Channel-Based Detection of Primary User Emulation Attacks in Cognitive Radios

Wen-Long Chin, Chun-Lin Tseng, Chun-Shen Tsai, Wei-Che Kao and Chun-Wei Kao
Department of Engineering Science,
National Cheng Kung University, Tainan, Taiwan.
wlchin@mail.ncku.edu.tw

***Abstract*—Recently, cognitive radio (CR) has recently emerged as a useful technology to improve the efficiency of spectrum utilization. However, wireless networks are accompanied with an important security flaw that they are much easier to be attacked than any wired network. Many security issues are discovered. Within which, the most important one is primary user emulation attack (PUEA). In this work, we propose a method by using the characteristics of wireless channels to identify the PUEA. In the wireless environment, the statistical property of the wireless channel between the receiver and transmitter is unique; therefore, we can use this feature as a radio fingerprint. By employing the capability of spectrum sensing in CR, we can identify primary user emulation attackers via the uniqueness of wireless channels. Compared with conventional security schemes based on higher layer protocols, whose information must be passed to the upper layers, the proposed scheme using physical layer is more efficient in terms of the detection time. Simulations confirm the advantages of the proposed scheme.**

I. Introduction

Wireless communication devices today have led to an urgent requirement for precious radio spectrum[1]. According to the study of Federal Communications Commission (FCC) on the traditional spectrum assignment policy, the utilization of static spectrum allocation at any time and space is between 15% and 85%[2]. This paradox situation can be solved by the emerging dynamic spectrum access (DSA) and cognition communication.

A. Cognitive Radio

Cognition communication is a popular technique, which can improve the spectrum utilization. The concept, proposed by Mitola [3], aims at solving the problem of scarce spectrum and poor allocation. The cognitive radio (CR) user needs to continuously monitor radio spectrum usage, which is used to give precedence to primary user (PU). That is, when PU starts to transmit signals, secondary users (SU) will switch to another spectrum hole.

In past few years, CR has received much attention. However, security issue are rarely discussed. The security issues were first investigated by Burbank [4] and Clancy [5] for cognitive radio networks (CRN).

B. Primary User Emulation Attacks

Malicious users may emulate PUs' signal characteristic, which can subsequently reduce the spectrum utilization. This behavior is named primary user emulation attacks (PUEA)[6]. Discrimination between PUs and SUs is an important ability against PUEA.

C. Related Works

In recent years, some works [7] and [8] address the issue of detection the PUEA in CR. In [7], the authors propose to distinguish the identity of transmitter by the wireless channel characteristic. However, the channel is modeled as a path-loss and large-scale shadowing. In [8], the authors consider sensing the unique physical property over time-invariant channels to differentiate the channel states between transmitters and receivers.

The main contribution of this paper is to distinguish the primary user emulate (PUE) attacker from PU by the channel-based detection. We employ the Neyman-Pearson test in discriminating channel states of transmitters over Rayleigh fading channels. The new scheme using physical layer is more efficient than conventional techniques in terms of the detection time.

D. Organization

Section II introduces the system model. Section III introduces the OFDM model and correlation characteristics and channel power estimation. Section IV presents the proposed Channel-Based Authentication. Section V demonstrates the simulation results. Finally, section V draw conclusions.

II. System Model

A. Scenario

In the multipath environment of wireless communication, the uniqueness of the channel between two locations has been proved in [9]. We seek to develop the concept of physical layer authentication for CR. Figure 1. depicts the scenario of the wireless orthogonal frequency division multiplexing (OFDM). The area in circle is the sensing area of SU. The SU might detect the PU, PUEA or other SUs during the spectrum sensing. Some malicious transmitters can emulate the signal of PU to achieve their selfish aims. The proposed detection method can distinguish the PU from PUEA.

