposed scheme is better than the K/N scheme except the cases that two MUs move to the same location of PT. In these situations, both schemes reach to the worst detection performance and they are both not able to identify MU from PT completely. Particularly, in the case that two SUs have different distances from the PT, the advantage of our method over the baseline one is more obvious. When the MUs are far from the SUs, the σ_{Ms}^2 received by the SUs are very small. Then, the channel state is most detected to be H_0 and the probability of detecting MU is low just shown in the left and right side of the curves.

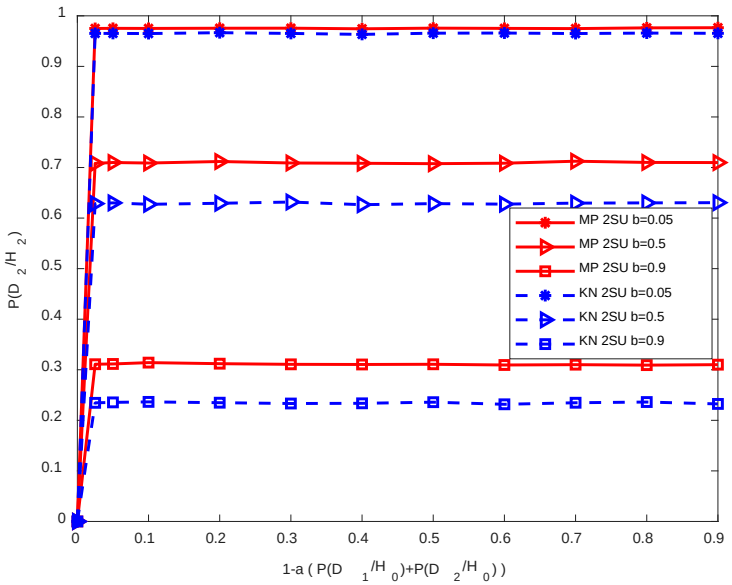

Fig. 6. $P(D_2/H_2)$ vs false alarm probability with different $P(D_1/H_1)$

The receiver operation characteristic (ROC) curves are always used to evaluate the detection performance of the traditional two-state hypothesis testing. For a three-state hypothesis, the similar curves can also be drawn. Since PU and PUEA are both the detection objects, $P(D_1/H_0)+P(D_2/H_0)$ could be taken as the false-alarm probability. Accordingly, the detection probability could be $P(D_1/H_1)+P(D_2/H_2)$. To show more details, the variation of $P(D_2/H_2)$ with the false-alarm probability under three fixed $P(D_1/H_1)$ is presented in Fig.6. Here, two SUs have different received SNRs from the PT and the MU, which are setting as $\gamma_{\mathrm{P1}}=5dB$, $\gamma_{\mathrm{P2}}=4dB$, $\gamma_{\mathrm{M1}}=5.5dB$ and $\gamma_{\mathrm{M2}}=4.5dB$, respectively. It can be seen that the PUEA detection probabilities for both schemes increase very fast with the false-alarm probability and soon converge to a high level at a very low false-alarm probability. This benefits from CSS of multiple SUs. Further, the proposed scheme still outperforms the K-out-N method especially at a high PU detection probability. From Fig.7, it is also demonstrated that $P(D_2/H_2)$ is almost independent on the false-alarm probability but significantly affected by PU detection probability. Therefore, in the following two figures, the variation of $P(D_2/H_2)$ with $P(D_1/H_1)$ is concerned.

