Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

On detecting primary user emulation attack using channel impulse response in the cognitive radio network*

Qiao-mu JIANG[1], Hui-fang CHEN‡[1,2], Lei XIE[1,2], Kuang WANG[1,2]

([1]*College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China*)

([2]*Zhejiang Provincial Key Laboratory of Information Processing, Communication and Networking, Hangzhou 310027, China*)

E-mail: jiangqm@zju.edu.cn; chenhf@zju.edu.cn; xiel@zju.edu.cn; wangk@zju.edu.cn

Received Mar. 23, 2017; Revision accepted Aug. 9, 2017; Crosschecked Oct. 10, 2017

Abstract: Cognitive radio is an effective technology to alleviate the spectrum resource scarcity problem by opportunistically allocating the spare spectrum to unauthorized users. However, a serious denial-of-service (DoS) attack, named the 'primary user emulation attack (PUEA)', exists in the network to deteriorate the system performance. In this paper, we propose a PUEA detection method that exploits the radio channel information to detect the PUEA in the cognitive radio network. In the proposed method, the uniqueness of the channel impulse response (CIR) between the secondary user (SU) and the signal source is used to determine whether the received signal is transmitted by the primary user (PU) or the primary user emulator (PUE). The closed-form expressions for the false-alarm probability and the detection probability of the proposed PUEA detection method are derived. In addition, a modified subspace-based blind channel estimation method is presented to estimate the CIR, in order for the proposed PUEA detection method to work in the scenario where the SU has no prior knowledge about the structure and content of the PU signal. Numerical results show that the proposed PUEA detection method performs well although the difference in channel characteristics between the PU and PUE is small.

Key words: Cognitive radio network; Primary user emulation attack; Subspace-based blind channel estimation; Channel impulse response

https://doi.org/10.1631/FITEE.1700203 **CLC number:** TN918.91

1 Introduction

With the rapid development of wireless communication technologies, the contradiction between the increasing demand of the spectrum band and the limited spectrum resource has become one of the main factors restricting the application of wireless systems. Cognitive radio (CR) has emerged as a promising technology for resolving the spectrum scarcity and underutilization problems (Haykin, 2005).

In a cognitive radio network (CRN), secondary users (SUs) are allowed to share the spectrum with primary users (PUs). SUs first identify the spare spectrum through spectrum sensing, and then share the spare spectrum for communication. However, the CRN is vulnerable to attacks, among which the primary user emulation attack (PUEA) is a typical one. In the PUEA, the attacker, named the 'primary user emulator (PUE)', emulates the PU signal to deter SUs from accessing the unoccupied spectrum band (Chen and Park, 2006).

‡ Corresponding author

* Project supported by the National Natural Science Foundation of China (Nos. 61471318 and 61671410), the Zhejiang Provincial Natural Science Foundation of China (No. LY14F010014), and the State Key Laboratory of Complex Electromagnetic Environment Effects on Electronics and Information System, China (No. CEMEE2015Z0202A)

ORCID: Hui-fang CHEN, http://orcid.org/0000-0002-1366-1030

In the past decade, the PUEA problem in the CRN has been widely investigated, and many PUEA detection methods have been proposed. Chen and Park (2006) proposed a transmitter location verification scheme to detect the PUEA, in which the distance ratio test and the distance difference test were used to implement location verification. Chen *et al.* (2008) proposed another transmitter location verification scheme, in which the received signal strength (RSS) was used to discover the location of the transmitter. Jin *et al.* (2009) proposed an energy detection method to detect the PUEA using two binary hypothesis tests, the Neyman-Pearson composite hypothesis test and the Wald sequential probability ratio test. In Nguyen *et al.* (2012), the radio frequency fingerprint of a transmitter in terms of the carrier frequency difference, the phase shift difference, and the second-order cyclostationary, was used to detect the PUEA. Xin and Song (2014) presented a novel PUEA detection method based on the activity pattern of the reconstructed signal. This method needs no prior knowledge about the PU signal and has no limitations on the type of PU. In Pu and Wyglinski (2014), the PU and PUE were identified respectively with a database and an artificial neural network using the action recognition technique to analyze the transmitted sequences in the frequency domain. Jin *et al.* (2015) proposed a PUEA detection method based on energy detection and localization, and introduced a decision mechanism with multiple thresholds. All these PUEA detection methods use two kinds of information: one is the characteristic of the transmitter, and the other is the characteristic of the received signal.

As we know, it is impossible for the PUE to emulate the multi-path channel characteristic in wireless communication. Therefore, the multi-path channel characteristic can be used to differentiate between signals from different sources. A PUEA detection method using the channel-tap power between the signal source and the receiver has been proposed (Chin *et al.*, 2014; Le *et al.*, 2015; 2016). However, this method uses only the amplitude of the multi-path channel impulse response (CIR). Therefore, in this work, we investigate the PUEA detection method based on the uniqueness of the CIR between the transmitter and the receiver.

To estimate the multi-path CIR, several channel estimation methods have been proposed. Channel estimation methods can be classified into two categories: data-aided channel estimation method and blind channel estimation method. The data-aided channel estimation method exploits the additional information known to the receiver, such as pilot symbols (Lalos *et al.*, 2010; Zhou and Lam, 2010), the pseudo noise sequence (Liu *et al.*, 2012), or previously estimated symbols (Tomasoni *et al.*, 2013), to estimate the instantaneous CIR. The blind channel estimation method uses the auto-correlation characteristic of the transmitted sequence and the second-order statistics feature of the received signal to realize an accurate estimation of the CIR without prior knowledge about the content of the transmitted signal. The most widely used blind channel estimation method is subspace-based estimation. Muquet *et al.* (2002) proposed a blind channel estimation algorithm for the orthogonal frequency division multiplexing (OFDM) system and proved that the CIR can be uniquely determined up to a scalar factor. By using the circulant property of the received signal, the improved subspace-based blind channel estimation algorithms proposed by Su and Vaidyanathan (2007) and Kim *et al.* (2012) significantly reduce the required number of received symbols. Fang *et al.* (2013) proposed a novel method to estimate the real and imaginary parts of the CIR individually by decoupling the real and imaginary parts of the received signal. In this study, we investigate the blind channel estimation method based on the work of Su and Vaidyanathan (2007).

In this study, we propose a PUEA detection method using the channel characteristic in the CRN, where both the amplitude and phase of the multi-path CIR are used. To estimate the multi-path CIR between the SU and the signal source (PU or PUE), a modified blind channel estimation method is presented, where prior knowledge about the structure and content of the PU signal is not needed. Based on the multi-path CIR, a binary hypothesis test is constructed to determine whether the received signal at the SU is transmitted by the PU or PUE. The performance of the proposed PUEA detection method is analyzed in terms of the false-alarm probability and the detection probability, and the closed-form expressions are derived. The proposed PUEA detection method is validated by Monte-Carlo simulations. Numerical results show that the proposed PUEA detection method performs well.

For clarity, we explain the denotation of some notations used in this study. Boldface lower and upper case letters denote column vectors and matrices, respectively. Superscripts $(\cdot)^*$, $(\cdot)^{\mathrm{T}}$, and $(\cdot)^{\mathrm{H}}$ represent the conjugate, transpose, and transpose-conjugate operations, respectively. $\boldsymbol{I}_N$ denotes an $N \times N$ identity matrix, $\boldsymbol{0}_{M\times N}$ denotes an $M \times N$ null matrix, and $\boldsymbol{F}_N$ denotes an $N \times N$ fast Fourier transform (FFT) matrix. For $\boldsymbol{v} = [v_1, v_2, \ldots, v_m]^{\mathrm{T}}$, $[\boldsymbol{v}]_b^a$ denotes a $(b - a + 1) \times 1$ column vector as $[\boldsymbol{v}]_b^a = [v_a, v_{a+1}, \ldots, v_b]^{\mathrm{T}}$, where $a \leq b$ and $v_k = v_{[(k-1) \bmod m]+1}$ if $k < 1$ or $k > m$.

2 System model and assumptions

As we know, IEEE 802.22 is the first worldwide effort to define a standard based on CR techniques, using the spare spectrum of the TV bands for opportunistic communication. We consider a CRN system consisting of a PU network and a CRN. In this study, the PU network is assumed to be the digital terrestrial multimedia broadcast (DTMB) network, in which the time-domain synchronization orthogonal frequency division multiplexing (TDS-OFDM) technology is adopted (National Standard of the People's Republic of China, 2007). In the CRN system, the PU refers to the TV transmitter, and multiple SUs are randomly distributed. A PUE exists in the CRN. The goal of the PUE is to deter the SUs from accessing the spare spectrum bands by emulating the PU signal.

Tugnait and Kim (2010) proved the uniqueness of the channel between the transmitter and the receiver located at two locations in a multi-path wireless communication environment. The characteristics of the wireless channel between the PU and an SU are different from those of the channel between the PUE and the SU. Therefore, from the SU's perspective, the multi-path CIRs can be used to distinguish the PU from the PUE. In addition, we assume that the SU has no prior knowledge about the structure and content of the PU's signal. If the SUs do not cooperate with each other to detect the PUEA, the analysis of the PUEA detection by a single SU can be extended to any SU. In this study, we focus on the detection of PUEA by one SU.