B. Channel Model

In this work, $h(l)$ denotes the lth channel impulse response of multipath channels with $(L+1)$ uncorrelated taps. The wireless channels are assumed to be Rayleigh fading. Based on

978-1-4673-0990-5/12/$31.00 ©2012 IEEE

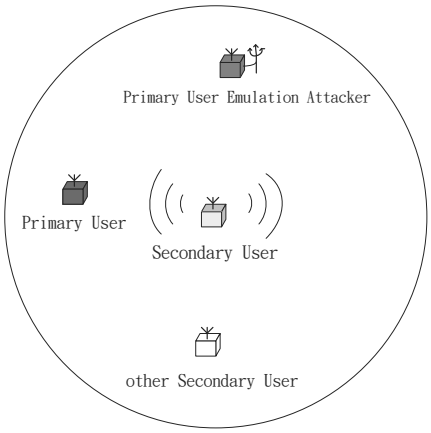

Fig. 1. Scenario of wireless OFDM

the assumption of uncorrelated scattering, the cross-correlation of the channel response can be expressed as

$$\begin{aligned} E\left[h\left(l_1\right)h^*\left(l_2\right)\right] = & \quad E\left[h\left(l_1\right)h^*\left(l_2\right)\right]\delta\left(l_1-l_2\right) \\ = & \quad \sigma^2_{h(l)}|_{l=l_1=l_2} \end{aligned} \tag{1}$$

where $\delta\left(\cdot\right)$ is the Dirac delta function and $\sigma^2_{h(l)} \equiv E\left[\left|h\left(l\right)\right|^2\right]$ is the power of the lth channel tap.

III. Correlation Characteristics Of OFDM And Channel Power Estimation

In the following discussion, since the time-domain correlation characteristics of OFDM symbols are related to neighboring symbols, the signal model will consider three symbols, that is, the previous, the current, and the next symbols. Consider an OFDM with N subcarriers. The complex data were modulated onto the N subcarriers by means of the inverse discrete Fourier transform (IDFT). The CP of length N_{CP} is inserted at the beginning of each OFDM symbol to prevent ISI and preserve the mutual orthogonality of subcarriers. Following serial-to parallel conversion, the current dth OFDM symbol $x_m\left(n\right)$, $n \in \{0,1,\ldots,N+N_{CP}-1\}$, is finally transmitted through a multipath channel $h\left(l\right)$. For $n \notin \{0,1,\ldots,N+N_{CP}-1\}$, $x_m\left(n\right)$ is zero. Due to the CP, the transmitted data have the following characteristics: if $n_2 \notin n_1$ and $n_2 \notin n_1+N$, then the correlation of $x_m\left(n\right)$ is $E\left[x_m\left(n_1\right)x^*_m\left(n_2\right)\right]=0$; otherwise $x_m\left(n\right)$ is $E\left[x_m\left(n_1\right)x^*_m\left(n_2\right)\right]=\sigma^2_x$ where σ^2_x is the signal power and $\left(\cdot\right)^*$ denotes the complex conjugate, m denotes the mth symbol of burst M.

At the receiver, considering the previous OFDM symbol $x_{m-1}\left(n\right)$ of the current symbol, the received sampled data $x_m\left(n\right)$ can be written as

$$\begin{aligned} \tilde{x}_m\left(n\right) &= \sum_{l=0}^{L} h\left(l\right)x_{m-1}\left(n-l\right) \\ &\quad + \sum_{l=0}^{L} h\left(l\right)x_m\left(n-l\right)+\omega\left(n\right) \\ &\quad n=\{0,1,...,N+N_{CP}-1\}. \end{aligned} \tag{2}$$

where $\omega(n)$is the additive white Gaussian noise (AWGN) with zero mean and variance σ^2_ω. Next, to obtain the correlation characteristics of separated-by-N data, $x_m\left(n+N\right)$ for $n \in \{0,1,\ldots,N+N_{CP}-1\}$ should be obtained

$$\begin{aligned} \tilde{x}_m\left(n+N\right) &= \sum_{l=0}^{L} h\left(l\right)x_m\left(n+N-l\right) \\ &\quad + \sum_{l=0}^{L} h\left(l\right)x_{m+1}\left(n+N-l\right)+\omega\left(n\right) \\ &\quad n=\{0,1,\cdots,N+N_{CP}-1\}. \end{aligned} \tag{3}$$