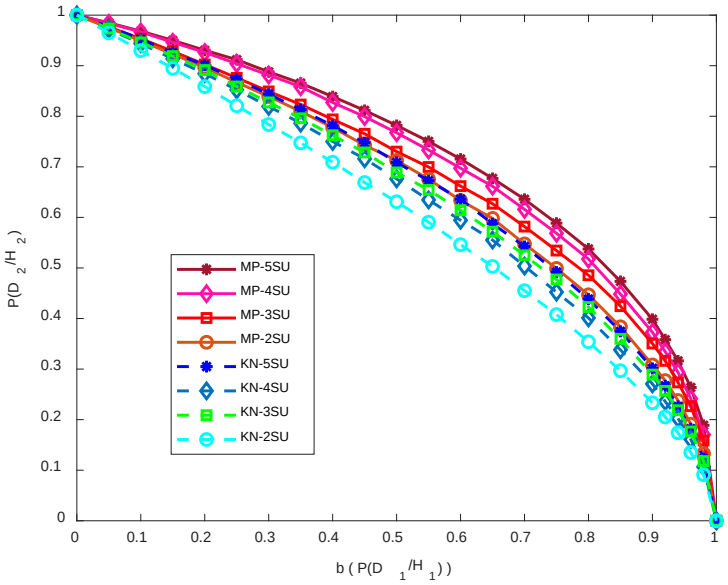

Fig. 7. $P(D_2 / H_2)$ vs $P(D_1 / H_1)$ with different numbers of SUs

Moreover, the various number of SUs from 2 to 5 is considered in **Fig. 7**. Here, the value of a in the constraint condition $P(D_0 / H_0) \geq a$ is fixed as 0.99 and we change the setting of b. SNRs of different SUs from the PT and MU are setting as $\gamma_{\mathrm{P1}} = 5dB$, $\gamma_{\mathrm{P2}} = 4dB$, $\gamma_{\mathrm{P3}} = 3dB$, $\gamma_{\mathrm{P4}} = 2dB$, $\gamma_{\mathrm{P5}} = 1dB$, $\gamma_{\mathrm{M1}} = 5.5dB$, $\gamma_{\mathrm{M2}} = 4.5dB$, $\gamma_{\mathrm{M3}} = 3.5dB$, $\gamma_{\mathrm{M4}} = 2.5dB$ and $\gamma_{\mathrm{M5}} = 1.5dB$, respectively. As can be seen from **Fig. 7**, the greater number of SUs is, the better detection performance is for the multiple-phase detection method. The proposed scheme outperforms the K/N one with the same number of SUs. Concretely, the MP detection scheme with two SUs has nearly the same detection performance as the K/N scheme with five SUs. Moreover, we can see that the detection probability of PUEA reduces with the detection probability of PU increasing.

In addition, **Fig. 8** shows the effect of the number of samples N on the PUEA detection performance. The other system assumption is same as the simulation of **Fig. 6**. From **Fig. 8**, it can be shown that the PUEA detection probability becomes larger with N growing for an appointed PU detection probability. The outperformance of our scheme over K/N method is more obvious with middle N, such as 100 and 500. In a practical system, for a longer N, the data transmission time left in a frame would be shorter and then the throughput of secondary network may reduce. Therefore, N should be selected appropriately to obtain a good tradeoff between the sensing performance and the throughput of secondary network. The optimization of N is not covered in our work yet, but it can be involved in the optimization problem for the resource allocation in future work.

5.2 Performance of Effective Capacity based Resource Allocation

In this section, the proposed effective capacity based joint SUs scheduling and power allocation scheme is evaluated. The performance indicator is the weighted sum of the two SUs' normalized effective rates over bandwidth *B*. Without loss of generality, we consider a

specific scenario where the transmitting powers are set as $P_{\mathrm{P}} = P_{\mathrm{M}} = \overline{P} = 100$, and the positions of the PT, MU, SU-1 and SU-2 are located at (0,0), (10,10), (10,0) and (5,0), respectively. The ST locates in the middle of two SUs. If there is no special explanation the multiple-phase (MP) energy detector proposed in Section 3 is used for spectrum sensing. Furthermore, the sensing time is 9% of one frame.

