Cooperative Spectrum Sensing in Cognitive Radio Networks in the Presence of the Primary User Emulation Attack

Chao Chen, Hongbing Cheng, *Member, IEEE*, and Yu-Dong Yao, *Fellow, IEEE*

***Abstract*—In recent years, the security issues of the cognitive radio (CR) networks have drawn a lot of research attentions. Primary user emulation attack (PUEA), as one of common attacks, compromises the spectrum sensing, where a malicious user forestalls vacant channels by impersonating the primary user to prevent other secondary users from accessing the idle frequency bands. In this paper, we propose a new cooperative spectrum sensing scheme, considering the existence of PUEA in CR networks. In the proposed scheme, the sensing information of different secondary users is combined at a fusion center and the combining weights are optimized with the objective of maximizing the detection probability of available channels under the constraint of a required false alarm probability. We also investigate the impact of the channel estimation errors on the detection probability. Simulation and numerical results illustrate the effectiveness of the proposed scheme in cooperative spectrum sensing in the presence of PUEA.**

***Index Terms*—Cognitive radio, cooperative spectrum sensing, primary user emulation attack, security, optimization.**

I. Introduction

As the ever-increasing growth of wireless communication technology and the high demand of the capacity for wireless services, the wireless frequency spectrum has become a scarce resource in the past decade. On one hand, the available spectrum is overcrowded and little space is left. On the other hand, however, the precious spectrum assigned for exclusive usage are not yet utilized efficiently. This situation gives rise to a new technology paradigm, called "cognitive radio" (CR), which allows unlicensed users to access the licensed frequency bands without interfering with the licensed users [1] [2]. With this novel technology, the spectral efficiency of the wireless system is dramatically improved.

Cognitive radio generally includes four basic elements: spectrum sensing, spectrum management, spectrum sharing and spectrum mobility. Among them, Spectrum sensing is a fundamental functionality where the secondary users monitor the frequency spectrum and detect vacant channels to use. The spectrum sensing can basically be classified as non-cooperative sensing, cooperative sensing and interference-based sensing [3]. Most research work currently focuses on the cooperative spectrum sensing technique where a set of secondary users exchange the sensing information or send the information to a fusion center to improve detection probability performance, taking into account that some secondary users' channels may be deteriorated by multi-path fading or shadowing [4]. So far, several algorithms have been proposed to implement cooperative sensing in CR networks. In [5], a hard combining (HDC) method is proposed where the binary detection results of multiple secondary users are converged to a fusion center and the final decision is made based on "1-out-of-n" rule. In [6], a soft combining method, equivalent to maximal ratio combining (MRC), is developed where the sensing statistics of different secondary users are combined by using the optimal weight coefficients determined by the instantaneous channel gain between the primary and secondary user. It is shown that the soft combination yields a higher detection probability than the hard combination. [7] formulates the cooperative spectrum sensing as a nonlinear optimization problem in which the interference to the primary users is minimized. Different from [5] and [6], [8] and [9] propose another cooperative sensing model without a fusion center which applies the cooperative diversity to the spectrum sensing and demonstrate that the performance gain is achieved due to the inherent characteristic of spatial diversity.

As far as the security is concerned, the intrinsic properties of CR networks pose new challenges to wireless communications. To date, there have been several research literatures studying the security issues of CR networks. The potential vulnerabilities and countermeasures for security are surveyed in [10]-[12]. [13] specifies the objective function attack which disrupts the artificial intelligence learning algorithms of cognitive radios. [14] and [15] discuss how the attacker compromises the transport (TCP) and MAC (IEEE 802.22) layer protocol in CR networks. [16]-[19] concentrate on the detection of the unknown/unauthorized users or malicious users sending out erroneous messages deliberately in CR networks. The primary user emulation attack (PUEA or PUE attack) is first identified in [20] where the attacker occupies the unused channels by emitting a signal with similar form as the primary user so as to deter the access of the vacant channels from other secondary users. A detection mechanism is also proposed in [20] which exploits the distance ratio and the distance difference to detect PUEA. In [21], PUEA is detected through a sequential test without any knowledge of location information, based on an analytical model on the probability of successful PUEA given in [22]. In [23], how the attacker emulates the characteristics of the primary user is

Manuscript received April 16, 2010; revised September 22, 2010 and February 11, 2011; accepted March 14, 2011. The associate editor coordinating the review of this paper and approving it for publication was T. Hou.

The authors are with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ 07030, USA (e-mail: {cchen3, hcheng, yyao}@stevens.edu).

Digital Object Identifier 10.1109/TWC.2011.041311.100626

1536-1276/11$25.00 © 2011 IEEE

modeled and the attacker is detected based on the difference between the attacker's and the primary user's communication channels. Apart from the detection of PUEA, the defense schemes against PUEA have been studied as well [24]-[26]. In [24], a localization based defense technique is employed in which a number of sensors are deployed to pinpoint the PUE attacker collaboratively. In [25] and [26], the defense against PUEA is modeled as a game theoretic or multi-armed bandit problem, with or without the knowledge of channel statistics respectively.