On the other hand, from the attacker's perspective, the PUE has to emulate the real-time CIR between the PU and the SU to bypass the CIR-based PUEA detection. However, due to the uniqueness and time-varying fluctuation of the CIR between the PU and the SU, the only way for the PUE to achieve this goal is to locate near the PU. In this case, because of the limited power resources of the PUE, the transmitted power of the PUE is much lower than that of the PU (i.e., the TV transmitter). Therefore, the PUE can be easily detected by the SU with the naive energy detection method proposed by Jin *et al.* (2009). Furthermore, in the extreme case where the PUE has enough resources to make its transmitted power qualified, the PUE would be captured by government agencies quickly due to its significant interference with the public DTMB system.

In this study, we consider an OFDM system with N subcarriers. At the transmitter, N complex data in an OFDM symbol are first modulated onto N subcarriers with an $N \times N$ inverse fast Fourier transform (IFFT) matrix. That is, $\boldsymbol{s}_N(k) = \boldsymbol{F}_N^{\mathrm{H}}\tilde{\boldsymbol{s}}_N(k)$, where $\tilde{\boldsymbol{s}}_N(k) = [\tilde{s}_1(k), \tilde{s}_2(k), \ldots, \tilde{s}_N(k)]^{\mathrm{T}}$ and $\boldsymbol{s}_N(k) = [s_1(k), s_2(k), \ldots, s_N(k)]^{\mathrm{T}}$ are N complex data and N transmitted signals of the kth OFDM symbol, respectively.

The transmitted OFDM symbol is then enlarged by a cyclic prefix (CP) with size N_{cp} to prevent the inter-symbol-interference (ISI) and to guarantee the orthogonality of the subcarriers. We have

$$\begin{aligned}\boldsymbol{s}(k) &= \left[\boldsymbol{s}_{\mathrm{cp}}^{\mathrm{T}}(k), \boldsymbol{s}_N^{\mathrm{T}}(k)\right]^{\mathrm{T}}\\ &= [\underbrace{s_{N-N_{\mathrm{cp}}+1}(k), s_{N-N_{\mathrm{cp}}+2}(k), \ldots, s_N(k)}_{N_{\mathrm{cp}}},\\ &\quad \underbrace{s_1(k), s_2(k), \ldots, s_N(k)}_{N}]^{\mathrm{T}}.\end{aligned}$$

SUs receive the OFDM symbol transmitted through a multi-path channel, where the CIR between the transmitter and a receiver can be represented as $\boldsymbol{h} = [h_0, h_1, \ldots, h_{N_{\mathrm{cp}}}]^{\mathrm{T}}$.

At a receiver, the received signal can be represented as

$$\begin{aligned}\boldsymbol{y}(k) &= [\underbrace{y_1(k), y_2(k), \ldots, y_{N_{\mathrm{cp}}}(k)}_{N_{\mathrm{cp}}},\\ &\quad \underbrace{y_{N_{\mathrm{cp}}+1}(k), y_{N_{\mathrm{cp}}+2}(k), \ldots, y_{N_{\mathrm{cp}}+N}(k)}_{N}]^{\mathrm{T}}\\ &= [\boldsymbol{y}_{\mathrm{cp}}^{\mathrm{T}}(k), \boldsymbol{y}_N^{\mathrm{T}}(k)]^{\mathrm{T}},\end{aligned}$$

where $\boldsymbol{y}_{\mathrm{cp}}(k) = \boldsymbol{H}_{N_{\mathrm{cp}}}[\boldsymbol{s}_{\mathrm{cp}}^{\mathrm{T}}(k-1), \boldsymbol{s}_{\mathrm{cp}}^{\mathrm{T}}(k)]^{\mathrm{T}} + \boldsymbol{w}_{\mathrm{cp}}(k)$ and $\boldsymbol{y}_N(k) = \boldsymbol{H}_N\boldsymbol{s}(k) + \boldsymbol{w}_N(k)$. $\boldsymbol{H}_k$ is a $k\times$

$(k+N_{\mathrm{cp}})$ Toeplitz matrix with first column $[h_{N_{\mathrm{cp}}}, \mathbf{0}_{1\times(k-1)}]^{\mathrm{T}}$ and first row $[h_{N_{\mathrm{cp}}}, h_{N_{\mathrm{cp}}-1}, \ldots, h_0, \mathbf{0}_{1\times(k-1)}]$. $\boldsymbol{w}(k)$ is the complex additive white Gaussian noise (AWGN) with zero-mean and variance σ_w^2, and

$$\begin{aligned}\boldsymbol{w}(k) =& [\underbrace{w_1(k), w_2(k), \ldots, w_{N_{\mathrm{cp}}}(k)}_{N_{\mathrm{cp}}},\\ &\underbrace{w_{N_{\mathrm{cp}}+1}(k), w_{N_{\mathrm{cp}}+2}(k), \ldots, w_{N_{\mathrm{cp}}+N}(k)}_{N}]^{\mathrm{T}}\\ =& \left[\boldsymbol{w}_{\mathrm{cp}}^{\mathrm{T}}(k), \boldsymbol{w}_N^{\mathrm{T}}(k)\right]^{\mathrm{T}}.\end{aligned}$$

3 Proposed primary user emulation attack detection method

In this section, we first propose a modified blind channel estimation method in an OFDM system, including OFDM symbol structure estimation and subspace-based CIR estimation. Then a PUEA detection method using the CIR is presented.

3.1 Blind channel estimation in an OFDM system

According to the assumption in Section 2, the SU has no prior knowledge about the structure of the OFDM symbol transmitted by the PU, namely N and N_{cp}. Furthermore, without additional information, the existing blind channel estimation methods can determine only the CIR up to a scalar factor, which is insufficient for PUEA detection because the SU needs to extract a unique CIR characteristic from the received signal to verify whether the received signal is from the PU. Therefore, in Section 3.1.1, we present a method for estimating the structure of the OFDM symbol. In Section 3.1.2, a modified subspace-based blind channel estimation method is presented on the basis of the method proposed by Su and Vaidyanathan (2007).

3.1.1 OFDM symbol structure estimation

The received signal sampled at time n at the SU can be written as $y_n = \sum_{l=0}^{N_{\mathrm{cp}}} h_l s_{n-l} + w_n$. Since a CP is inserted at the first part of each OFDM symbol, the transmitted data has the auto-correlation characteristic as follows: if s_n is an element in the CP, $E[s_n s_{n+i}^*] = P_s[\delta(i) + \delta(i-N)]$; otherwise, $E[s_n s_{n+i}^*] = P_s\delta(i)$, where $\delta(i)$ is the Kronecker delta function, and $P_s = E[s_n s_n^*]$ is the average transmitted signal power.

Based on the aforementioned auto-correlation characteristic of the transmitted data, the structure of an OFDM symbol, N and N_{cp}, can be estimated sequentially as

$$\begin{aligned}\hat{N} =& \arg\max_{n\in\mathbb{Z}_+}\max_{n_{\mathrm{cp}}\in[1,n]}\max_{i\in[1,n+n_{\mathrm{cp}}]}\frac{1}{M_t}\\ &\cdot\sum_{k=1}^{M_t} y_{i+(k-1)(n+n_{\mathrm{cp}})}y^*_{i+n+(k-1)(n+n_{\mathrm{cp}})}, \quad (1)\\ \hat{N}_{\mathrm{cp}} =& \arg\max_{n_{\mathrm{cp}}\in[1,\hat{N}]}\max_{i\in[1,\hat{N}+n_{\mathrm{cp}}]}\frac{1}{M_t}\\ &\cdot\sum_{k=1}^{M_t} y_{i+(k-1)(\hat{N}+n_{\mathrm{cp}})}y^*_{i+\hat{N}+(k-1)(\hat{N}+n_{\mathrm{cp}})}, \quad (2)\end{aligned}$$

where M_t is the number of hypothetical OFDM symbols used for estimation. The searching set for $\hat{N}$ is $n\in\mathbb{Z}_+$, while the searching set for $\hat{N}_{\mathrm{cp}}$ is $n_{\mathrm{cp}}\in[1,\hat{N}]$, because the CP length cannot exceed the number of subcarriers. Given a hypothetical CP length and a hypothetical number of subcarriers, the position with the largest statistical auto-correlation value is searched within the length of a hypothetical OFDM symbol, i.e., $i\in[1,n+n_{\mathrm{cp}}]$ and $i\in[1,\hat{N}+n_{\mathrm{cp}}]$ in Eqs. (1) and (2), respectively. The cost function in Eqs. (1) and (2) represents the statistical auto-correlation of the received signal y_n when the delay of the auto-correlation is the hypothetical number of subcarriers, i.e., n and $\hat{N}$ in Eqs. (1) and (2), respectively.

Lemma 1 The expectation of the cost function in Eqs. (1) and (2) is maximized if and only if $\hat{N}=N$ and $\hat{N}_{\mathrm{cp}}=N_{\mathrm{cp}}$.

Proof In the following demonstration, one finds that Lemma 1 holds no matter when $|h_0|\geq|h_{N_{\mathrm{cp}}}|$ or $|h_0|\leq|h_{N_{\mathrm{cp}}}|$, where $|\cdot|$ denotes the absolute value of a complex number. Without loss of generality, we can assume that $|h_0|\geq|h_{N_{\mathrm{cp}}}|$.