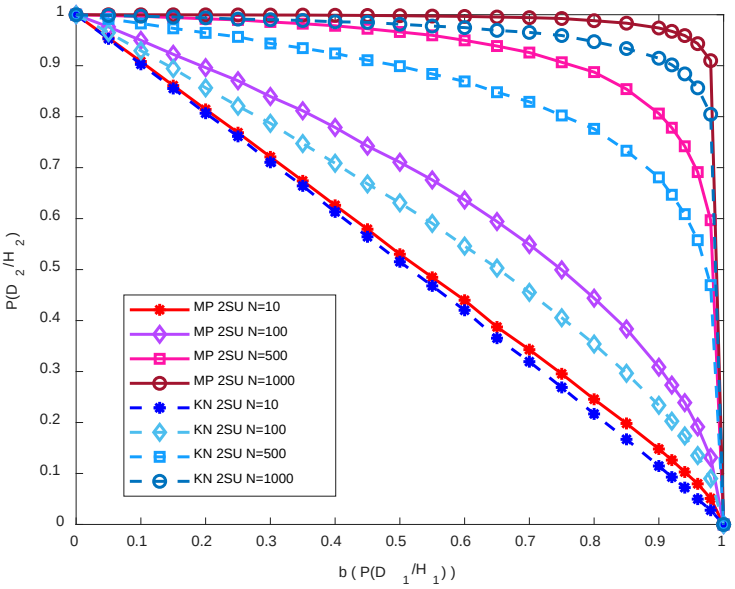

Fig. 8. $P(D_2 / H_2)$ vs $P(D_1 / H_1)$ with different sensing lengths

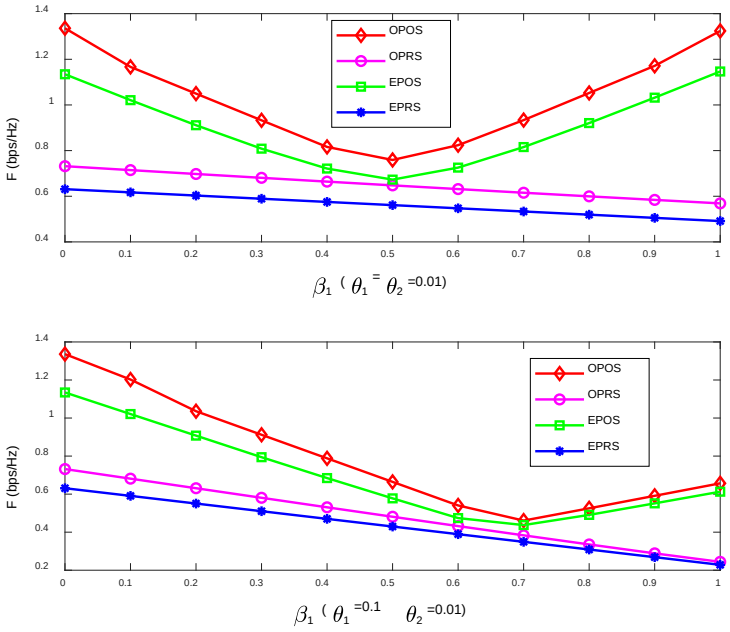

Fig. 9. Weighted sum of two SU's effective rates of various schemes vs β_1

We compare the proposed joint optimization scheme, denoted by OPOS in the following figures, with the schemes called the optimized-power allocation and random-scheduling (OPRS), the equal-power allocation and optimized-scheduling (EPOS) and the equal-power allocation and random-scheduling (EPRS). Here, the equal-power allocation indicates that the transmission powers of the ST under two detected statues D_0 and D_2 are equal and keep stable for any SU's channel state. The Random-Scheduling indicates that the scheduling matrix is randomly selected among the set of $[1,...,M]^{K^M}$.

Fig. 9 shows the weighted sum of two SU's effective rates versus the weighting factor β_1 under the conditions of $\theta_2 = \theta_1$ and $\theta_2 \neq \theta_1$, respectively. It can be seen obviously that the joint optimization schemes proposed has the highest weighted sum of two SUs' effective capacity. Specially, we can see from the below subfigure that the right end points of two curves including optimized-scheduling are both lower than the left end points. The formers correspond to the case only serving SU-1 and the letter ones indicate that SU-2 is always scheduled. This result show that the effective rate is smaller for a larger θ, which satisfies the basic principle of effective capacity. Specially, we can find from two subfigures that the improvement of optimization-scheduling is more evident than the optimization-power allocation as a whole.