Although a variety of research efforts have been directed on the detection and defense schemes of PUEA, the cooperative spectrum sensing technique with the existence of PUEA is not well understood. In this paper, we establish a model of cooperative spectrum sensing in the presence of PUEA and propose a scheme to maximize the detection probability of primary user. As the PUEA is launched in a CR network using cooperative sensing technique, each secondary user receives the signals from both the attacker and the primary user and sends its sensing information to a fusion center. The received signal (or the sensing information) is then optimally combined with some appropriate weights to maximize the detection probability with a constraint of false alarm probability. The optimal weights are related to the channel state information (CSI) between the attacker and secondary users and between the primary user and secondary users, which are estimated by using existing channel estimation algorithms. The main contribution of this paper is to maximize the detection probability of the primary user by deriving the optimal combining weights, considering the existence of the PUEA in a CR network. Note that we assume the PUE attacker has been detected and this paper thus centers on the detection of the primary user rather than the detection of PUEA as in [16] and [21].

The rest of the paper is organized as follows. Section II establishes the system model of cooperative sensing in CR networks when PUEA is present and formulates the detection probability of the primary user in the presence of PUEA. Section III presents the optimal combining scheme and derives the optimal weights to maximize the detection probability. Simulation results are given in Section IV and the conclusion is drawn in Section V.

II. System Model

In this paper, we consider cooperative spectrum sensing in a CR network where N secondary users detect the presence of one primary transmitter, as shown in Figure 1. Taking PUEA into the consideration, for $1 \leq i \leq N$, the signal received by the ith secondary user at the kth time instant is,

$$y_i(k) = \alpha\sqrt{P_p}h_{pi}(k)x_p(k) + \beta\sqrt{P_m}h_{mi}(k)x_m(k) + n_i(k), \quad (1)$$

where $x_p(k)$ and $x_m(k)$ are the signal transmitted by primary user and attacker, with the power P_p and P_m respectively. $h_{pi}(k)$ and $h_{mi}(k)$ denote the instantaneous channel response between primary user and ith secondary user and between attacker and ith secondary user, respectively. $n_i(k)$ is the additive white Gaussian noise at the ith secondary user with zero mean and variance σ_n^2. α and β are two binary indicators where $\alpha = 1$ or $\beta = 1$ indicates the presence of primary user or attacker and $\alpha = 0$ or $\beta = 0$ implies their absence. If no PUE attacker is detected, the indicator of the attacker $\beta = 0$ and the conventional MRC method can be used in the cooperative spectrum sensing [6]. Otherwise, $\beta = 1$, which indicates that the PUE attacker is present and therefore the combining scheme of MRC has to be redesigned to optimize the performance of the spectrum sensing. In a cooperative manner, the signals received by secondary users are weighted by some coefficients $w_i, i = 1, 2, ..., N$ and converged to a fusion center where a final decision is made, depending on the absence or presence of the primary user. It is assumed that the channels from secondary users to the fusion center are perfect, e.g., dedicated control channel [6]. The combined signal in the fusion center at the kth time instant is given in Eq.(2). Note that the significant bandwidth is required in forwarding continuous values of $y_i(k)$, $1 \leq i \leq N$. Some forms of quantization for $y_i(k)$ thus need to be implemented in practice. However, this issue is not studied in the paper.

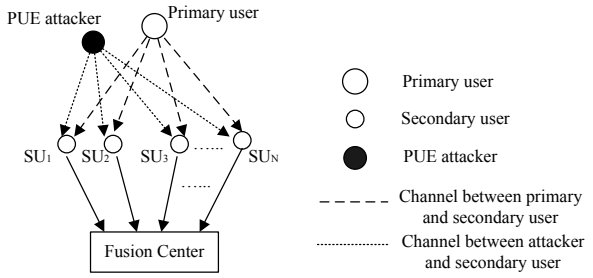


Fig. 1. System model of cooperative spectrum sensing with PUEA in cognitive radio network.

We denote the absence and presence of primary user, when the PUE attacker is present, as two hypotheses, $\mathcal{H}_0$ and $\mathcal{H}_1$ respectively, as given in Eq.(3). To classify between $\mathcal{H}_0$ and $\mathcal{H}_1$, several methods can be applied in cooperative sensing, such as matched filter detection, energy detection and cyclostationary detection [3]. In this paper, we adopt the energy detection method [4] in which M samples of the energy of $y(k)$ are summed during one detection interval,

$$Y = \sum_{k=1}^{M} |y(k)|^2 . \quad (4)$$

The fusion center then calculates the decision statistic Y for each detection interval to make a global decision.

The objective of cooperative spectrum sensing, as we will discuss in Section III, is to find optimal weights $w_i, i = 1, 2, ..., N$, to maximize the detection probability of the primary user under the constraint of a false alarm probability. This paper differs from the previous work, such as [6] and [7], in considering the existence of the PUE attacker in the cognitive radio network.