As $x_m\left(n\right)$, $x_{m-1}\left(n\right)$, $x_{m+1}\left(n\right)$, $h(l)$, and $\omega\left(n\right)$ are uncorrelated, the correlation between $\tilde{x}_m\left(n\right)$ and $\tilde{x}_m\left(n+N\right)$ can be expressed as

$$E\left[\tilde{x}_m\left(n\right)\tilde{x}^*_m\left(n+N\right)\right] = \begin{cases} \sigma^2_x \sum\limits_{l=0}^{n-\theta} \sigma^2_{h(l)} & ,n \in I_1 \\ \sigma^2_x \sum\limits_{l=0}^{L} \sigma^2_{h(l)} & ,n \in I_2 \\ \sigma^2_x \sum\limits_{l=n-\theta-N_{CP}+1}^{L} \sigma^2_{h(l)} & ,n \in I_3 \\ 0 & ,n \in I_4 \end{cases} \tag{4}$$

where

$$\begin{aligned} &I_1 \equiv \{0,1,...,L-1\} \\ &I_2 \equiv \{L,L+1,...,N_{CP}-1\} \\ &I_3 \equiv \{N_{CP},N_{CP}+1,...,N_{CP}+L-1\} \\ &I_4 \equiv \{N_{CP}+L,N_{CP}+L+1,...,N_{CP}+N-1\}. \end{aligned} \tag{5}$$

The correlation can be written in a matrix form as

$$\mathbf{r} = \sigma^2_x \mathbf{D}\mathbf{p} \tag{6}$$

where the correlation vector

$$\begin{aligned} \mathbf{r} &= \left[r\left(0\right),r\left(1\right),...,r\left(N+N_{CP}-1\right)\right]^T \\ &\equiv E\left[\tilde{x}_m\left(0\right)\otimes\tilde{x}^*_m\left(N\right)\right] \end{aligned} \tag{7}$$

the $\otimes$ is the Hadamard product.

$$\begin{aligned} \tilde{x}_m\left(i\right) &= \left[\tilde{x}_m\left(i\right),\tilde{x}_m\left(i+1\right),\cdots,\tilde{x}_m\left(i+N+N_{CP}-1\right)\right]^T. \\ \mathbf{p} &= \left[\sigma^2_{h(0)},\sigma^2_{h(1)},\cdots,\sigma^2_{h(L)}\right]^T \end{aligned}$$

$$\mathbf{D} \equiv \begin{bmatrix} \mathbf{D}_1 \\ \mathbf{D}_2 \\ \mathbf{D}_3 \\ \mathbf{D}_4 \end{bmatrix}_{(N+N_{CP})\times(L+1)} \tag{8}$$

$$\mathbf{D}_1 \equiv \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 0 & 1 \end{bmatrix}_{L\times(L+1)} \tag{9}$$

$$\mathbf{D}_2 \equiv \mathbf{1}_{(N_{CP}-L)\times(L+1)} \tag{10}$$

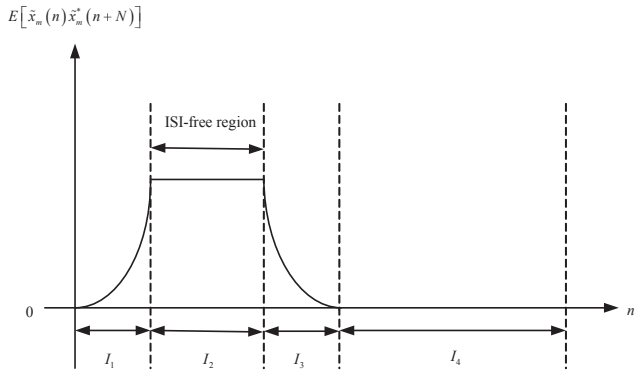

Fig. 2. Correlation characteristics of received separated-by-N data.

$$\mathbf{D}_3 \equiv \begin{bmatrix} 0 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 0 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}_{L\times(L+1)} \tag{11}$$

$$\mathbf{D}_4 \equiv \mathbf{0}_{(N-L)\times(L+1)}. \tag{12}$$

$\mathbf{1}_{(N_{CP}-L)\times(L+1)}$/$\mathbf{0}_{(N-L)\times(L+1)}$ matrix with all-unity/all-zero elements, $(\cdot)^T$ is the transpose. The correlation has the following property.