If $\hat{N}=N$ and $\hat{N}_{\mathrm{cp}}=N_{\mathrm{cp}}$, the expectation of the cost function in Eqs. (1) and (2) can be expressed as

$$\begin{aligned}E\Bigg[&\max_{i\in[1,N+N_{\mathrm{cp}}]}\frac{1}{M_t}\\ &\cdot\sum_{k=1}^{M_t} y_{i+(k-1)(N+N_{\mathrm{cp}})}y^*_{i+N+(k-1)(N+N_{\mathrm{cp}})}\Bigg]\end{aligned}$$

$$
\begin{aligned}
&=E\Big[\Big(\sum_{l=0}^{N_{\mathrm{cp}}-1} h_l s_{N_{\mathrm{cp}}-l}(k)+w_{N_{\mathrm{cp}}}(k)\Big)\\
&\quad\cdot\Big(\sum_{l=0}^{N_{\mathrm{cp}}-1} h_l s_{N+N_{\mathrm{cp}}-l}(k)+w_{N+N_{\mathrm{cp}}}(k)\Big)^*\Big]\\
&=P_s\sum_{l=0}^{N_{\mathrm{cp}}-1} h_l h_l^*=P_s\sum_{l=0}^{N_{\mathrm{cp}}-1}\sigma_{h_l}^2, \qquad (3)
\end{aligned}
$$

where $\sigma_{h_l}^2=h_l h_l^*$ is the channel-tap power (Chin *et al.*, 2014), and the position with the largest statistical auto-correlation value within the length of a hypothetical OFDM symbol is $i=N_{\mathrm{cp}}$. When $|h_0|\le\left|h_{N_{\mathrm{cp}}}\right|$, the position becomes $i=N_{\mathrm{cp}}+1$, and the result in Eq. (3) becomes $P_s\sum_{l=1}^{N_{\mathrm{cp}}}\sigma_{h_l}^2$, which does not affect the following demonstration.

If $\hat{N}\neq N$ or $\hat{N}_{\mathrm{cp}}\neq N_{\mathrm{cp}}$, then there are two possible cases:

Case 1: If $\hat{N}+\hat{N}_{\mathrm{cp}}=N+N_{\mathrm{cp}}$, the length of the hypothetical OFDM symbol equals the length of the real received one. Due to $0<\hat{N}_{\mathrm{cp}}\le\hat{N}$, the difference between $\hat{N}_{\mathrm{cp}}$ and N_{cp} is $c=\hat{N}_{\mathrm{cp}}-N_{\mathrm{cp}}$, where $-N_{\mathrm{cp}}<c\le(N-N_{\mathrm{cp}})/2$ and $c\neq 0$. That is, $\hat{N}=N-c$.

If $c\le N_{\mathrm{cp}}$, the expectation of the cost function in Eqs. (1) and (2) can be expressed as

$$
\begin{aligned}
&E\Big[\max_{i\in[1,N+N_{\mathrm{cp}}]}\frac{1}{M_t}\\
&\quad\cdot\sum_{k=1}^{M_t} y_{i+(k-1)(N+N_{\mathrm{cp}})}y_{i+\hat{N}+(k-1)(N+N_{\mathrm{cp}})}^*\Big]\\
&=E\Big[\Big(\sum_{l=0}^{N_{\mathrm{cp}}-1} h_l s_{N_{\mathrm{cp}}-l}(k)+w_{N_{\mathrm{cp}}}(k)\Big)\\
&\quad\cdot\Big(\sum_{l=0}^{N_{\mathrm{cp}}-1} h_l s_{N-c+N_{\mathrm{cp}}-l}(k)+w_{N-c+N_{\mathrm{cp}}}(k)\Big)^*\Big]\\
&=P_s\sum_{l=0}^{N_{\mathrm{cp}}-|c|} h_l h_{l+|c|}^*, \qquad (4)
\end{aligned}
$$

where the position with the largest statistical auto-correlation value is $i=N_{\mathrm{cp}}$.

Hence, it is easy to prove that

$$
\begin{aligned}
&\sum_{l=0}^{N_{\mathrm{cp}}-1}\sigma_{h_l}^2\ge\frac{1}{2}\Big(\sum_{l=0}^{N_{\mathrm{cp}}-1}\sigma_{h_l}^2+\sum_{l=1}^{N_{\mathrm{cp}}}\sigma_{h_l}^2\Big)>\sum_{l=0}^{N_{\mathrm{cp}}-1} h_l h_{l+1}^*,\\
&\sum_{l=0}^{N_{\mathrm{cp}}-1}\sigma_{h_l}^2\ge\frac{1}{2}\Big(\sum_{l=0}^{N_{\mathrm{cp}}-1}\sigma_{h_l}^2+\sum_{l=1}^{N_{\mathrm{cp}}}\sigma_{h_l}^2\Big)>\sum_{l=0}^{N_{\mathrm{cp}}-2} h_l h_{l+2}^*,\\
&\quad\vdots\\
&\sum_{l=0}^{N_{\mathrm{cp}}-1}\sigma_{h_l}^2\ge\frac{1}{2}\Big(\sum_{l=0}^{N_{\mathrm{cp}}-1}\sigma_{h_l}^2+\sum_{l=1}^{N_{\mathrm{cp}}}\sigma_{h_l}^2\Big)>h_0 h_{N_{\mathrm{cp}}}^*. \qquad (5)
\end{aligned}
$$

If $c>N_{\mathrm{cp}}$, then $\hat{N}<N-N_{\mathrm{cp}}$. Due to the auto-correlation characteristic of the transmitted data, the expectation of the cost function in Eqs. (1) and (2) is zero, which is definitely smaller than the value computed in Eq. (3).

Hence, in case 1, the expectation of the cost function in Eqs. (1) and (2) can be maximized if and only if $\hat{N}=N$ and $\hat{N}_{\mathrm{cp}}=N_{\mathrm{cp}}$.

Case 2: If $\hat{N}+\hat{N}_{\mathrm{cp}}\neq N+N_{\mathrm{cp}}$, then the length of the hypothetical OFDM symbol does not equal the length of the real received one.

If $\hat{N}\neq N$, then for an arbitrary hypothetical OFDM symbol k, $\forall k\in\mathbb{Z}_+$, we have

$$
\begin{aligned}
&E\Big[\max_{i\in[1,\hat{N}+\hat{N}_{\mathrm{cp}}]} y_{i+(k-1)(\hat{N}+\hat{N}_{\mathrm{cp}})}y_{i+\hat{N}+(k-1)(\hat{N}+\hat{N}_{\mathrm{cp}})}^*\Big]\\
&\le P_s\max\Big\{\sum_{l=0}^{N_{\mathrm{cp}}-1} h_l h_{l+1}^*,\ \sum_{l=0}^{N_{\mathrm{cp}}-2} h_l h_{l+2}^*,\ldots,h_0 h_{N_{\mathrm{cp}}}^*\Big\}\\
&<P_s\sum_{l=0}^{N_{\mathrm{cp}}-1}\sigma_{h_l}^2. \qquad (6)
\end{aligned}
$$

Otherwise, if $\hat{N}=N$, then for an arbitrary hypothetical OFDM symbol k, $\forall k\in\mathbb{Z}_+$, we have

$$
\begin{aligned}
&E\Big[\max_{i\in[1,\hat{N}+\hat{N}_{\mathrm{cp}}]} y_{i+(k-1)(\hat{N}+\hat{N}_{\mathrm{cp}})}y_{i+N+(k-1)(\hat{N}+\hat{N}_{\mathrm{cp}})}^*\Big]\\
&\le P_s\max\Big\{\sum_{l=0}^{N_{\mathrm{cp}}-1}\sigma_{h_l}^2,\ \sum_{l=0}^{N_{\mathrm{cp}}-1} h_l h_{l+1}^*,\ \sum_{l=0}^{N_{\mathrm{cp}}-2} h_l h_{l+2}^*,\\
&\qquad\ldots,h_0 h_{N_{\mathrm{cp}}}^*\Big\}=P_s\sum_{l=0}^{N_{\mathrm{cp}}-1}\sigma_{h_l}^2. \qquad (7)
\end{aligned}
$$

Because $\hat{N}+\hat{N}_{\mathrm{cp}}\neq N+N_{\mathrm{cp}}$ and $\hat{N}\ge\hat{N}_{\mathrm{cp}}$, it is impossible that the expectations of the kth and $(k+1)$th hypothetical OFDM symbols computed in Eq. (7) equal $P_s\sum_{l=0}^{N_{\mathrm{cp}}-1}\sigma_{h_l}^2$ simultaneously.

Hence, in case 2, the expectation of the cost function in Eqs. (1) and (2) is smaller than that computed in Eq. (3). Therefore, the expectation of

the cost function in Eqs. (1) and (2) is maximized if and only if $\hat{N}=N$ and $\hat{N}_{\mathrm{cp}}=N_{\mathrm{cp}}$.

From Lemma 1, one finds that if M_t is large enough, then the structure of an OFDM symbol can be correctly estimated by Eqs. (1) and (2) without prior knowledge about the structure and content of the PU signal.