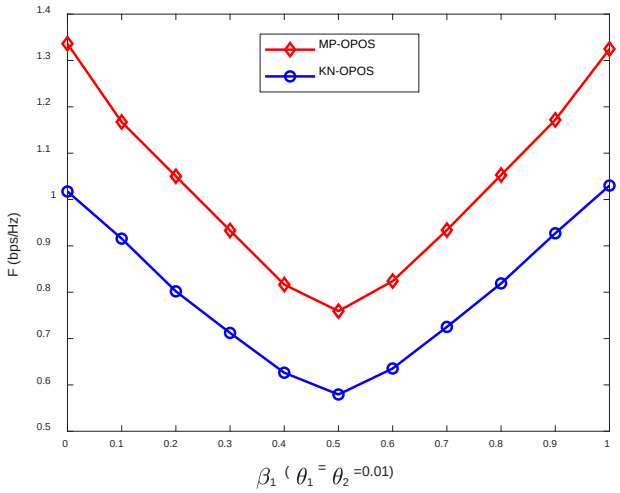

Fig. 10. Weighted sum of two SU's effective rates with two PUEA detectors

In **Fig. 10**, the performance of OPOS scheme is given under two cases that the proposed MP energy detection and the K/N detection are used, respectively. It can be seen that the improvement of the detection accuracy can obtain better effective rate. The performance gain with the MP detector is about 0.3 bps/Hz under the specific scenario in our simulation. This is because the detection probabilities have an obvious effect on the resource allocation. Concretely, $P(D_0, H_1)$ and $P(D_2, H_1)$ would affect the setting of $\eta\left(m_k, D_j\right)$ and $P(D_2, H_2)$ would affect the opportunity of SUs to transmit data.

In **Fig. 11**, we compare two transmission modes, namely the D_0 and D_2 mode and the only D_0 mode. The former one means SUs will transmit data when the detection result is D_0 or D_2. The letter one corresponds to that SUs will transmit data only when the detection result is D_0

and this mode is also the pure overlay mode in [27]. It can be seen that F is larger for the D_0 and D_2 mode than that for the only D_0 mode. That is the advantage caused by letting SU transmit data under the status D_2. In both modes, $E_{z,D_i}\left[\eta\left(m_k, D_i\right)\right]$ is close to 1. However, under the D_0 and D_2 mode, the real interference power I is close to the upper limit P_{up} (0.1), while under only D_0 mode, the interference power I is nearly 0. The light improved interference of SU to the PU is just the cost of the proposed scheme.