III. Cooperative Spectrum Sensing in the Presence of PUEA

In this section, we will derive the optimal weights to maximize the detection performance in cooperative sensing with the presence of PUEA. We will also examine the impact of the channel estimation error on the detection performance.

$$\begin{aligned} y(k) &= \sum_{i=1}^{N} w_i y_i(k) \\ &= \sum_{i=1}^{N} w_i \left(\alpha\sqrt{P_p} h_{pi}(k) x_p(k) + \beta\sqrt{P_m} h_{mi}(k) x_m(k) + n_i(k) \right) \\ &= \underbrace{\alpha\sqrt{P_p} \sum_{i=1}^{N} w_i h_{pi}(k) x_p(k)}_{\textbf{primary signal component}} + \underbrace{\beta\sqrt{P_m} \sum_{i=1}^{N} w_i h_{mi}(k) x_m(k)}_{\textbf{malicious signal component}} \\ &\quad + \underbrace{\sum_{i=1}^{N} w_i n_i(k)}_{\textbf{noise component}}, \end{aligned} \tag{2}$$

$$y(k) = \begin{cases} \sqrt{P_m} \sum_{i=1}^{N} w_i h_{mi}(k) x_m(k) + \sum_{i=1}^{N} w_i n_i(k), & \mathcal{H}_0(\alpha = 0) \\ \sqrt{P_p} \sum_{i=1}^{N} w_i h_{pi}(k) x_p(k) + \sqrt{P_m} \sum_{i=1}^{N} w_i h_{mi}(k) x_m(k) + \sum_{i=1}^{N} w_i n_i(k), & \mathcal{H}_1(\alpha = 1) \end{cases} \tag{3}$$

A. Optimal Combining Scheme

In the spectrum sensing of cognitive radio networks, false alarm probability P_f and detection probability P_d over a detection interval are defined as [27],

$$P_f = P_r(Y \geq T | \mathcal{H}_0), \tag{5}$$

$$P_d = P_r(Y \geq T | \mathcal{H}_1), \tag{6}$$

where T is a detection threshold. The following derivation obtains the optimal weights $\mathbf{w_{opt}}$ so that the detection probability P_d is maximized under the constraint of a false alarm probability P_f. Therefore, the detection problem is described as,

$$\mathbf{w_{opt}} = arg \max_{\mathbf{w}} \{P_d | P_f = \zeta\}, \tag{7}$$

where ζ denotes a predefined false alarm probability and $\mathbf{w}$ is a vector of weights for the combination at the fusion center, which is given by,

$$\mathbf{w} = [w_1, w_2, ..., w_N], \tag{8}$$

and $\mathbf{w_{opt}}$ is a vector of optimal weights,

$$\mathbf{w_{opt}} = [w_{1_{opt}}, w_{2_{opt}}, ..., w_{N_{opt}}], \tag{9}$$

As in [6], primary user's signal x_p is assumed to be independently and identically distributed (i.i.d) complex Gaussian random variable with zero mean and unit variance. Due to the similarity between malicious and primary signal in PUEA, the attacker's signal x_m can also follow the complex Gaussian distribution. We assume that the existence of PUEA has been detected by some detection approach [19] [21], such that $\beta = 1$ for the entire spectrum sensing process. In addition, all the channels are considered to be subject to block fading, that is, $h_{pi}(k)$ and $h_{mi}(k)$ are constant within one detection interval and k can thereby be omitted. For given h_{pi} and h_{mi}, the combined signal $y(k)$ is also a complex Gaussian distributed random variable,

$$y(k) \sim \begin{cases} \mathcal{CN}(0, \sigma_0^2), & \mathcal{H}_0 \\ \mathcal{CN}(0, \sigma_1^2), & \mathcal{H}_1 \end{cases} \tag{10}$$

where σ_0^2 and σ_1^2 are the variance of $y(k)$ for $\mathcal{H}_0$ and $\mathcal{H}_1$ respectively,

$$\sigma_0^2 = P_m \left| \sum_{i=1}^{N} w_i h_{mi} \right|^2 + \sum_{i=1}^{N} |w_i|^2 \sigma_n^2, \tag{11}$$

$$\sigma_1^2 = P_m \left| \sum_{i=1}^{N} w_i h_{mi} \right|^2 + P_p \left| \sum_{i=1}^{N} w_i h_{pi} \right|^2 + \sum_{i=1}^{N} |w_i|^2 \sigma_n^2, \tag{12}$$

As such, the decision statistic Y is compliant with the central Chi-square (χ^2) distribution with $2M$ degrees of freedom and parameters σ_0^2 and σ_1^2 for $\mathcal{H}_0$ and $\mathcal{H}_1$ respectively [27],

$$Y = \sum_{i=1}^{M} |y(k)|^2 = \begin{cases} Y_0 \sim \chi^2_{2M}(\sigma_0^2), & \mathcal{H}_0 \\ Y_1 \sim \chi^2_{2M}(\sigma_1^2), & \mathcal{H}_1 \end{cases} \tag{13}$$

Hence, the false alarm probability P_f and the detection probability P_d are expressed as,

$$P_f = \frac{\Gamma(M, \frac{T}{\sigma_0^2})}{\Gamma(M)}, \tag{14}$$

$$P_d = \frac{\Gamma(M, \frac{T}{\sigma_1^2})}{\Gamma(M)}, \tag{15}$$

where $\Gamma(\cdot)$ and $\Gamma(\cdot, \cdot)$ are Gamma function and upper incomplete Gamma function respectively [31].