3.1.2 Subspace-based blind channel estimation

At the SU, the received OFDM symbols are repeatedly used to create a received symbol matrix and a transmitted symbol matrix as $\boldsymbol{Y}(k)=[\bar{\boldsymbol{y}}_{0,Q-1}(k),\bar{\boldsymbol{y}}_{1,Q-2}(k),\dots,\bar{\boldsymbol{y}}_{Q-1,0}(k)]$ and $\boldsymbol{S}(k)=[\bar{\boldsymbol{s}}_{0,Q-1}(k),\bar{\boldsymbol{s}}_{1,Q-2}(k),\dots,\bar{\boldsymbol{s}}_{Q-1,0}(k)]$, where

$$\bar{\boldsymbol{y}}_{a,b}(k)=\begin{bmatrix}[\boldsymbol{y}_N(k-1)]_N^{1-a}\\ [\boldsymbol{y}_N(k)]_{N+b}^{1-N_{\mathrm{cp}}}\end{bmatrix},$$

$$\bar{\boldsymbol{s}}_{a,b}(k)=\begin{bmatrix}[\boldsymbol{s}_N(k-1)]_N^{1-a}\\ [\boldsymbol{s}_N(k)]_{N-N_{\mathrm{cp}}+b}^{1-N_{\mathrm{cp}}}\end{bmatrix},$$

and Q, the repetition index, is the number of times that the first received OFDM symbol is repeatedly used.

The relationship between the received symbol matrix and the transmitted symbol matrix can be presented as

$$\boldsymbol{Y}(k)=\boldsymbol{H}\boldsymbol{S}(k), \tag{8}$$

where

$$\boldsymbol{H}=\begin{bmatrix}\boldsymbol{H}_A & & \boldsymbol{0}_{N\times(N+Q-1)}\\ \boldsymbol{0}_{(N_{\mathrm{cp}}+Q-1)\times(N-N_{\mathrm{cp}})} & \boldsymbol{H}_B & \boldsymbol{0}_{(N_{\mathrm{cp}}+Q-1)\times(N-N_{\mathrm{cp}})}\\ \boldsymbol{0}_{N\times(N+Q-1)} & & \boldsymbol{H}_C\end{bmatrix}$$

is the transmission matrix, in which $\boldsymbol{H}_A$, $\boldsymbol{H}_B$, and $\boldsymbol{H}_C$ are Toeplitz matrices. The first column and the first row of $\boldsymbol{H}_A$ are $[h_0,h_1,\dots,h_{N_{\mathrm{cp}}},\boldsymbol{0}_{1\times(N-N_{\mathrm{cp}}-1)}]^{\mathrm{T}}$ and $[h_0,\boldsymbol{0}_{1\times(N-N_{\mathrm{cp}}-1)},h_{N_{\mathrm{cp}}},h_{N_{\mathrm{cp}}-1},\dots,h_1]$, respectively. The first column and the first row of $\boldsymbol{H}_B$ are $[h_{N_{\mathrm{cp}}},\boldsymbol{0}_{1\times(N_{\mathrm{cp}}+Q-2)}]^{\mathrm{T}}$ and $[h_{N_{\mathrm{cp}}},h_{N_{\mathrm{cp}}-1},\dots,h_0,\boldsymbol{0}_{1\times(N_{\mathrm{cp}}+Q-2)}]$, respectively. The first column and first row of $\boldsymbol{H}_C$ are $[h_{N_{\mathrm{cp}}},\boldsymbol{0}_{1\times(N-N_{\mathrm{cp}}-1)},h_0,h_1,\dots,h_{N_{\mathrm{cp}}-1}]^{\mathrm{T}}$ and $[h_{N_{\mathrm{cp}}},h_{N_{\mathrm{cp}}-1},\dots,h_0,\boldsymbol{0}_{1\times(N-N_{\mathrm{cp}}-1)}]$, respectively.

Muquet *et al.* (2002) and Su and Vaidyanathan (2007) proved that if the number of received OFDM symbols used for blind channel estimation, M_{h}, satisfies $M_{\mathrm{h}}\geq\dfrac{2N-1}{Q}+2$, then the normalized CIR between the SU and the signal source (PU or PUE) can be effectively estimated by the SU. The channel estimation procedure is summarized as follows:

Step 1: The auto-correlation matrix $\boldsymbol{R}_{\boldsymbol{YY}}$ is calculated as $\boldsymbol{R}_{\boldsymbol{YY}}=\dfrac{1}{M_{\mathrm{h}}-1}\sum_{k=2}^{M_{\mathrm{h}}}\boldsymbol{Y}(k)\boldsymbol{Y}^{\mathrm{H}}(k)$.

Step 2: The eigenvalue decomposition is performed on $\boldsymbol{R}_{\boldsymbol{YY}}$ to obtain the noise subspace of the received signal, which is spanned by a basis set of N_{cp} eigenvectors associated with N_{cp} smallest eigenvalues of $\boldsymbol{R}_{\boldsymbol{YY}}$, i.e., $\boldsymbol{g}_1,\boldsymbol{g}_2,\dots,\boldsymbol{g}_{N_{\mathrm{cp}}}$.

Step 3: Using $\boldsymbol{g}_1,\boldsymbol{g}_2,\dots,\boldsymbol{g}_{N_{\mathrm{cp}}}$, N_{cp} matrices are constructed as $\boldsymbol{B}_i=\mathrm{Hankel}(\boldsymbol{b}_{i,1},\boldsymbol{b}_{i,2}^{\mathrm{T}})$, $1\leq i\leq N_{\mathrm{cp}}$, where $\boldsymbol{b}_{i,1}=[\boldsymbol{0}_{1\times N_{\mathrm{cp}}},g_i(1)]^{\mathrm{T}}$ and $\boldsymbol{b}_{i,2}^{\mathrm{T}}=[\boldsymbol{g}_i^{\mathrm{T}},\boldsymbol{0}_{1\times N_{\mathrm{cp}}}]$ denote the first column and the last row of the $(N_{\mathrm{cp}}+1)\times(2N+2N_{\mathrm{cp}}+Q-1)$ Hankel matrix $\boldsymbol{B}_i$, respectively, and $g_i(1)$ denotes the first element of $\boldsymbol{g}_i$.

Step 4: Matrix $\boldsymbol{A}$ is defined as $\boldsymbol{A}=\left[\boldsymbol{A}_1^{\mathrm{T}},\boldsymbol{I}_{2N+Q-1},\boldsymbol{A}_2^{\mathrm{T}}\right]^{\mathrm{T}}$, where $\boldsymbol{A}_1=[\boldsymbol{0}_{N_{\mathrm{cp}}\times(N-N_{\mathrm{cp}})},\boldsymbol{I}_{N_{\mathrm{cp}}},\boldsymbol{0}_{N_{\mathrm{cp}}\times(N+Q-1)}]$ and $\boldsymbol{A}_2=[\boldsymbol{0}_{N_{\mathrm{cp}}\times(N+Q-1)},\boldsymbol{I}_{N_{\mathrm{cp}}},\boldsymbol{0}_{N_{\mathrm{cp}}\times(N-N_{\mathrm{cp}})}]$. Hence, N_{cp} matrices $\boldsymbol{G}_i$ with size $(N_{\mathrm{cp}}+1)\times(2N+Q-1)$, $1\leq i\leq N_{\mathrm{cp}}$, can be constructed as $\boldsymbol{G}_i=\boldsymbol{B}_i\boldsymbol{A}$.

Step 5: The estimation of the normalized CIR between the SU and the signal source (PU or PUE) can be uniquely obtained by solving the quadratic optimization problem as

$$\begin{aligned}\hat{\boldsymbol{h}}=\arg\min_{\boldsymbol{h}}\ &\boldsymbol{h}^{\mathrm{H}}\left(\textstyle\sum_{i=1}^{N_{\mathrm{cp}}}\boldsymbol{G}_i\boldsymbol{G}_i^{\mathrm{H}}\right)\boldsymbol{h}\\ \text{s.t.}\ \ &\|\boldsymbol{h}\|_2=1,\ h_0^*=h_0,\end{aligned} \tag{9}$$

where $\|\cdot\|_2$ denotes the 2-norm of a vector. If the constraint conditions are omitted, the problem formulated in Eq. (9) can be resolved and obtains only the CIR up to a complex scalar factor. Since the estimate of the CIR is used for PUEA detection, the SU has to extract a unique CIR characteristic from the received signal to verify whether the received signal is from the PU. Therefore, we add two constraints in the formulated problem. The problem formulated in Eq. (9) can be solved by calculating the eigenvector associated with the smallest eigenvalue of $\sum_{i=1}^{N_{\mathrm{cp}}}\boldsymbol{G}_i\boldsymbol{G}_i^{\mathrm{H}}$ with unit-norm and the phase of the 0th channel-tap coefficient being zero.

3.2 Proposed PUEA detection method using CIR

In this subsection, using the modified blind channel estimation method in Section 3.1, a binary

hypothesis test is constructed to infer that the received signal at the SU is transmitted by the PU or PUE.

3.2.1 Proposed method

It is assumed that PUEA is not launched in the initialization phase of the CRN, and that the signals received by the SU are transmitted by the PU. This assumption is justified because in the initialization phase, the CRN has not yet started; therefore, the PUE cannot transmit data through the CRN. In other words, launching PUEA is just a waste of energy for the PUE. Moreover, if the PUE does not care whether the CRN is started and launches PUEA continuously on a spectrum band, the CRN should choose another underutilized spectrum band.