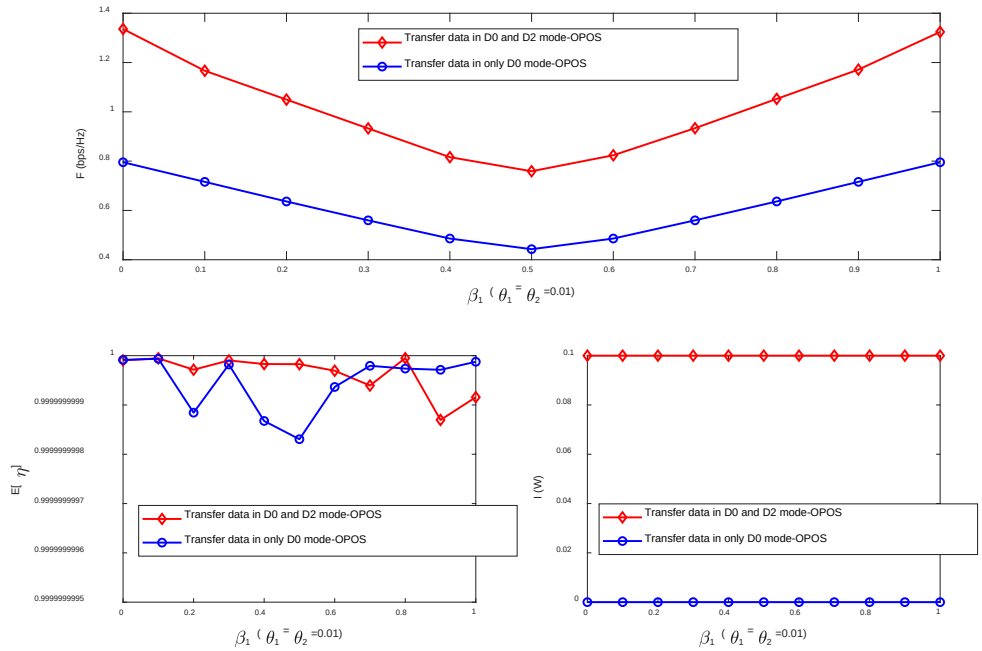

Fig. 11. Weighted sum of two SU's effective rates under two transmission modes

In order to show the computation efficiency of our resource allocation scheme, the runtime is recorded during simulation operation. Using MATLAB on an Intel(R) Core(TM) i3-7100 3.90GHz with Windows operation system (OS), the average runtime needed by searching S for one time is about 5.07 seconds. The mean runtime of CVX to find $\mathbf{\Gamma}$ is approximately 11.74 seconds. The number of iteration is about 4 in our simulation. Thus, the overall computation cost is about 67 seconds. Here, M=2 and K=4. The overall computation cost is more dependent on the operation overhead of CVX toolbox, which is consistent with the analysis in Section 4.3.

5. Conclusions

Primary user emulation attack (PUEA) could worsen the QoS of SUs in cognitive radio networks through emulating the PU to transmit signals over the idle primary channel and trying to prevent SUs from accessing the spectrum. Aiming at this attack problem, a multiple-phase energy detection scheme based on the cooperation of multiple secondary users is first proposed to detect the PUEA more accurately. Further, the weights in detection statistics and the decision thresholds are determined. Second, a joint SUs scheduling and

power allocation scheme based on effective capacity is proposed to guarantee the different delay QoS of multiply SUs. Its objective is to maximize the weighted effective capacity of the SUs with a constraint of the average interference to the PU. The simulation results show that the proposed PUEA detector has higher detection accuracy for PUEA. The new resource allocation scheme can effectively improve the weighted sum effective capacity of SUs by allowing SUs to transmit data when the primary channel is detected to be occupied by the attacker. However, the given PUEA detector is still based on the simple energy detection. Then, the detection will be false when the MU can emulate the received energy feature at all the SUs similar as from the PT. Since such an attack is not difficult for the MU with the developing of signal processing ability and smart level. Therefore, a more efficient detector would be studied in future, which can explore more features of transmitting signals and use intelligent learning technique. In addition, the parameters in both the sensing phase and the data transmitting phase would be optimized jointly to obtain the better whole system performance.

Appendix

The probabilities of nine PUEA detection cases with two SUs are calculated as

Case 1:

$$P_{00} = P(H_0)P(D_0 / H_0) = P(H_0)P(V_1 \le \lambda_0) = P(H_0)\left[1 - Q\left((\lambda_0 - \beta_{i0})/\sqrt{\delta_{i0}^2}\right)\right]$$

Case 2:

$$P_{01} = P(H_0)\int_{\lambda_{11}}^{\lambda_{12}}\int_{\lambda_{21}}^{\lambda_{22}}[2\pi\delta_{10}\delta_{20}\sqrt{1-\rho^2}]^{-1}\exp\left\{-[2(1-\rho^2)]^{-1}\left[(V_1-\beta_{10})/\delta_{10} - \sqrt{\rho}(V_2-\beta_{20})/\delta_{20}\right]^2\right\}dV_1dV_2$$

Case 3:

$$P_{02} = P(H_0)P(D_2 / H_0) = P(H_0)\left\{Q\left((\lambda_0-\beta_{10})/\sqrt{\delta_{10}^2}\right) - Q\left((\lambda_{11}-\beta_{10})/\sqrt{\delta_{10}^2}\right) + Q\left((\lambda_{12}-\beta_{10})/\sqrt{\delta_{10}^2}\right) + \right.$$
$$\int_{\lambda_{11}}^{\lambda_{12}}\int_{0}^{\lambda_{21}}(2\pi\delta_{10}\delta_{20}\sqrt{1-\rho^2})^{-1}\exp\left\{-[2(1-\rho^2)]^{-1}\left[(V_1-\beta_{10})/\delta_{10} - \sqrt{\rho}(V_2-\beta_{20})/\delta_{20}\right]^2\right\}dV_1dV_2 +$$
$$\left.\int_{\lambda_{11}}^{\lambda_{12}}\int_{\lambda_{22}}^{\infty}(2\pi\delta_{10}\delta_{20}\sqrt{1-\rho^2})^{-1}\exp\left\{-[2(1-\rho^2)]^{-1}\left[(V_1-\beta_{10})/\delta_{10} - \sqrt{\rho}(V_2-\beta_{20})/\delta_{20}\right]^2\right\}dV_1dV_2\right\}$$