Property 1: The correlation of separated-by-N samples has the complement property for separated-by-N_{CP} correlations in I_1 and I_3. That is,

$$\begin{aligned} &E\left[\tilde{x}_m(n)\,\tilde{x}_m^*(n+N)\right]+ \\ &E\left[\tilde{x}_m(n+N_{CP})\,\tilde{x}_m^*(n+N+N_{CP})\right] \\ &=Const \qquad \text{for} \quad n\in I_1. \end{aligned} \tag{13}$$

The correlation (4) is illustrated in Fig. 2. Note that actual values depend on the channel-tap gains. Non-zero correlation values of separated-by-N samples are owing to the CP. Due to the linear convolution of the transmitted data with the channel, the length of nonzero correlation values is N_{CP} + L.

Theorem 1: Let $\hat{\mathrm{r}}_{k,m}(n) \equiv \left\langle \tilde{x}_{k,m}(n)\,\tilde{x}_{k,m}^*(n+N)\right\rangle$ be the maximum likelihood estimation of $r_{k,m} \equiv E\left[\tilde{x}_{k,m}(n)\,\tilde{x}_{k,m}(n+N)\right]$ over all symbols within the mth, superscript k denotes the current burst, where $\langle\cdot\rangle$ is the time average over M symbols, then $\hat{\mathrm{r}}_{k,m}(n)$ is asymptotically distributed according to

$$\hat{\mathrm{r}}_k(n) \sim \mathcal{N}_r\left(\mathrm{r}_k(n), \frac{\left(\sigma^2-\mathrm{r}_k^2(n)\right)^2}{M\sigma^2}\right) \tag{14}$$

where $\mathcal{N}_r(\cdot)$ denotes the Gaussian distribution for a real random variable and σ is

$$\begin{aligned} \sigma \quad &\equiv E\left[\left|\tilde{x}_{k,m}(n)^2\right|\right] = E\left[\left|\tilde{x}_{k,m}(n+N)^2\right|\right] \\ &= \sigma_x^2\textstyle\sum_l \sigma_{h_1(l)}^2+\sigma_\omega^2 \end{aligned} \tag{15}$$

According to the (3),the channel-tap power can be obtained by

$$\hat{\mathbf{p}} = \sigma_x^{-2}\mathbf{D}^\dagger\hat{\mathbf{r}}. \tag{16}$$

Since the estimation (16) is a linear combination of Gaussian random variables, the power estimate is also Gaussian distributed with

$$\hat{\mathbf{p}} \sim \mathcal{N}_r\left(\bar{\mathbf{p}}, \mathbf{C}\right) \tag{17}$$

where

$$\bar{\mathbf{p}} \equiv \sigma_x^{-2}E\left[\mathbf{D}^\dagger\hat{\mathbf{r}}\right], \mathbf{C} \equiv \sigma_x^{-4}\mathrm{Cov}\left(\mathbf{D}^\dagger\hat{\mathbf{r}}\right).$$

IV. Channel-Based Authentication

Section III estimates the channel-tap power over the Rayleigh fading channel. In this section, we use the hypothesis test to decide if the transmission terminal is PU or PUEA, i.e.,

$$\begin{aligned} &\mathcal{H}_0 : \hat{\mathbf{p}} \quad \text{is} \quad \text{PU} \\ &\mathcal{H}_1 : \hat{\mathbf{p}} \quad \text{is} \quad \text{PUEA}. \end{aligned} \tag{18}$$