Given $P_f = \zeta$, $\zeta \in [0, 1]$, the decision threshold T is represented as,

$$T = \Gamma^{-1}(M, \zeta\Gamma(M))\sigma_0^2, \tag{16}$$

where $\Gamma^{-1}(\cdot,\cdot)$ is the inverse incomplete Gamma function [31]. By inserting (16) into (15), P_d can be rewritten as,

$$P_d = \frac{\Gamma\big(M, \Gamma^{-1}(M, \zeta\Gamma(M))\frac{\sigma_0^2}{\sigma_1^2}\big)}{\Gamma(M)}, \tag{17}$$

Due to the monotonicity of Gamma function, for given M and ζ, the optimization problem in (17) is equivalent to minimize σ_0^2/σ_1^2.

Let $\mathbf{h_m} = [h_{m1}(k), h_{m2}(k), ..., h_{mN}(k)]^T$, $\mathbf{h_p} = [h_{p1}(k), h_{p2}(k), ..., h_{pN}(k)]^T$, σ_0^2 and σ_1^2 can be denoted by two quadratic forms,

$$\sigma_0^2 = P_m \mathbf{w}\mathbf{H_m}\mathbf{w}^H + \sigma_n^2 \mathbf{w}\mathbf{w}^H, \tag{18}$$

$$\sigma_1^2 = P_m \mathbf{w}\mathbf{H_m}\mathbf{w}^H + P_p \mathbf{w}\mathbf{H_p}\mathbf{w}^H + \sigma_n^2 \mathbf{w}\mathbf{w}^H, \tag{19}$$

where H is the Hermitian transpose and $\mathbf{H_m} = \mathbf{h_m}\mathbf{h_m}^H$, $\mathbf{H_p} = \mathbf{h_p}\mathbf{h_p}^H$. Then,

$$\begin{aligned}\frac{\sigma_0^2}{\sigma_1^2} &= \frac{P_m \mathbf{w}\mathbf{H_m}\mathbf{w}^H + \sigma_n^2 \mathbf{w}\mathbf{w}^H}{P_m \mathbf{w}\mathbf{H_m}\mathbf{w}^H + P_p \mathbf{w}\mathbf{H_p}\mathbf{w}^H + \sigma_n^2 \mathbf{w}\mathbf{w}^H} \\ &= \frac{1}{1 + \dfrac{\mathbf{w}\boldsymbol{\Theta}\mathbf{w}^H}{\mathbf{w}\boldsymbol{\Phi}\mathbf{w}^H}},\end{aligned} \tag{20}$$

where $\boldsymbol{\Theta} = P_p\mathbf{H_p}$, $\boldsymbol{\Phi} = P_m\mathbf{H_m} + \sigma_n^2\mathbf{I}$ and $\mathbf{I}$ is the identity matrix. Note that $\boldsymbol{\Theta}$ and $\boldsymbol{\Phi}$ are both symmetric and $\boldsymbol{\Theta}$ is positive definite and of rank 1, according to [28], the optimal weight vector $\mathbf{w_{opt}}$ is,

$$\mathbf{w_{opt}} = (\boldsymbol{\Phi}^{-1}\mathbf{h_p})^H, \tag{21}$$

and the minimal σ_0^2/σ_1^2 is,

$$(\frac{\sigma_0^2}{\sigma_1^2})_{min} = \frac{1}{1 + P_p \mathbf{h_p}^H \boldsymbol{\Phi}^{-1}\mathbf{h_p}}, \tag{22}$$

which can also be given by the largest eigenvalue λ_{max} of $\boldsymbol{\Theta}\boldsymbol{\Phi}^{-1}$ [28]. Using (17) and (22), the maximal detection probability $P_d(\mathbf{w_{opt}})$ is,

$$P_d(\mathbf{w_{opt}}) = \frac{\Gamma\big(M, \Gamma^{-1}(M, \zeta\Gamma(M))\frac{1}{1+\lambda_{max}}\big)}{\Gamma(M)}, \tag{23}$$

Specially, if $P_m = 0$, i.e., the signal strength of the attacker is negligible, $\mathbf{w_{opt}}$ is simplified to $\mathbf{h_p}^H$ which is identical to the conventional MRC method.

The rationale behind the proposed optimal combining scheme is that the optimal weights form a "virtual" antenna array which steers "null point" of its radiation pattern towards the malicious user in order that the malicious signal component can be eliminated from the received signal.

We have derived the optimal weights over one detection interval during which the channel response is considered to be constant. The average detection probability $\bar{P}_d$ can be obtained by averaging $P_d(\mathbf{w})$ over fading channels [5],

$$\bar{P}_d = \iint P_d(\mathbf{w_{opt}}) f(\mathbf{h_p}) f(\mathbf{h_m}) d\mathbf{h_p} d\mathbf{h_m}. \tag{24}$$

where $f(\mathbf{h_p})$ and $f(\mathbf{h_m})$ denote the probability density functions (PDF) of the signal-to-noise ratio (SNR) over the fading channel which may follow Rayleigh, Rician or Nakagami distribution.

B. Impact of the Channel Estimation Error on Detection Probability

From the above derivations, we find that the optimization of the combining weights requires the information of $\mathbf{h_p}$ and $\mathbf{h_m}$, which are the channel state information between the primary user and secondary users and between the attacker and secondary users. Due to the lack of interaction between primary and secondary users in cognitive radio networks, it is difficult for secondary users to have the perfect channel state information. However, the channel information, both for the primary user and the attacker, can be obtained by the blind estimation method [23] [29].