Case 4:

$$P_{10} = P(H_1)P(D_0 / H_1) = P(H_1)\left[1 - Q\left((\lambda_0 - \beta_{1P})/\sqrt{\delta_{1P}^2}\right)\right]$$

Case 5:

$$P_{11} = P(H_1)\int_{\lambda_{11}}^{\lambda_{12}}\int_{\lambda_{21}}^{\lambda_{22}}(2\pi\delta_{1P}\delta_{2P}\sqrt{1-\rho^2})^{-1}\exp\left\{-[2(1-\rho^2)]^{-1}\left[(V_1-\beta_{1P})/\delta_{1P} - \sqrt{\rho}(V_2-\beta_{2P})/\delta_{2P}\right]^2\right\}dV_1dV_2$$

Case 6:

$$P_{12} = P(H_1)P(D_2 / H_1) = P(H_1)\left\{Q\left((\lambda_0-\beta_{1P})/\sqrt{\delta_{1P}^2}\right) - Q\left((\lambda_{11}-\beta_{1P})/\sqrt{\delta_{1P}^2}\right) + Q\left((\lambda_{12}-\beta_{1P})/\sqrt{\delta_{1P}^2}\right) + \right.$$
$$\int_{\lambda_{11}}^{\lambda_{12}}\int_{0}^{\lambda_{21}}(2\pi\delta_{1P}\delta_{2P}\sqrt{1-\rho^2})^{-1}\exp\left\{-[2(1-\rho^2)]^{-1}\left[(V_1-\beta_{1P})/\delta_{1P} - \sqrt{\rho}(V_2-\beta_{2P})/\delta_{2P}\right]^2\right\}dV_1dV_2 +$$
$$\left.\int_{\lambda_{11}}^{\lambda_{12}}\int_{\lambda_{22}}^{\infty}(2\pi\delta_{1P}\delta_{2P}\sqrt{1-\rho^2})^{-1}\exp\left\{-[2(1-\rho^2)]^{-1}\left[(V_1-\beta_{1P})/\delta_{1P} - \sqrt{\rho}(V_2-\beta_{2P})/\delta_{2P}\right]^2\right\}dV_1dV_2\right\}$$

Case 7:

$$P_{20} = P(H_2)P(D_0 / H_2) = P(H_2)\left[1 - Q\left((\lambda_0 - \beta_{1M})/\sqrt{\delta_{1M}^2}\right)\right]$$

Case 8:

$$P_{21} = P(H_2)\int_{\lambda_{11}}^{\lambda_{12}}\int_{\lambda_{21}}^{\lambda_{22}}(2\pi\delta_{1M}\delta_{2M}\sqrt{1-\rho^2})^{-1}\exp\left\{-[2(1-\rho^2)]^{-1}\left[(V_1-\beta_{1M})/\delta_{1M} - \sqrt{\rho}(V_2-\beta_{2M})/\delta_{2M}\right]^2\right\}dV_1dV_2$$