According to (17), the properties of the hypotheses are

$$\begin{aligned} &\mathcal{H}_0 : \hat{\mathbf{p}} \sim \mathcal{N}\left(\mathbf{p}_\mathrm{I}, \mathbf{C}_\mathrm{I}\right) \\ &\mathcal{H}_1 : \hat{\mathbf{p}} \sim \mathcal{N}\left(\mathbf{p}_\mathrm{A}, \mathbf{C}_\mathrm{A}\right) \end{aligned} \tag{19}$$

where superscripts I and A denote PU and PUEA, respectively, $\mathbf{C}$ denotes the coveriance matrix. The likelihood ratio test(LRT) can be expressed as

$$\begin{aligned} \Lambda &= \tfrac{f(\hat{\mathbf{p}}|\mathcal{H}_1)}{f(\hat{\mathbf{p}}|\mathcal{H}_0)} \\ &= \sqrt{\tfrac{\det(\mathbf{C}_\mathrm{I})}{\det(\mathbf{C}_\mathrm{A})}} \times \exp\{\tfrac{1}{2}\left(\hat{\mathbf{p}}-\mathbf{p}_\mathrm{I}\right)^T\mathbf{C}_\mathrm{I}^{-1}\left(\hat{\mathbf{p}}-\mathbf{p}_\mathrm{I}\right) \\ &\quad -\left(\hat{\mathbf{p}}-\mathbf{p}_\mathrm{A}\right)^T\mathbf{C}_\mathrm{A}^{-1}\left(\hat{\mathbf{p}}-\mathbf{p}_\mathrm{A}\right)\} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta_1 \end{aligned} \tag{20}$$

where η_1 is threshold. The Log-Likelihood ratio test (LLRT) can be expressed as

$$\begin{aligned} \zeta &= \log\left(\sqrt{\tfrac{\det(\mathbf{C}_\mathrm{I})}{\det(\mathbf{C}_\mathbf{A})}}\right)+ \\ &\quad \tfrac{1}{2}\hat{\mathbf{p}}^\mathbf{T}\left(\mathbf{C}_\mathbf{I}^{-1}-\mathbf{C}_\mathbf{A}^{-1}\right)\hat{\mathbf{p}}+\hat{\mathbf{p}}^\mathbf{T}\left(\mathbf{C}_\mathbf{A}^{-1}\mathbf{p}_\mathbf{A}-\mathbf{C}_\mathbf{I}^{-1}\mathbf{p}_\mathbf{I}\right)+ \\ &\quad \tfrac{1}{2}\left(\mathbf{p}_\mathbf{I}^\mathbf{T}\mathbf{C}_\mathbf{I}^{-1}\mathbf{p}_\mathbf{I}-\mathbf{p}_\mathbf{A}^\mathbf{T}\mathbf{C}_\mathbf{A}^{-1}\mathbf{p}_\mathbf{A}\right) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta_2. \end{aligned} \tag{21}$$

According to (14) and (15), and the approximation of $\mathbf{C}_\mathrm{I} \approx \mathbf{C}_\mathrm{A} \equiv \mathbf{C}$, under the low SNR case, (21) can be determined as

$$\begin{aligned} \zeta &= \hat{\mathbf{p}}^T\left(\mathbf{C}^{-1}\mathbf{p}_\mathrm{A}-\mathbf{C}^{-1}\mathbf{p}_\mathrm{I}\right)+\frac{1}{2}\left(\mathbf{p}_\mathrm{I}^T\mathbf{C}^{-1}\mathbf{p}_\mathrm{I}-\mathbf{p}_\mathrm{A}^T\mathbf{C}^{-1}\mathbf{p}_\mathrm{A}\right) \\ &= \hat{\mathbf{p}}^T\mathbf{C}^{-1}\left(\mathbf{p}_\mathrm{A}-\mathbf{p}_\mathrm{I}\right)-\frac{1}{2}\left(\mathbf{p}_\mathrm{A}+\mathbf{p}_\mathrm{I}\right)^T\mathbf{C}^{-1}\left(\mathbf{p}_\mathrm{A}-\mathbf{p}_\mathrm{I}\right) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta_2. \end{aligned} \tag{22}$$