Compared with the conventional energy detection, the proposed scheme needs to estimate the channel information and the estimation error of CSI is not negligible. To give an in-depth insight to the impact of the channel estimation error on the detection performance, we model the estimated CSI $\hat{\mathbf{h}}_\mathbf{p}$ and $\hat{\mathbf{h}}_\mathbf{m}$ as,

$$\hat{\mathbf{h}}_\mathbf{p} = \mathbf{h_p} + \mathbf{e_p}, \tag{25}$$

$$\hat{\mathbf{h}}_\mathbf{m} = \mathbf{h_m} + \mathbf{e_m}, \tag{26}$$

where $\mathbf{e_p}$ and $\mathbf{e_m}$ represent the estimation error which can be assumed to be Gaussian distributed random variables with the mean square values $\sigma_{e_p}^2$ and $\sigma_{e_m}^2$ respectively [30]. In consideration of the channel estimation error, the average detection probability in (24) can be rewritten as,

$$\bar{P}_d = \iint P_d(\hat{\mathbf{w}}_\mathbf{opt}) f(\mathbf{h_p}) f(\mathbf{h_m}) f(\mathbf{e_p}) f(\mathbf{e_m}) d\mathbf{h_p} d\mathbf{h_m} d\mathbf{e_p} d\mathbf{e_m}. \tag{27}$$

where $\hat{\mathbf{w}}_\mathbf{opt} = [\hat{w}_{1_{opt}}, \hat{w}_{2_{opt}}, ..., \hat{w}_{N_{opt}}]$ is a vector of optimal weights calculated by (21) using $\hat{\mathbf{h}}_\mathbf{p}$ and $\hat{\mathbf{h}}_\mathbf{m}$. We will show the impact of different mean square estimation (MSE) error on the detection performance in Section IV.

IV. Simulation Results

We implement the simulations of the cooperative sensing scheme with the existence of PUEA. The channels are assumed to be identically and independently distributed block Rayleigh fading. The number of samples within a detection interval is $M = 3$.

Figure 2 displays the detection probability versus false alarm probability for our optimal combining scheme, the conventional MRC and non-cooperative sensing scheme when considering the presence of PUEA in the CR network. In the simulation, all channel information are assumed to be known to the secondary users. The average SNR is set as 0 dB and the emitting power of the primary user and the attacker is $P_p = P_m = 1$. Since we assume that the channel information can be obtained by secondary users through the estimation algorithm, the optimal weight in conventional MRC is modified as h_{pi}^* rather than $|h_{pi}|^2$ as in [6]. From Figure 2, we find that the detection probability of conventional MRC and non-cooperative schemes are both severely compromised by PUEA. In our optimal combining scheme, as the PUEA has been detected, the optimal weights are set as in (21) and a significant improvement of detection performance is observed, compared to the conventional MRC and non-cooperation schemes. Essentially, the proposed optimal combining scheme

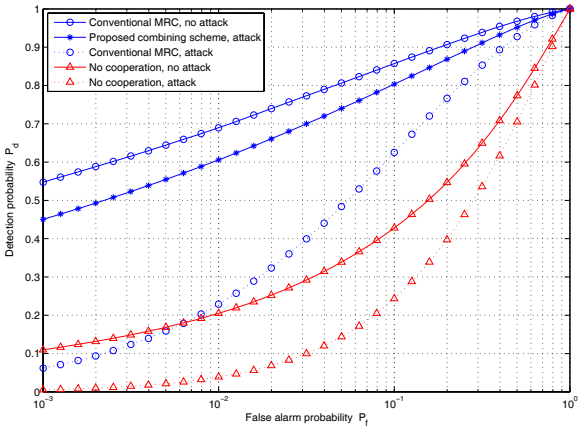


Fig. 2. Detection probability versus false alarm probability for the proposed optimal combining, conventional MRC and non-cooperative sensing schemes, SNR = 0 dB, $N = 4$.

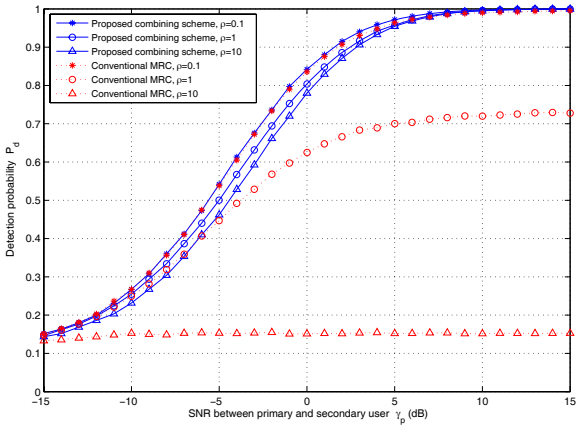


Fig. 3. Detection probability versus average SNR γ_p for the proposed optimal combining and conventional MRC schemes, $P_f = 10^{-1}$ and $\rho = 0.1, 1, 10$, $N = 4$.

considers the channel information between the attacker and secondary users, $\mathbf{h_m}$, as a result, the malicious signal is mitigated from received signal and thus the better detection performance is obtained.