During the initialization phase, the SU receives the PU signal and performs blind channel estimation. The expectation and covariance matrix of the estimate of normalized CIR are expressed as

$$\hat{\boldsymbol{\mu}}_{\mathrm{p}} = \frac{1}{M_{\mathrm{s}}} \sum_{i=1}^{M_{\mathrm{s}}} \hat{\boldsymbol{h}}_{\mathrm{p},i} \tag{10}$$

and

$$\hat{\boldsymbol{C}}_{\mathrm{p}} = \frac{1}{M_{\mathrm{s}}-1} \sum_{i=1}^{M_{\mathrm{s}}} (\hat{\boldsymbol{h}}_{\mathrm{p},i} - \hat{\boldsymbol{\mu}}_{\mathrm{p}})(\hat{\boldsymbol{h}}_{\mathrm{p},i} - \hat{\boldsymbol{\mu}}_{\mathrm{p}})^{\mathrm{H}}, \tag{11}$$

where M_{s} is the number of times that the SU performs the subspace-based blind channel estimation of the CIR between the PU and the SU, and $\hat{\boldsymbol{h}}_{\mathrm{p},i}$ denotes the ith estimation result. The procedures in Eqs. (10) and (11) are also known as system training.

Owing to the complex AWGN at the SU, each result of the blind channel estimation follows the multivariate complex normal distribution as $\hat{\boldsymbol{h}}_{\mathrm{p},i} \sim \mathcal{CN}(\boldsymbol{\mu}_{\mathrm{p}}, \boldsymbol{C}_{\mathrm{p}})$. Therefore, according to Kay (1993), $\hat{\boldsymbol{\mu}}_{\mathrm{p}}$ and $\hat{\boldsymbol{C}}_{\mathrm{p}}$ in Eqs. (10) and (11) are the unbiased estimates of $\boldsymbol{\mu}_{\mathrm{p}} = E\left[\hat{\boldsymbol{h}}_{\mathrm{p},i}\right]$ and $\boldsymbol{C}_{\mathrm{p}} = E\left[(\hat{\boldsymbol{h}}_{\mathrm{p},i} - \boldsymbol{\mu}_{\mathrm{p}})(\hat{\boldsymbol{h}}_{\mathrm{p},i} - \boldsymbol{\mu}_{\mathrm{p}})^{\mathrm{H}}\right]$, respectively.

After the initialization phase, when the SU receives an unknown signal, the subspace-based blind channel estimation method is performed on the received signal to estimate the CIR as $\boldsymbol{h}_{\mathrm{T}}$.

A binary hypothesis test is constructed to determine whether the source of the unknown signal is the PU or PUE. The binary hypothesis test statistic is defined as

$$T = (\boldsymbol{h}_{\mathrm{T}} - \hat{\boldsymbol{\mu}}_{\mathrm{p}})^{\mathrm{H}} \hat{\boldsymbol{C}}_{\mathrm{p}}^{-1} (\boldsymbol{h}_{\mathrm{T}} - \hat{\boldsymbol{\mu}}_{\mathrm{p}}). \tag{12}$$

The binary hypothesis test is

$$T \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} \lambda, \tag{13}$$

where λ is the pre-defined decision threshold, $\mathcal{H}_0$ and $\mathcal{H}_1$ denote the hypotheses that the received signal is transmitted by the PU and PUE, respectively.

Fig. 1 illustrates the flowchart of the proposed PUEA detection method.

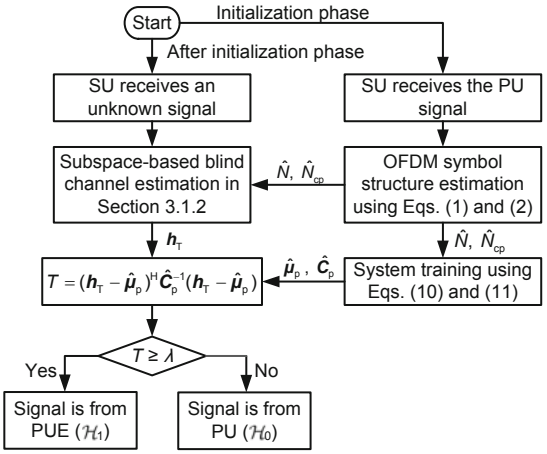

Fig. 1 Flowchart of the proposed PUEA detection method

3.2.2 Performance analysis

Since the estimate of the CIR between the PU and SU, $\hat{\boldsymbol{h}}_{\mathrm{p}}$, follows the multivariate complex normal distribution as $\hat{\boldsymbol{h}}_{\mathrm{p},i} \sim \mathcal{CN}(\boldsymbol{\mu}_{\mathrm{p}}, \boldsymbol{C}_{\mathrm{p}})$, T in Eq. (12) asymptotically follows the central chi-square distribution with $2(N_{\mathrm{cp}}+1)$ degrees of freedom if the received signal is from the PU. That is,

$$T \,|\, \mathcal{H}_0 = (\hat{\boldsymbol{h}}_{\mathrm{p}} - \hat{\boldsymbol{\mu}}_{\mathrm{p}})^{\mathrm{H}} \hat{\boldsymbol{C}}_{\mathrm{p}}^{-1} (\hat{\boldsymbol{h}}_{\mathrm{p}} - \hat{\boldsymbol{\mu}}_{\mathrm{p}}) \sim \chi^2_{2(N_{\mathrm{cp}}+1)}. \tag{14}$$

The cumulative distribution function (CDF) of the central chi-square distribution with $2(N_{\mathrm{cp}}+1)$ degrees of freedom is

$$F_{\chi^2_{2(N_{\mathrm{cp}}+1)}}(x) = \int_0^x \frac{t^{N_{\mathrm{cp}}} \exp(-t/2)}{2^{N_{\mathrm{cp}}+1}\Gamma(N_{\mathrm{cp}}+1)} \mathrm{d}t,\ x > 0.$$

Hence, the false-alarm probability, P_{fa}, can be defined and calculated with Eqs. (13) and (14). That is,

$$P_{\mathrm{fa}} \triangleq \Pr(T > \lambda \,|\, \mathcal{H}_0) = 1 - F_{\chi^2_{2(N_{\mathrm{cp}}+1)}}(\lambda). \tag{15}$$

On the other hand, if the source of the received signal is the PUE, T can be expressed as

$$T \,|\, \mathcal{H}_1 = (\hat{\boldsymbol{h}}_{\mathrm{m}} - \hat{\boldsymbol{\mu}}_{\mathrm{p}})^{\mathrm{H}} \hat{\boldsymbol{C}}_{\mathrm{p}}^{-1} (\hat{\boldsymbol{h}}_{\mathrm{m}} - \hat{\boldsymbol{\mu}}_{\mathrm{p}}), \tag{16}$$

where $\hat{\boldsymbol{h}}_{\mathrm{m}}$ is the estimate of the CIR between the PUE and SU. Similarly, $\hat{\boldsymbol{h}}_{\mathrm{m}}$ follows the multivariable complex normal distribution as $\hat{\boldsymbol{h}}_{\mathrm{m}} \sim \mathcal{CN}(\boldsymbol{\mu}_{\mathrm{m}}, \boldsymbol{C}_{\mathrm{m}})$, and $(\hat{\boldsymbol{h}}_{\mathrm{m}} - \boldsymbol{\mu}_{\mathrm{m}})^{\mathrm{H}} \boldsymbol{C}_{\mathrm{m}}^{-1} (\hat{\boldsymbol{h}}_{\mathrm{m}} - \boldsymbol{\mu}_{\mathrm{m}}) \sim \chi^2_{2(N_{\mathrm{cp}}+1)}$.

For simplicity, it is assumed that $\boldsymbol{C}_{\mathrm{p}} \approx \boldsymbol{C}_{\mathrm{m}} \approx \boldsymbol{C}$ at a high signal-to-noise ratio (SNR). Furthermore, M_{s} in Eqs. (10) and (11) should be large enough in order that the SU estimates the expectation and covariance matrix of the estimation of the normalized CIR accurately, i.e., $\hat{\boldsymbol{\mu}}_{\mathrm{p}} \approx \boldsymbol{\mu}_{\mathrm{p}}$ and $\hat{\boldsymbol{C}}_{\mathrm{p}} \approx \boldsymbol{C}_{\mathrm{p}} \approx \boldsymbol{C}$.