The detection process is illustrated in Fig. 3.. According to (19) and (22), under the two hypotheses, we have

$$\begin{aligned} &\mathcal{H}_0 : \zeta \sim \mathcal{N}\left(m_0, \sigma_\zeta^2\right) \\ &\mathcal{H}_1 : \zeta \sim \mathcal{N}\left(m_1, \sigma_\zeta^2\right) \end{aligned} \tag{23}$$

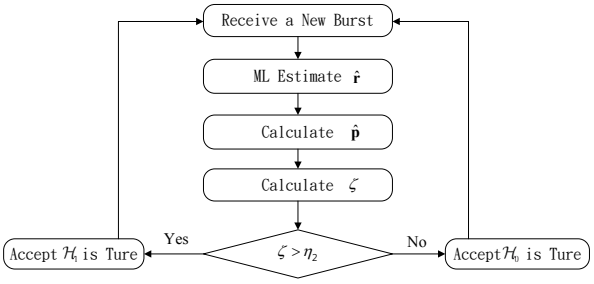

Fig. 3. Detection process.

where

$$
\begin{aligned}
m_0 &= \frac{1}{2}\left(\mathbf{p}_{\mathrm{I}}-\mathbf{p}_{\mathrm{A}}\right)^T \mathbf{C}^{-1}\left(\mathbf{p}_{\mathrm{A}}-\mathbf{p}_{\mathrm{I}}\right) \\
m_1 &= \frac{1}{2}\left(\mathbf{p}_{\mathrm{A}}-\mathbf{p}_{\mathrm{I}}\right)^T \mathbf{C}^{-1}\left(\mathbf{p}_{\mathrm{A}}-\mathbf{p}_{\mathrm{I}}\right) \\
\sigma_\zeta^2 &= \left(\mathbf{p}_{\mathrm{A}}-\mathbf{p}_{\mathrm{I}}\right)^T \mathbf{C}^{-1}\left(\mathbf{p}_{\mathrm{A}}-\mathbf{p}_{\mathrm{I}}\right).
\end{aligned} \tag{24}
$$

We consider the Neyman-Pearson detector to achieve the constant false alarm (CFAR) rate. For a Gaussian random variable $x \sim \mathcal{N}(m_x, \sigma_x^2)$, one has

$$
P\left(x \geq \eta\right) = \frac{1}{2}\mathrm{erfc}\left(\frac{\eta - m_x}{\sqrt{2}\sigma_x}\right) \tag{25}
$$

where erfc(.) is the complementary error function. Using (25), the false alarm probability P_{fa} is given by

$$
\begin{aligned}
P_{fa} &= P\left(\zeta \geq \eta_2 | \mathcal{H}_0\right) \\
&= \frac{1}{2}\mathrm{erfc}\left(\frac{\eta_2 - m_0}{\sqrt{2}\sigma_\zeta}\right).
\end{aligned} \tag{26}
$$

Thus the threshold at the detector can be calculated as

$$
\eta_2 = \sqrt{2}\sigma_\zeta \mathrm{erfc}^{-1}\left(P_{fa}\right) + m_0. \tag{27}
$$

Finally, the probability of detection P_d is given by

$$
\begin{aligned}
P_d &= P\left(\zeta \geq \eta_2 | \mathcal{H}_1\right) \\
&= P\left(\zeta \geq \sqrt{2}\sigma_\zeta \mathrm{erfc}^{-1}\left(P_{fa}\right) + m_0 | \mathcal{H}_1\right) \\
&= \frac{1}{2}\mathrm{erfc}\left(\frac{\eta_2 - m_1}{\sqrt{2}\sigma_\zeta}\right) \\
&= \frac{1}{2}\mathrm{erfc}\left(\frac{\sqrt{2}\sigma_\zeta \mathrm{erfc}^{-1}\left(P_{fa}\right) + m_0 - m_1}{\sqrt{2}\sigma_\zeta}\right).
\end{aligned} \tag{28}
$$