Figure 3 illustrates the performance of the detection probability versus the signal-to-noise ratio of the cooperative sensing when PUEA is present. In the simulation, the false alarm probability is set as $P_f = 10^{-1}$ and SNR between primary and secondary users is defined as γ_p which is assumed to be same for each secondary user. Here, we define

$$\rho = \frac{P_m}{P_p}. \tag{28}$$

which normalizes attacker's power in terms of primary user's power. A large ρ indicates a strong attacker. In Figure 3, the detection performance of the proposed combination scheme is compared with the conventional MRC scheme where the ρ is given as 0.1, 1 and 10, respectively. It is seen from Figure 3 that the detection probability is improved with increasing average SNR. It also notes that the proposed combining scheme always has performance gain over the conventional MRC as the SNR increases from -15 dB to 15 dB. And as ρ increases from 0.1 to 10, the detection probabilities of both schemes are decreased and the conventional MRC exhibits more remarkable performance degradation. It is also viewed that the detection probability of conventional MRC is approximately constant over different SNR when $\rho = 10$. This is because the strength of malicious signal is dominant over the noise power such that the detection performance is poor even when the average SNR is very high.

Furthermore, we plot the detection performance considering various values of $\sigma^2_{e_p}$ and $\sigma^2_{e_m}$, which indicates the accuracy of the channel estimation. In our simulation, the one of $\sigma^2_{e_p}$ and $\sigma^2_{e_m}$ is set as -15 dB, -10 dB and -5 dB and the other is fixed to be -15dB. The larger error implies the more difficulty of the estimation method. The average SNR is 0 dB. Considering the difficulties of estimating the CSI at the secondary users, we investigate the detection performance with a relatively large channel estimation error in the simulation

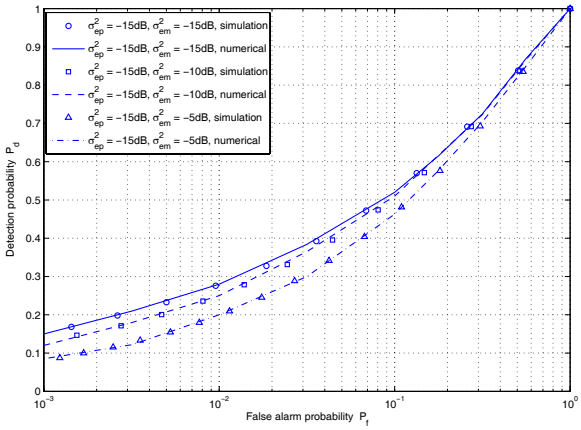


Fig. 4. Comparison of simulation and numerical results when $\sigma^2_{e_p}$ = -15 dB and $\sigma^2_{e_m}$ = -15 dB, -10 dB, -5 dB, SNR = 0 dB, $N = 2$.

(e.g., -5 dB). We also perform the numerical calculation of the detection probability and compare the results with the simulation in Figure 4 and 5. Figure 4 compares the simulation and numerical results when $\sigma^2_{e_p}$ = -15 dB and $\sigma^2_{e_m}$ = -15 dB, -10 dB, -5 dB and Figure 5 compares the simulation and numerical results when $\sigma^2_{e_m}$ = -15 dB and $\sigma^2_{e_p}$ = -15 dB, -10 dB, -5 dB. The numerical results are calculated based on Eq.(27). The number of secondary users is set to be $N = 2$ instead of $N = 4$ due to the high complexity of the numerical calculation for the case of four or more secondary users. The results of comparison in Figure 4 and 5 show that the simulation and numerical results match very well.

In addition, Figure 6 and 7 compare the detection performance of the proposed combination with the conventional MRC scheme when the number of secondary users $N = 4$. Similar as the two secondary users case, the one of $\sigma^2_{e_p}$ and $\sigma^2_{e_m}$ is set as -15 dB, -10 dB and -5 dB and the other is fixed to be -15dB. It is seen that the proposed optimal combining scheme exhibits better performance than the conventional MRC for the various estimation error. Notice that the conventional MRC scheme does not require the CSI

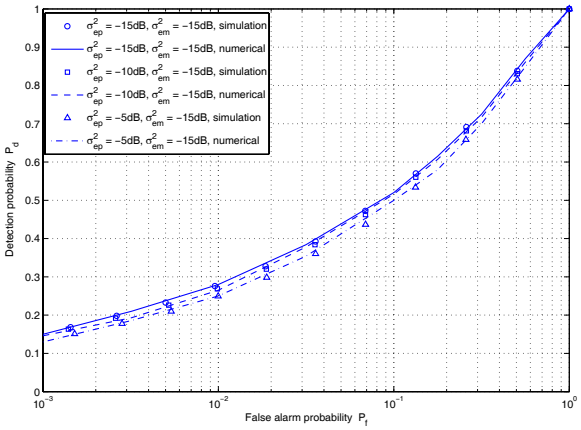


Fig. 5. Comparison of simulation and numerical results when $\sigma^2_{e_m}$ = -15 dB and $\sigma^2_{e_p}$ = -15 dB, -10 dB, -5 dB, SNR = 0 dB, $N = 2$.