Using the assumptions mentioned above, the detection probability of the proposed PUEA detection method, P_{d}, can be approximated with Eqs. (13) and (16). That is,

$$\begin{aligned} P_{\mathrm{d}} &\triangleq \Pr(T \geq \lambda \,|\, \mathcal{H}_1) \\ &\approx \Pr\big[(\hat{\boldsymbol{h}}_{\mathrm{m}} - \boldsymbol{\mu}_{\mathrm{p}})^{\mathrm{H}} \boldsymbol{C}^{-1} (\hat{\boldsymbol{h}}_{\mathrm{m}} - \boldsymbol{\mu}_{\mathrm{p}}) \geq \lambda\big] \\ &= \Pr\big[(\hat{\boldsymbol{h}}_{\mathrm{m}} - \boldsymbol{\mu}_{\mathrm{m}} + \boldsymbol{\mu}_{\mathrm{m}} - \boldsymbol{\mu}_{\mathrm{p}})^{\mathrm{H}} \boldsymbol{C}^{-1} \\ &\qquad \cdot (\hat{\boldsymbol{h}}_{\mathrm{m}} - \boldsymbol{\mu}_{\mathrm{m}} + \boldsymbol{\mu}_{\mathrm{m}} - \boldsymbol{\mu}_{\mathrm{p}}) \geq \lambda\big] \\ &= \Pr\big[(\boldsymbol{e}_{\mathrm{m}} + \boldsymbol{\Delta})^{\mathrm{H}} \boldsymbol{C}^{-1} (\boldsymbol{e}_{\mathrm{m}} + \boldsymbol{\Delta}) \geq \lambda\big] \\ &= \Pr\big[\boldsymbol{e}_{\mathrm{m}}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{e}_{\mathrm{m}} + 2\mathrm{Re}(\boldsymbol{\Delta}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{e}_{\mathrm{m}}) \\ &\qquad + \boldsymbol{\Delta}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{\Delta} \geq \lambda\big], \end{aligned} \tag{17}$$

where $\boldsymbol{e}_{\mathrm{m}} = \hat{\boldsymbol{h}}_{\mathrm{m}} - \boldsymbol{\mu}_{\mathrm{m}}$ denotes the estimation error of the CIR between the PUE and SU, and it follows the multivariate complex normal distribution as $\boldsymbol{e}_{\mathrm{m}} \sim \mathcal{CN}(\boldsymbol{0}_{(N_{\mathrm{cp}}+1)\times 1}, \boldsymbol{C})$ because $\hat{\boldsymbol{h}}_{\mathrm{m}} \sim \mathcal{CN}(\boldsymbol{\mu}_{\mathrm{m}}, \boldsymbol{C})$, $\boldsymbol{\Delta} = \boldsymbol{\mu}_{\mathrm{m}} - \boldsymbol{\mu}_{\mathrm{p}}$ denotes the CIR difference between the PU-SU and PUE-SU channels, and $\mathrm{Re}(\cdot)$ denotes the real part of a complex number.

In the wireless environment, it is reasonable to assume that the difference between $\boldsymbol{\mu}_{\mathrm{m}}$ and $\boldsymbol{\mu}_{\mathrm{p}}$ is much larger than the CIR estimation error. Hence, two conditions, $\Pr(|\boldsymbol{\Delta}| \gg |\boldsymbol{e}_{\mathrm{m}}|) \approx 1$ and $\mathrm{Re}\left[(2\boldsymbol{\Delta} + \boldsymbol{e}_{\mathrm{m}})^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{e}_{\mathrm{m}}\right] \approx 2\mathrm{Re}\left(\boldsymbol{\Delta}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{e}_{\mathrm{m}}\right)$, are assumed to be satisfied. With these two assumptions, the detection probability in Eq. (17) can be approximatively expressed as

$$\begin{aligned} P_{\mathrm{d}} &\approx \Pr\big[2\mathrm{Re}(\boldsymbol{\Delta}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{e}_{\mathrm{m}}) + \boldsymbol{\Delta}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{\Delta} \geq \lambda\big] \\ &= \Pr\left[\mathrm{Re}(\boldsymbol{\Delta}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{e}_{\mathrm{m}}) \geq \frac{\lambda - \boldsymbol{\Delta}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{\Delta}}{2}\right]. \end{aligned} \tag{18}$$

According to Wooding (1956) and Rao (1973), if an $n \times 1$ stochastic vector $\boldsymbol{z}$ follows the multivariate complex normal distribution as $\boldsymbol{z} \sim \mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{P})$, $\mathrm{Re}(\boldsymbol{k}^{\mathrm{H}} \boldsymbol{z})$ follows the univariate real normal distribution as $\mathrm{Re}(\boldsymbol{k}^{\mathrm{H}} \boldsymbol{z}) \sim \mathcal{N}\left(\mathrm{Re}(\boldsymbol{k}^{\mathrm{H}} \boldsymbol{\mu}), \frac{1}{2} \boldsymbol{k}^{\mathrm{H}} \boldsymbol{P} \boldsymbol{k}\right)$ for any given $n \times 1$ complex vector $\boldsymbol{k}$. Since $\boldsymbol{e}_{\mathrm{m}} \sim \mathcal{CN}(\boldsymbol{0}_{(N_{\mathrm{cp}}+1)\times 1}, \boldsymbol{C})$, $\mathrm{Re}(\boldsymbol{\Delta}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{e}_{\mathrm{m}})$ follows the univariate real normal distribution, i.e., $\mathrm{Re}(\boldsymbol{\Delta}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{e}_{\mathrm{m}}) \sim \mathcal{N}\left(0, \frac{\boldsymbol{\Delta}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{\Delta}}{2}\right)$. Thus, the PUEA detection probability in Eq. (18) can be approximated as

$$P_{\mathrm{d}} \approx Q\left(\frac{\lambda - \boldsymbol{\Delta}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{\Delta}}{\sqrt{2 \boldsymbol{\Delta}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{\Delta}}}\right), \tag{19}$$

where $Q(x)$ is the complementary cumulative distribution function of the standard normal distribution, i.e., $Q(x) = \int_x^{\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{1}{2} t^2\right) \mathrm{d}t$.

Using a Neyman-Pearson framework, the decision threshold λ can be calculated to satisfy the required false-alarm probablity of the proposed PUEA detection method, $\bar{P}_{\mathrm{fa}}$, according to Eq. (15):

$$\lambda = F^{-1}_{\chi^2_{2(N_{\mathrm{cp}}+1)}}(1 - \bar{P}_{\mathrm{fa}}). \tag{20}$$

According to Eqs. (19) and (20), given the required false-alarm probability ($\bar{P}_{\mathrm{fa}}$), the PUEA detection probability can be calculated as

$$P_{\mathrm{d}} \approx Q\left(\frac{F^{-1}_{\chi^2_{2(N_{\mathrm{cp}}+1)}}(1 - \bar{P}_{\mathrm{fa}}) - \boldsymbol{\Delta}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{\Delta}}{\sqrt{2 \boldsymbol{\Delta}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{\Delta}}}\right). \tag{21}$$

From Eq. (21), one finds that the PUEA detection probability monotonically increases as $\bar{P}_{\mathrm{fa}}$ or $\left(\boldsymbol{\Delta}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{\Delta}\right)$ increases. Thus, $\left(\boldsymbol{\Delta}^{\mathrm{H}} \boldsymbol{C}^{-1} \boldsymbol{\Delta}\right)$ increases as $|\boldsymbol{\Delta}|$ increases or the accuracy of blind channel estimation is improved.

4 Simulation results and discussion

In this section, the performances of the proposed modified subspace-based blind channel estimation method and the PUEA detection method using the CIR are evaluated by Monte-Carlo simulations. The CRN operates in a DTMB system. The central frequency of the PU signal is set to be 503.25 MHz, and the signal bandwidth is 7.56 MHz. The structure of an OFDM symbol is set as $N = 64$ and $N_{\mathrm{cp}} = 16$. Each subcarrier is modulated with 16-QAM (quadrature amplitude modulation). The

sample period is 0.132 275 μs and the OFDM symbol length is 10.582 01 μs. M_s is set as 40. The multi-path CIRs of the PU-SU and PUE-SU channels are modeled in Table 1. According to Table 1, one finds that only the phases of the first six channel-tap coefficients are different.

In the simulations, the SU first receives the PU signal in the initialization phase and performs OFDM symbol structure estimation. The numerical results in Fig. 2 show that if the value of M_t is large enough, for example, $M_t \geq 30$, then the SU can obtain the accurate estimation of the OFDM symbol structure as $\hat{N} = 64$ and $\hat{N}_{cp} = 16$. In the following simulations, M_t is set as 35.

When the OFDM symbol structure estimation procedure is finished, the SU performs system training to obtain $\hat{\boldsymbol{\mu}}_p$ and $\hat{\boldsymbol{C}}_p$. After the initialization phase, when the SU receives an unknown signal, the binary hypothesis test (Eq. (13)) is constructed to determine whether the source of the unknown signal is PU or PUE.

In the following simulations, we first evaluate the performance of the modified blind channel estimation method in terms of the CIR estimation error. Then the performance of the proposed PUEA detection method is evaluated in terms of the receiver operating characteristic (ROC) curve. All the simulation results are averaged over 5000 realizations.

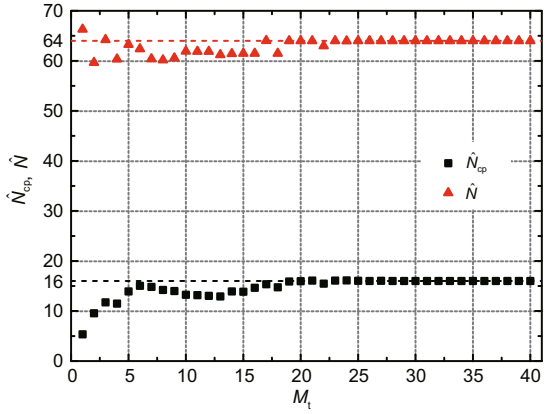

Fig. 2 $\hat{N}$ and $\hat{N}_{cp}$ versus M_t

4.1 Performance of the blind channel estimation method

Here, the CIR estimation error, defined as $\|\hat{\boldsymbol{h}}_p - \boldsymbol{\mu}_p\|_2^2$, is regarded as the performance of the blind channel estimation method. Moreover, the received SNR is defined as $P_s\|\boldsymbol{h}\|_2^2/\sigma_w^2$.