V. Simulations

Monte Carlo simulations are conducted to evaluate the performance of the detector. An OFDM system with N = 64 and N_{CP} = 16 is considered. The simulated modulation scheme is QPSK. The signal bandwidth is 0.8 MHz, and the radio frequency is 2.4 GHz. The subcarrier spacing is 12.5 kHz. The OFDM symbol duration is 80 μs. The channel taps are randomly generated using independent zero−mean and unity-variance complex Gaussian variables.

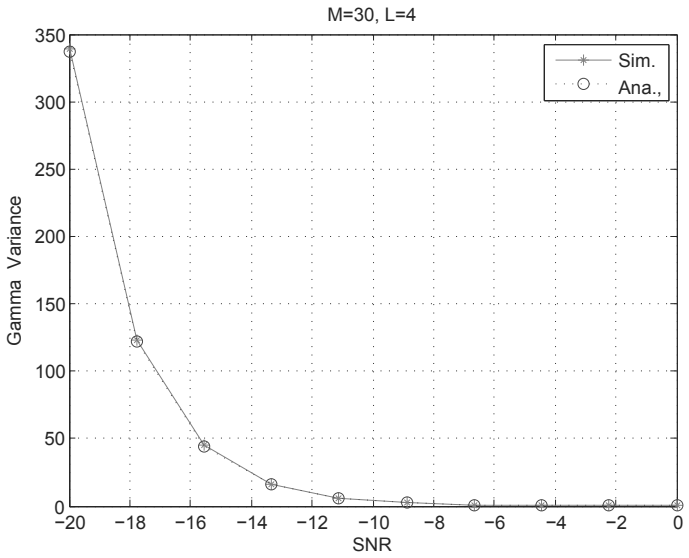

Fig. 4. The simulation of var($\hat{\mathbf{r}}$) , theoretical analysis and simulation results are close.

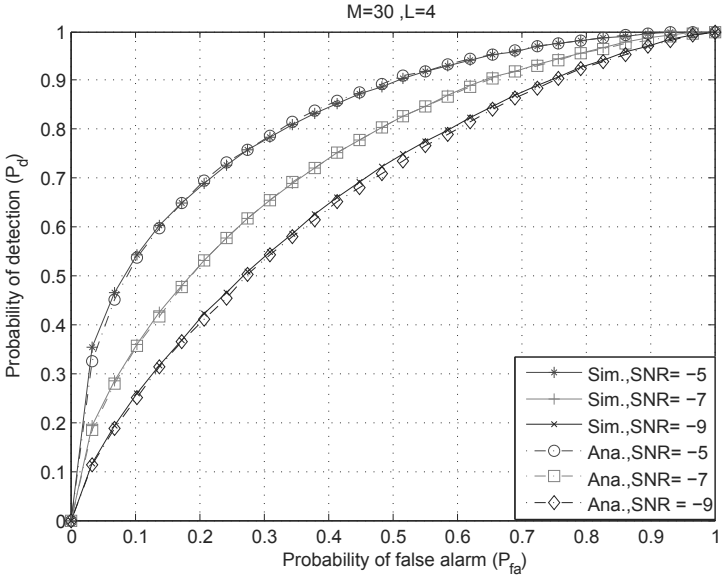

Fig. 5. The detection performance under different SNR case.

Figure 4. shows the variance of $\hat{\mathbf{r}}$ under various SNRs. As shown, when SNR increases, the estimate of the variance of $\hat{\mathbf{r}}$ is less influenced by noise than low SNRs.

Figure 5. plots the probability of detection as a function of probability of false-alarm under various SNRs and M = 30. The influence of SNR on P_d resembles that of M. For a given M, when P_{fa} increases, P_d also increases. It must be noted that the performance can be improved by increasing SNR.