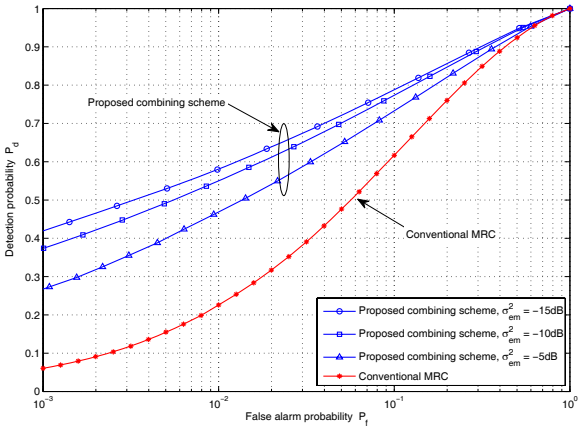


Fig. 6. Detection performance of proposed optimal combining and conventional MRC scheme, $\sigma^2_{e_m}$ = -15 dB, -10 dB, -5 dB and $\sigma^2_{e_p}$ = -15 dB, SNR = 0 dB, $N = 4$.

between attacker and secondary user, its performance is not affected by the change of $\sigma^2_{e_m}$ (see Figure 6).

V. Conclusion

In this paper, we have studied cooperative spectrum sensing in CR network in the presence of primary user emulation attack. PUEA is an attack in cognitive radio networks where the malicious user pretends to be the primary user to preempt idle channels by transmitting a similar signal as the primary user. To maximize the detection probability of primary user with the presence of PUEA, we use the channel information between primary user and secondary users and between attacker and secondary users to derive the optimal weights for a optimal combining scheme so that the detection probability of the primary user is optimized under the constraint of a required false alarm probability. In essence, the proposed scheme takes advantage of a set of cooperative sensors to eliminate the malicious signal. Simulation results show the detection performance improvement of the proposed optimal combining scheme. The simulation results show that the optimal combining scheme yields better performance than the

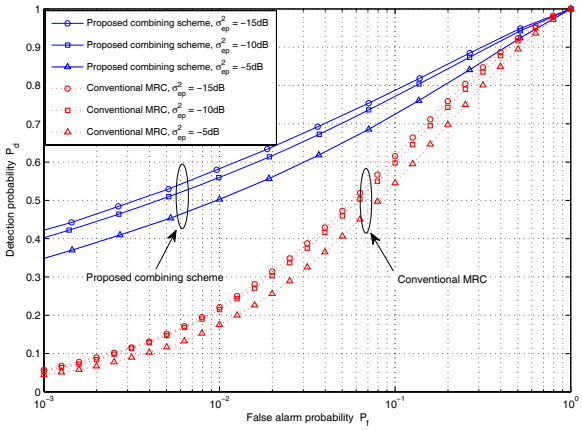


Fig. 7. Detection performance of proposed optimal combining and conventional MRC scheme, $\sigma^2_{e_p}$ = -15 dB, -10 dB, -5 dB and $\sigma^2_{e_m}$ = -15 dB, SNR = 0 dB, $N = 4$.

conventional MRC method. We also analyze the impact of channel estimation error on the detection performance. The numerical results accord with the simulation results and the detection performance is improved even when the channel estimation error is relatively large.

References

[1] J. Mitola and G. Maguire, "Cognitive radio: making software radios more personal," *IEEE Commun. Mag.*, vol. 6, no. 4, pp. 13-18, Aug. 1999.

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

[3] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Elsevier Comput. Netw.*, vol. 50, pp. 2127-2159, 2006.

[4] D. Cabric, S. Mishra, and R. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Proc. Asilomar Conf. Signals, Syst. Comput.*, Nov. 2004, pp. 772-776.

[5] A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *Proc. IEEE International Dynamic Spectrum Access Netw.*, Nov. 2005, pp. 131-136.

[6] J. Ma, G. Zhao, and Y. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4502-4507, Nov. 2008.

[7] Z. Quan, S. Cui, and A. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 28-40, Feb. 2008.

[8] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio, part I: two user networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 6, pp. 2204-2213, June 2007.

[9] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio, part II: multiuser networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 6, pp. 2214-2222, June 2007.

[10] T. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: a multi-dimensional analysis and assessment," in *Proc. IEEE International Conf. Cognitive Radio Oriented Wireless Netw. Commun.*, Aug. 2007, pp. 456-464.

[11] J. Burbank, "Security in cognitive radio networks: the required evolution in approaches to wireless network security," in *Proc. IEEE International Conf. Cognitive Radio Oriented Wireless Netw. Commun.*, May 2008, pp. 1-7.

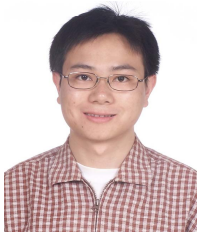
[12] G. Jakimoski and K. Subbalakshmi, "Denial-of-service attacks on dynamic spectrum access networks," in *Proc. IEEE International Conf. Commun.*, May 2008, pp. 524-528.

[13] T. Clancy and N. Goergen, "Security in cognitive radio networks: threats and mitigation," in *Proc. IEEE International Conf. Cognitive Radio Oriented Wireless Netw. Commun.*, May 2008, pp. 1-8.

[14] O. Leon, J. Hernandez-Serrano, and M. Soriano, "A new cross-layer attack to TCP in cognitive radio networks," in *Proc. IEEE International Workshop Cross Layer Design*, June 2009, pp. 1-5.