Fig. 3 shows the impact of the received SNR on the CIR estimation error of the modified blind channel estimation method, where $Q = 12$ and $M_h = 40$. From Fig. 3, one finds that the CIR estimation error reduces significantly as the received SNR increases, which means that the modified blind channel estimation method is sensitive to the received SNR. The reason for this phenomenon is that the modified blind channel estimation method uses the noise subspace of the received signal. The eigenvalues of the autocorrelation matrix $\boldsymbol{R}_{\boldsymbol{YY}}$ would be close to each other when the received SNR is low, which could make the SU choose the false eigenvectors as the basis set of the noise subspace, and results in an inaccurate estimate of the CIR.

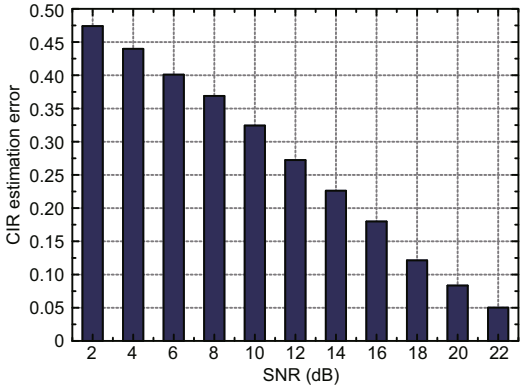

Fig. 3 Impact of the received SNR on the CIR estimation error ($Q = 12$, M_h=40)

Table 1 Multi-path propagation channel model

Delay	Channel-tap coefficient		Delay	Channel-tap coefficient		Delay	Channel-tap coefficient	
(μs)	PU-SU	PUE-SU	(μs)	PU-SU	PUE-SU	(μs)	PU-SU	PUE-SU
0	0.910+0.220i	0.830−0.433i	6	0.460+0.100i	0.460+0.100i	12	0.270+0.090i	0.270+0.090i
1	0.840−0.150i	0.368+0.770i	7	0.440−0.150i	0.440−0.150i	13	0.210−0.050i	0.210−0.050i
2	0.790−0.370i	0.850−0.196i	8	0.380+0.070i	0.380+0.070i	14	0.180+0.067i	0.180+0.067i
3	0.660+0.250i	0.320+0.629i	9	0.350−0.140i	0.350−0.140i	15	0.110+0.023i	0.110+0.023i
4	0.580−0.150i	0.384−0.460i	10	0.330−0.130i	0.330−0.130i	16	0.007−0.008i	0.007−0.008i
5	0.550+0.200i	0.290+0.508i	11	0.300+0.080i	0.300+0.080i			

Fig. 4 shows the impact of M_{h} on the CIR estimation error, where SNR = 18 dB and Q=12. From Fig. 4, one finds that the CIR estimation error decreases as M_{h} increases, especially for a small value of M_{h}. This is because the auto-correlation matrix $\boldsymbol{R_{YY}}$ constructed by the SU is closer to the real auto-correlation matrix of the received signal when more received OFDM symbols are used for channel estimation, which leads to a more accurate estimate of the CIR. Moreover, from Fig. 4, one finds that when M_{h} is large enough, the descending rate of the CIR estimation error becomes negligible.

Fig. 5 shows the impact of Q on the CIR estimation error, where SNR = 18 dB and M_{h}=40. From Fig. 5, one finds that the CIR estimation error reduces as Q increases. The reason for this phenomenon is that when a larger value of Q is set, the auto-correlation matrix $\boldsymbol{R_{YY}}$ constructed by the SU has a higher probability of being full rank, and is closer to the real auto-correlation matrix of the received signal.

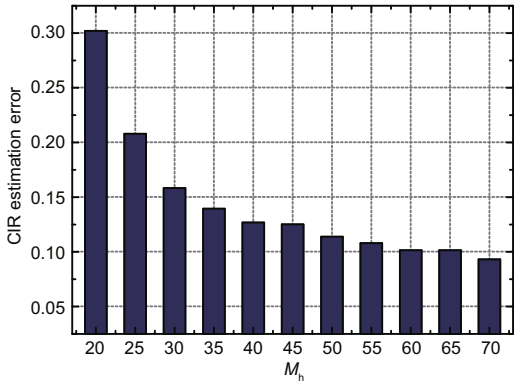

Fig. 4 Impact of M_{h} on the CIR estimation error (SNR=18 dB, Q=12)

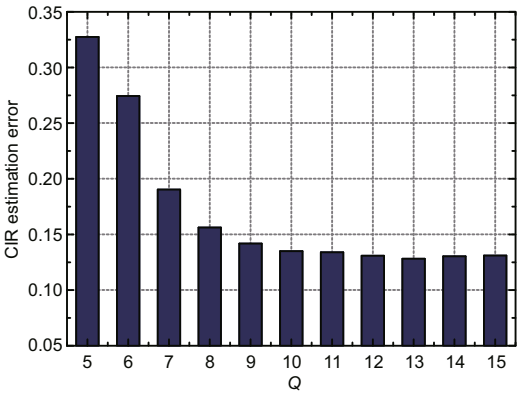

Fig. 5 Impact of Q on the CIR estimation error (SNR=18 dB, M_{h}=40)

4.2 Performance of the proposed PUEA detection method

Fig. 6 shows the ROC curves of the proposed PUEA detection method with different received SNR, where M_{h}=30 and Q=10. From Fig. 6, one finds that as the received SNR increases, the detection performance of the proposed PUEA detection method increases significantly. The reason for this phenomenon is revealed in the results in Fig. 3; that is, the accuracy of the channel estimation improves as the received SNR increases. Hence, the proposed PUEA detection method performs well even though only six channel-tap coefficients between PU-SU and PUE-SU channels are different.

Fig. 7 shows the ROC curves of the proposed PUEA detection method with different M_{h} values, where SNR=5 dB and Q=10. From Fig. 7, one finds that as M_{h} increases, the detection performance of the proposed PUEA detection method improves significantly, which is consistent with the results shown

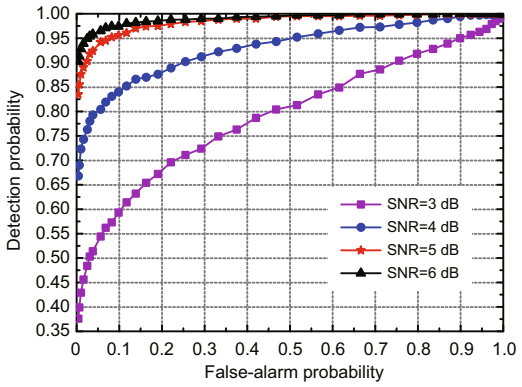

Fig. 6 Detection performance under different SNR (M_{h}=30, Q=10)

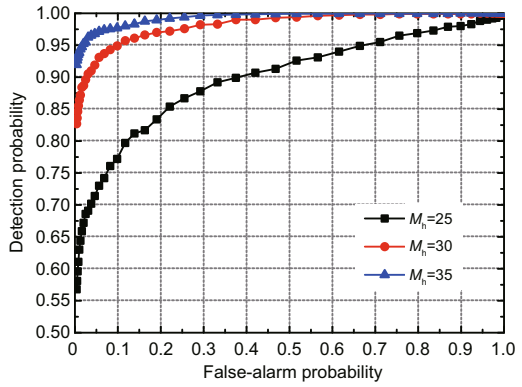

Fig. 7 Detection performance under different M_{h} (SNR=5 dB, Q=10)

in Fig. 4. However, the value of M_{h} should be chosen appropriately because a larger M_{h} will cause a longer time for channel estimation, which makes the SU difficult in adapting the fast-variant wireless channel.

Fig. 8 shows the ROC curves of the proposed PUEA detection method with different Q values, where SNR=5 dB and M_{h}=30. From Fig. 8, one finds that the detection performance of the proposed method improves significantly as Q increases, which is consistent with the results shown in Fig. 5. However, the larger Q means higher computational complexity and larger memory requirements for channel estimation.

Fig. 9 shows the comparison of the detection performance between the proposed PUEA detection method and the PUEA detection method proposed by Chin *et al.* (2014), where Q=10 and M_{h}=30. From Fig. 9, one finds that the performance of the proposed PUEA detection method is much better than that of the PUEA detection method that uses the channel-tap power. The reason for this phenomenon is that in the proposed PUEA detection method, both the amplitude and the phase of the multi-path CIR are used to distinguish PU from PUE, while only channel-tap power is used in the PUEA detection method proposed by Chin *et al.* (2014).