Case 9:

$$P_{22} = P(H_2)P(D_2 / H_2) = P(H_2)\left\{Q\left((\lambda_0-\beta_{1M})/\sqrt{\delta_{1M}^2}\right) - Q\left((\lambda_{11}-\beta_{1M})/\sqrt{\delta_{1M}^2}\right) + Q\left((\lambda_{12}-\beta_{1M})/\sqrt{\delta_{1M}^2}\right) + \right.$$

$$\int_{\lambda_{11}}^{\lambda_{12}}\int_{0}^{\lambda_{21}}(2\pi\delta_{1M}\delta_{2M}\sqrt{1-\rho^2})^{-1}\exp\left\{-[2(1-\rho^2)]^{-1}\left[(V_1-\beta_{1M})/\delta_{1M} - \sqrt{\rho}(V_2-\beta_{2M})/\delta_{2M}\right]^2\right\}dV_1dV_2 +$$

$$\left.\int_{\lambda_{11}}^{\lambda_{12}}\int_{\lambda_{22}}^{\infty}(2\pi\delta_{1M}\delta_{2M}\sqrt{1-\rho^2})^{-1}\exp\left\{-[2(1-\rho^2)]^{-1}\left[(V_1-\beta_{1M})/\delta_{1M} - \sqrt{\rho}(V_2-\beta_{2M})/\delta_{2M}\right]^2\right\}dV_1dV_2\right\}$$

where ρ is the correlation coefficient between V_1 and V_2.

References

[1] Liang, Ying Chang, et al., "Cognitive radio networking and communications: An Overview," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 7, pp. 3386-3407, Sept. 2011. Article (CrossRef Link).

[2] F.C.C.S.P.T. Force, "Report of the spectrum efficiency working group," *Federal Communications Commission, Tech. Report*, pp.2–155, 2002. Article (CrossRef Link).

[3] Sasipriya S, Vigneshram R, "An overview of cognitive radio in 5G wireless communications," in *Proc. of IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1-5, Chennai, December 15-17, 2016. Article (CrossRef Link).

[4] Hu F, Chen B, Zhu K, "Full spectrum sharing in cognitive radio networks toward 5G: A survey," *IEEE Access*, vol. 6, pp. 15754-15776, 2018. Article (CrossRef Link).

[5] Chen, Ruiliang, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25-37, Jan. 2008. Article (CrossRef Link).

[6] W. Ghanem, R. Essam, M. Dessouky, "Proposed particle swarm optimization approaches for detection and localization of the primary user emulation attack in cognitive radio networks," in *Proc. of 35th National Radio Science Conference*, pp. 309-318, Cairo, March 27-29, 2018.

[7] Dang, Manman, Z. Zhao, and H. Zhang, "Optimal cooperative detection of primary user emulation attacks in distributed cognitive radio network," in *Proc. of 8th International Conference on Communications and Networking, Guilin*, pp. 368-373, August 14-16, 2013. Article (CrossRef Link).

[8] Saber M J, Sajad Sadough S M, "Optimization of cooperative spectrum sensing for cognitive radio networks in the presence of smart primary user emulation attack," *Transactions on Emerging Telecommunications Technologies, Tehran*, vol. 28, no. 1, pp.1113-1116, 2014. Article (CrossRef Link)

[9] Ali S A, Mohammad M B, "Performance improvement of cooperative spectrum sensing in the presence of primary user emulation attack," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 42, no. 4, pp.493-499, 2018.Article (CrossRef Link)

[10] Shrivastava S, Rajesh A, Bora P K, "A simplified counter approach to primary user emulation attacks from secondary user perspective," in *Proc. of 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications* , pp. 2149-2154, Hong Kong, Aug 30- Sept 2, 2015. Article (CrossRef Link)