Figure 6. plots the detection probability as a function of false-alarm probability under various M and SNR = -5(dB).

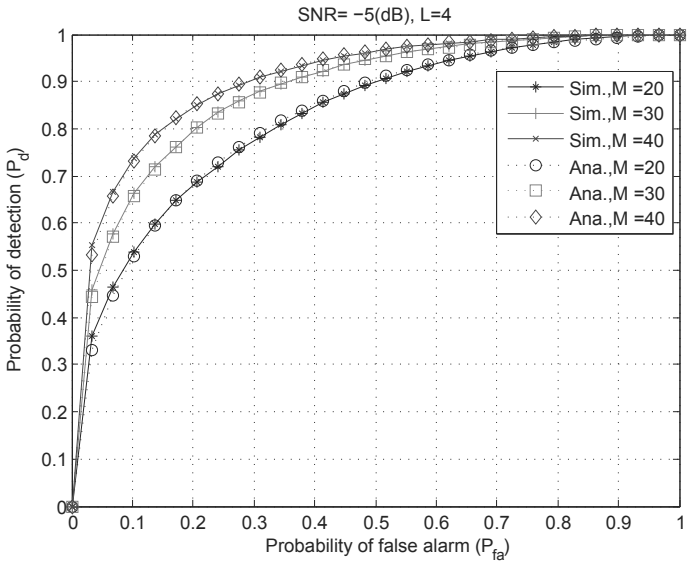

Fig. 6. The detection performance under different M case.

As shown, when M increases, for a given P_{fa}, P_d increases accordingly.

VI. Conclusion

In this paper, we propose a new method to against the PUEA in CRN. The uniqueness of channel-tap powers between the receiver and transmitter is utilized. Simulations indicate that the proposed anti-PUEA technique has good performance. Accordingly, the proposed technique can identify the transmitters to defend against PUEA. The proposed scheme using physical layer is more efficient than conventional techniques in terms of detection time. In the future, we will study a cooperative detection method and analyze more wireless attacks by using the features of wireless channels.

References

[1] S. Haykin, "Cognitive radio: brain-empowered wireless communication," *IEEE Jorunal in Selected Areas in Commun.,* vol. 23, no. 2, pp. 201-220, Feb. 2005.

[2] Federal Communications Commission, Cognitive Radio Technologies Proceeding (CRTP), ET Ducket 03-108 [Online]. Available: http://www.fcc.gov/oet/cognitiveradio/

[3] J. Mitola III, *Cognitive radio: Anintegrated agent architecture for software defined radio.* Ph. D. dissertation, KTH, Stockholm, Sweden, May 2000.

[4] J. L. Burbank, "Security in cognitive radio networks: the required evolution in approaches to wireless network security," *IEEE Cognitive Radio Oriented Wireless Networks and Communications(Crown COM.)*, pp. 1-7, May 2008.

[5] T. C. Clancy, N. Goergen, "Security in cognitive radio networks: threats and mitigation," *IEEE Cognitive Radio Oriented Wireless Networks and Communications(Crown COM.)*, pp. 1-8, May 2008.

[6] R. Chen, J. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1,pp. 25-37, Jan. 2008.

[7] Z.Chen, T. Cooklev, C. Chen, P. R. Carlos, " Modeling primary user emulation attacks and defenses in cognitive radio networks," *IEEE Performance Computing and Communications Conference (IPCCC)*, pp.208-215, Dec. 2009.

[8] C. Zhao, L. Xie, X. Jiang, L. Huang, Y. Yao, "A PHY-layer authentication approach for transmitter identification in cognitive radio networks," *IEEE Communications and Mobile Computing (CMC)*, vol.2, pp.154-158, Apr. 2010.

[9] J. K. Tugnait and H. Kim, "A channel-based hypothesis testing approach to enhance user authentication in wireless networks," *IEEE Communication Systems and Networks (COMSNETS)*, pp. 1-9, 2010.