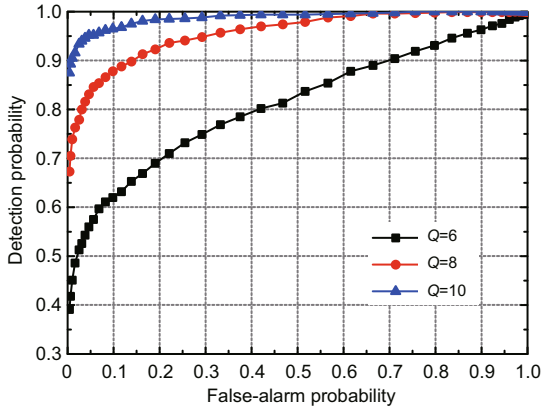

Fig. 8 Detection performance under different Q (SNR=5 dB, M_{h}=30)

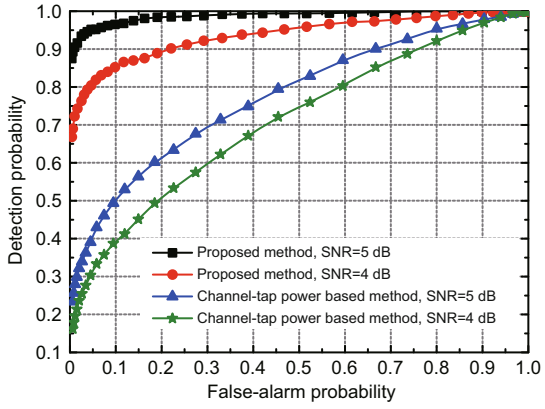

Fig. 9 Comparison of the detection performance under the proposed method and channel-tap power based method with SNR=5 dB or 4 dB (Q=10, M_{h}=30)

Finally, we validate the performance analysis in Section 3.2.2. The theoretical relationship between the detection probability and false-alarm probability is calculated using Eq. (21). To satisfy all the assumptions in Section 3.2.2, the simulation parameters are set as SNR=30 dB, Q = 15, and M_{h}=80. The CIR of the PU-SU channel is set the same as in Table 1, while the difference between the CIRs of PU-SU and PUE-SU channels is set as $\boldsymbol{\Delta} = [-0.01 - 0.02\mathrm{i}, -0.04 + 0.05\mathrm{i}, \mathbf{0}_{1\times 15}]^{\mathrm{T}}$. From Fig. 10, one finds that the simulation results of the ROC curve are considerably close to the corresponding theoretical ones. However, one also finds that with the same false-alarm probability, the simulated detection probability is slightly higher than the theoretical value. The reason for this phenomenon is that the two assumptions used to derive Eq. (18) make the detection probability in Eq. (18) slightly smaller than that in Eq. (17).

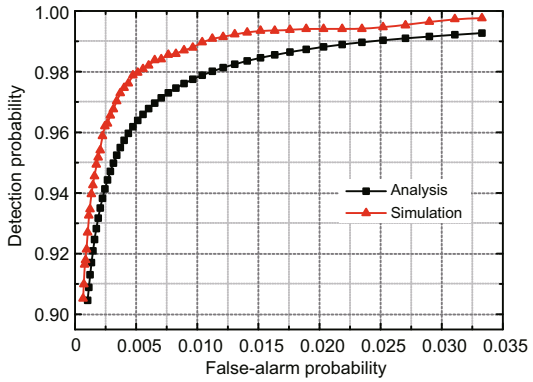

Fig. 10 Comparison between analytical and numerical results of detection performance

5 Conclusions

In this paper, we have proposed a method for detecting the PUEA using the uniqueness of the multi-path CIR between the transmitter and the receiver. Adopting OFDM symbol structure estimation and

subspace-based blind channel estimation, the proposed PUEA detection method needs no prior knowledge about the structure and content of the PU signal. Based on the estimated CIR between the SU and the signal source (PU or PUE), a binary hypothesis test was constructed to determine whether the received signal at the SU is transmitted from PU or PUE. The performance of the proposed PUEA detection method was theoretically analyzed, and the closed-form expression of the detection performance was derived. The analytical results were verified by Monte-Carlo simulation results. Numerical results show that the proposed PUEA detection method can detect the PUEA effectively.

References

Chen, R.L., Park, J.M., 2006. Ensuring trustworthy spectrum sensing in cognitive radio networks. Proc. 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, p.110-119. https://doi.org/10.1109/SDR.2006.4286333

Chen, R.L., Park, J.M., Reed, J.H., 2008. Defense against primary user emulation attacks in cognitive radio networks. *IEEE J. Sel. Areas Commun.*, **26**(1):25-37. https://doi.org/10.1109/JSAC.2008.080104

Chin, W.L., Le, T.N., Tseng, C.L., *et al.*, 2014. Cooperative detection of primary user emulation attacks based on channel-tap power in mobile cognitive radio networks. *Int. J. Ad Hoc Ubiq. Comput.*, **15**(4):263-274. https://doi.org/10.1504/ijahuc.2014.061005

Fang, S.H., Chen, J.Y., Shieh, M.D., *et al.*, 2013. Subspace-based blind channel estimation by separating real and imaginary symbols for cyclic-prefixed single-carrier systems. *IEEE Trans. Broadcast.*, **59**(4):698-704. https://doi.org/10.1109/TBC.2013.2281950

Haykin, S., 2005. Cognitive radio: brain-empowered wireless communications. *IEEE J. Sel. Areas Commun.*, **23**(2): 201-220. https://doi.org/10.1109/JSAC.2004.839380

Jin, F., Varadharajan, V., Tupakula, U., 2015. Improved detection of primary user emulation attacks in cognitive radio networks. Proc. Int. Telecommunication Networks and Applications Conf., p.274-279. https://doi.org/10.1109/ATNAC.2015.7366825

Jin, Z., Anand, S., Subbalakshmi, K.P., 2009. Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing. *ACM SIGMOBILE Mob. Comput. Commun. Rev.*, **13**(2):74-85. https://doi.org/10.1145/1621076.1621084

Kay, S.M., 1993. Fundamentals of Statistical Signal Processing: Estimation Theory. Prentice-Hall, New Jersey, p.27-82.

Kim, J.G., Oh, J.H., Lim, J.T., 2012. Subspace-based channel estimation for MIMO-OFDM systems with few received blocks. *IEEE Signal Process. Lett.*, **19**(7):435-438. https://doi.org/10.1109/LSP.2012.2197201

Lalos, A.S., Rontogiannis, A.A., Berberidis, K., 2010. Frequency domain channel estimation for cooperative communication networks. *IEEE Trans. Signal Process.*, **58**(6):3400-3405. https://doi.org/10.1109/TSP.2010.2045413

Le, T.N., Chin, W.L., Kao, W.C., 2015. Cross-layer design for primary user emulation attacks detection in mobile cognitive radio networks. *IEEE Commun. Lett.*, **19**(5):799-802. https://doi.org/10.1109/LCOMM.2015.2399920

Le, T.N., Chin, W.L., Lin, Y.H., 2016. Non-cooperative and cooperative PUEA detection using physical layer in mobile OFDM-based cognitive radio networks. Proc. Int. Conf. on Computing, Networking and Communications, p.1-5. https://doi.org/10.1109/ICCNC.2016.7440583

Liu, M., Crussiere, M., Helard, J.F., 2012. A novel data-aided channel estimation with reduced complexity for TDS-OFDM systems. *IEEE Trans. Broadcast.*, **58**(2):247-260. https://doi.org/10.1109/TBC.2012.2184152

Muquet, B., de Courville, M., Duhamel, P., 2002. Subspace-based blind and semi-blind channel estimation for OFDM systems. *IEEE Trans. Signal Process.*, **50**(7): 1699-1712. https://doi.org/10.1109/TSP.2002.1011210

National Standard of the People's Republic of China, 2007. Framing Structure, Channel Coding and Modulation for Digital Television Terrestrial Broadcasting System. GB 206000-2006 (in Chinese).

Nguyen, N.T., Zheng, R., Han, Z., 2012. On identifying primary user emulation attacks in cognitive radio systems using nonparametric Bayesian classification. *IEEE Trans. Signal Process.*, **60**(3):1432-1445. https://doi.org/10.1109/TSP.2011.2178407

Pu, D., Wyglinski, A.M., 2014. Primary-user emulation detection using database-assisted frequency-domain action recognition. *IEEE Trans. Veh. Technol.*, **63**(9):4372-4382. https://doi.org/10.1109/TVT.2014.2316831

Rao, C.R., 1973. Linear Statistical Inference and Its Applications. John Wiley & Sons, New York, p.516-604. https://doi.org/10.1002/9780470316436

Su, B., Vaidyanathan, P.P., 2007. Subspace-based blind channel identification for cyclic prefix systems using few received blocks. *IEEE Trans. Signal Process.*, **55**(10): 4979-4993. https://doi.org/10.1109/TSP.2007.896262

Tomasoni, A., Gatti, D., Bellini, S., *et al.*, 2013. Efficient OFDM channel estimation via an information criterion. *IEEE Trans. Wirel. Commun.*, **12**(3):1352-1362. https://doi.org/10.1109/TWC.2013.022713.120961

Tugnait, J.K., Kim, H., 2010. A channel-based hypothesis testing approach to enhance user authentication in wireless networks. Proc. 2nd Int. Conf. on Communication Systems and Networks, p.1-9. https://doi.org/10.1109/comsnets.2010.5432018

Wooding, R.A., 1956. The multivariate distribution of complex normal variables. *Biometrika*, **43**(1-2):212-215. https://doi.org/10.2307/2333597

Xin, C.S., Song, M., 2014. Detection of PUE attacks in cognitive radio networks based on signal activity pattern. *IEEE Trans. Mob. Comput.*, **13**(5):1022-1034. https://doi.org/10.1109/TMC.2013.121

Zhou, W., Lam, W.H., 2010. Channel estimation and data detection for OFDM systems over fast-fading and dispersive channels. *IEEE Trans. Veh. Technol.*, **59**(3): 1381-1392. https://doi.org/10.1109/TVT.2009.2037639