[15] K. Bian and J. Park, "Security vulnerabilities in IEEE 802.22," in *Proc. International Wireless Internet Conf.*, 2008, pp. 1-9.
[16] R. Chen, J. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2008, pp. 1876-1884.
[17] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *Proc. IEEE International Conf. Commun.*, May 2008, pp. 3406-3410.
[18] W. Wang, H. Li, Y. Sun, and Z. Han, "CatchIt: detect malicious nodes in collaborative spectrum sensing," in *Proc. IEEE Global Commun. Conf.*, Nov. 2009, pp. 1-6.
[19] S. Liu, Y. Chen, W. Trappe, and L. Greenstein "ALDO: an anomaly detection framework for dynamic spectrum access networks," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2009, pp. 675-683.
[20] R. Chen, J. Park, and J. Reed, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *Proc. IEEE Workshop Netw. Technol. Software Defined Radio Netw.*, Sept. 2006, pp. 110-119.
[21] Z. Jin, S. Anand, and K. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *Proc. IEEE International Conf. Commun.*, June 2009, pp. 1-5.
[22] S. Anand, Z. Jin, and K. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in *Proc. IEEE International Dynamic Spectrum Access Netw.*, Oct. 2008, pp. 1-6.
[23] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in *Proc. IEEE International Performance Comput. Commun. Conf.*, Dec. 2009, pp. 208-215.
[24] R. Chen, J. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 25-37, Jan. 2008.
[25] H. Li and Z. Han, "Dogfight in spectrum: jamming and anti-jamming in multichannel cognitive radio systems," in *Proc. IEEE Global Telecommun. Conf.*, Nov. 2009, pp. 1-6.
[26] H. Li and Z. Han, "Blind dogfight in spectrum: combating primary user emulation attacks in cognitive radio systems with unknown channel statistics," in *Proc. IEEE International Conf. Commun.*, May. 2010, pp. 1-6.
[27] F. Digham, M. Alouini, and M. Simon, "On the energy detection of unknown signals over fading channels," in *Proc. IEEE International Conf. Commun.*, May 2003, pp. 3575-3579.
[28] D. Tracy and P. Dwyer, "Multivariate maxima and minima with matrix derivatives," *J. American Statistical Assoc.*, vol. 64, no. 328, pp. 1576-1594, Dec. 1969.
[29] A. Taherpour, M. Nasiri-Kenari, and S. Gazor, "Multiple antenna spectrum sensing in cognitive radios," *IEEE Trans. Wireless Commun.*, vol. 9, no. 2, pp. 814-823, Feb. 2010.
[30] Y. Chen and N. Beaulieu, "Performance of collaborative spectrum sensing for cognitive radio in the presence of channel estimation error," *IEEE Trans. Commun.*, vol. 57, no. 7, pp. 1944-1947, July 2009.
[31] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*, 5th edition. Academic Press, 1994.

Chao Chen received his B.Eng. and M.Eng. degrees from Nanjing University of Posts and Telecommunications(NUPT), Nanjing, China, in 2004 and 2007, both in electrical engineering. He is working towards his Ph.D degree in the department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ. His research interests include wireless communication and networking, routing protocols for wireless ad hoc and sensor networks, wireless network security and cognitive radio technology.



Hongbing Cheng (S'03-M'07) received his B.S. and Ph.D. degrees in Electronic Engineering from Peking University, Beijing, China, in 2002 and 2007, respectively. He is currently a research assistant professor with the Department of ECE, Stevens Institute of Technology, Hoboken, NJ, USA. His research interests include wireless communication theory, communication system design, broadband multiple access techniques, resource allocation for cellular and ad hoc networks, cooperative relay and cognitive radio. He served as a technical session chair in WOCC 2009 and a TPC member in IEEE ICC¡¯10 and IEEE GLOBECOM'08 and was invited as technical reviewers for many technical journals and conferences.

Yu-Dong Yao (S'88-M'88-SM'94'-F'11) has been with Stevens Institute of Technology, Hoboken, New Jersey, since 2000 and is currently a professor and department director of electrical and computer engineering. He is also a director of Stevens' Wireless Information Systems Engineering Laboratory (WISELAB). Previously, from 1989 and 1990, he was at Carleton University, Ottawa, Canada, as a Research Associate working on mobile radio communications. From 1990 to 1994, he was with Spar Aerospace Ltd., Montreal, Canada, where he was involved in research on satellite communications. From 1994 to 2000, he was with Qualcomm Inc., San Diego, CA, where he participated in research and development in wireless code-division multiple-access (CDMA) systems.

He holds one Chinese patent and twelve U.S. patents. His research interests include wireless communications and networks, spread spectrum and CDMA, antenna arrays and beamforming, cognitive and software defined radio (CSDR), and digital signal processing for wireless systems. Dr. Yao was an Associate Editor of IEEE COMMUNICATIONS LETTERS and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and an Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He received the B.Eng. and M.Eng. degrees from Nanjing University of Posts and Telecommunications, Nanjing, China, in 1982 and 1985, respectively, and the Ph.D. degree from Southeast University, Nanjing, China, in 1988, all in electrical engineering.