[11] Sharifi M, Sharifi A A, Niya M J M, "Cooperative spectrum sensing in the presence of primary user emulation attack in cognitive radio network: multi-level hypotheses test approach," *Wireless Networks*, vol. 24, no. 1, pp.61-68, 2018.Article (CrossRef Link)
[12] Jo M, Han L, Kim D, et al., "Selfish attacks and detection in cognitive radio Ad-Hoc networks," *IEEE Network*, vol. 27, no. 3, pp. 46-50, May-June 2013. Article (CrossRef Link).
[13] Wu, Dapeng, and R. Negi, "Effective capacity: a wireless link model for support of quality of service," *IEEE Trans. on Wireless Communications*, vol. 2, no. 4, pp. 630-643, July 2003. Article (CrossRef Link).
[14] Haghighat M, Fathi H, Sadough S M S, "Robust resource allocation for OFDM-based cognitive radio in the presence of primary user emulation attack," *RadioEngineering*, vol. 21, no. 4, pp. 1085-1091, 2012.
[15] Karimi M, "Efficient joint resource allocation and spectrum sensing in multiband cognitive radio systems in the presence of PUEA," *International Journal of Advanced Research in Electronics and Communication Engineering*, vol. 4, no. 8, pp.2231-2235, 2015. Article (CrossRef Link).
[16] Das D, Das S, "Intelligent resource allocation scheme for the cognitive radio network in the presence of primary user emulation attack," *IET Communications*, vol. 11, no. 15, pp. 2370-2379, 2017.Article (CrossRef Link).
[17] Das D, Das S, "An intelligent resource management scheme for SDF-based cooperative spectrum sensing in the presence of primary user emulation attack," *Computers & Electrical Engineering*, vol. 69, pp. 555-571, 2017.Article (CrossRef Link)
[18] Akin, S., and M. C. Gursoy, "Effective capacity analysis of cognitive radio channels for quality of service provisioning," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3354-3364, Nov 2010. Article (CrossRef Link).
[19] Liang Y C, Zeng Y, Peh E C Y, et al., "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1326-1337, April 2008. Article (CrossRef Link).
[20] Jin F, Varadharajan V, Tupakula U, "Improved detection of primary user emulation attacks in cognitive radio networks," in *Proc. of International Telecommunication Networks and Applications Conference*, pp. 274-279, Sydney, November, 18-20, 2015. Article (CrossRef Link).
[21] Balasubramanian A, Miller S L, "The effective capacity of A time division downlink scheduling system," *IEEE Transactions on Communications*, vol. 58, no. 1, pp. 73-78, January 2010. Article (CrossRef Link).
[22] Wu D, Negi R, "Effective capacity: a wireless link model for support of quality of service," *IEEE Transactions on Wireless Communications*, vol. 2, no. 4, pp. 630-643, July 2003. Article (CrossRef Link).
[23] Xu, Yuhua, J. Wang, and Q. Wu, "Effective capacity region of two-user opportunistic spectrum access in fading channel under discrete transmission rate policy," in *Proc. of IEEE International Conference on Wireless Communications and Signal Processing*, pp. 1-5, Oct 21-23, 2010. Article (CrossRef Link).
[24] Liu Q, Zhou S, Giannakis G B, "Queuing with adaptive modulation and coding over wireless links: cross-Layer analysis and design," *IEEE Transactions on Wireless Communications*, vol. 4, no. 3, pp. 1142-1153, May 2005. Article (CrossRef Link).
[25] Mattingley J, Boyd S, "Real-time convex optimization in signal processing," *IEEE Signal Processing Magazine*, vol. 27, no. 3, pp. 50-61, May 2010. Article (CrossRef Link).
[26] Haghighat M, Sadough S M, "Cooperative spectrum sensing in cognitive radio networks under primary user emulation attacks," in *Proc. of IEEE The Sixth International Symposium on Telecommunications, Tehran*, pp. 148-151, Nov 6-8,2012. Article (CrossRef Link).
[27] R. Menon, R. M. Buehrer, and J. H. Reed, "Outage probability based comparison of underlay and overlay spectrum sharing techniques," in *Proc. of First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, pp. 101–109, Nov. 8-11, 2005. Article (CrossRef Link).

Zongyi Liu is currently a Researcher in Xi'an Research Institute of Surveying and Mapping, Xi'an, China. His research interests mainly include signal processing technology, geographical remote sensing technology and GNSS technology.

Guomei Zhang is currently an Associate Professor in the School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China. Her research interests mainly include Massive MIMO, 3D MIMO, physical layer security and interference management in wireless communications.

Wei Meng is currently a graduate student in the School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China. His research interests include signal processing technology.

Xiaohui Ma is currently an Engineer in Xi'an Research Institute of Surveying and Mapping, Xi'an, China. His research interests include space geodesy, invariant reference point simulation of VLBI, and wireless communications techniques in GNSS.

Guobing Li is currently an Associate Professor in the School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China. His research interests include wireless relay network, MIMO techniques and 5G mobile communication systems.