Cross-Layer Design for Primary User Emulation Attacks Detection in Mobile Cognitive Radio Networks

Trong Nghia Le, *Student Member, IEEE*, Wen-Long Chin, *Senior Member, IEEE*, and Wei-Che Kao

Abstract—In this letter, the channel-tap power is utilized as a radio-frequency fingerprint (RF) to completely identify primary user emulation attacks (PUEAs) over multipath Rayleigh fading channels. To accurately know identities of primary users (PUs) and PUEAs, the cross-layer intelligent learning ability of a mobile secondary user (SU) is exploited to establish detection databases by seamlessly combining the quick detection of physical (PHY) layer with the accuracy of higher layer authentication. The proposed method helps PHY layer completely detect the identities of PUs and PUEAs. For SNR = -2 dB and the false alarm probability of 0.1, the SU can detect a PUEA with the detection probability of 0.9673 under the mobile speed of 70 km/h.

***Index Terms*—Channel-tap power, cross-layer design, primary user emulation attacks (PUEAs).**

I. Introduction

THE concept of cognitive radio (CR) was proposed to solve the problem of scarce spectrum and poor allocation of traditional spectrum policies. CR users or legitimate secondary users (SUs) use spectrum sensing technologies to detect vacant spectrum of primary users (PUs) and utilize them opportunistically, increasing the efficiency of spectrum usage. Various spectrum sensing technologies, such as matched filter detection, energy detection, cyclostationary feature detection, and intelligent detection [1], have been proposed. When a SU is using vacant spectrum of PU and detects the presence of PU signals, it must immediately switch to another idle spectral hole. However, malicious SUs may emulate the signal of PUs, referred to as primary user emulation attacks (PUEAs), with the aims of obtaining higher access priority or degrading the performance of the whole CR networks. This property is a new vulnerability in CR networks, because the spectrum sensing technologies are unable to differentiate the identities of PUs and PUEAs.

To overcome this vulnerability, recently, the physical (PHY) layer detection [2]-[4] and higher layer authentication [5] schemes have been separately developed to identify PUEAs. Z. Chen *et al.* considered energy based mechanism [2], which employs the path loss and the log-normal shadowing of a communication channel to detect the presence of PUEA. However, the authors assume that the locations of PUs, PUEAs and SUs are fixed. To improve the performance of detection in fading environment, the work [3] utilized the channel-tap power as a radio-frequency fingerprint (RF), which is a one-to-one relation between transmitters (Txs) and SU, to directly detect PUEAs and PUs via PHY layer. Although different users can be distinguished, it is still impossible to exactly tell identity of a Tx as PU or PUEA. The detection time of PHY layer is typically more efficient than that of conventional techniques based on higher layer protocols. Recently, Liu *et al.* proposed a PU authentication system [4] at PHY layer without using hypothesis test. Nevertheless, it depends on the authentication information from a helper node, which uses cryptographic signatures to authenticate signals of PU.

As an improvement, in [5], the authors proposed PU authentication mechanism based on public key cryptography that is used as digital signatures by the higher layer protocols. The PU encrypts its identification with its private key and appends the encrypted signature to its transmission. Since only the PU knows its private key, malicious SUs cannot produce a valid signature to emulate the PU. As a result, the higher layer authentication is hard to break and can obtain accurate identification of PUEAs and PUs. However, a continuous application of cryptographic signatures will lead to substantial overheads on SUs as well as CR networks, because the higher layer authentication is considered to be energy inefficient, heavy computation, and time consuming.

In this letter, to completely identify PUEAs and PUs at PHY layer over multipath Rayleigh fading channels [6] in mobile CR networks, a cross-layer intelligent learning ability of SU is exploited to establish RF databases by seamlessly combining the accuracy and ability of higher layer authentication [5] with the quick detection of PHY layer. The proposed cross-layer design not only differentiates different Txs, but also exactly tells the identity of a Tx as either a PU or a PUEA by using the PHY layer. To the best of our knowledge, this important issue has not been disclosed in previous works. Simulations confirm the advantages of the proposed detection method.

II. System Model

A. Channel Model

Our system consists of a set of PUs, SUs and PUEAs, coexisting within a mobile CR network based on orthogonal frequency-division multiplexing (OFDM) with N subcarriers using burst-mode transmission that includes M consecutive symbols. Some malicious Txs (PUEAs) can emulate the signal of PUs to achieve their selfish aims. In this letter, $h_m(n,l)$ denotes the lth channel impulse response of multipath channels at time n with (L+1) uncorrelated taps, undergone by the mth OFDM symbol. Based on the assumption of wide-sense stationary and uncorrelated scattering, the cross-correlation of

Manuscript received Oct. 31, 2014; revised December 26, 2015; accepted January 31, 2015. This work is supported in part by the grant MOST 103-2221-E-006-082, Taiwan.

Trong Nghia Le is with Le Quy Don Technical University, Hanoi, Vietnam (email: nghiahp79@gmail.com). Wen-Long Chin and Wei-Che Kao are with National Cheng Kung University, Tainan 701, Taiwan, ROC (email: wlchin@mail.ncku.edu.tw; speakfool4@hotmail.com).

the channel response within a symbol can be expressed as

$$\begin{aligned} E[h_m(n_1,l_1)h_m^*(n_2,l_2)] &= E[h_m(n_1,l_1)h_m^*(n_2,l_2)]\delta(l_1-l_2) \\ &= J_0(\beta\Delta)\sigma^2_{h_m(l)}|_{l=l_1=l_2} \end{aligned} \quad (1)$$

where $\delta(\cdot)$ is the Dirac delta function; $J_0(\cdot)$ is the zeroth-order Bessel function of the first kind; $\Delta \equiv n_2 - n_1$; $\sigma^2_{h_m(l)} \equiv E\left[|h_m(l)|^2\right]$ is the lth channel-tap power, and $\beta = 2\pi f_d T_s$, f_d is the maximum Doppler shift, T_s is the sampling interval.

The complex data are modulated onto the N subcarriers by means of the inverse discrete Fourier transform (IDFT). A cyclic prefix (CP) of length N_{CP} is inserted at the beginning of each OFDM symbol to prevent intersymbol interference (ISI) and preserve the mutual orthogonality of subcarriers. Following serial-to-parallel conversion, the current mth OFDM symbol $x_m(n)$, $n \in \{0, 1, \ldots, N + N_{CP} - 1\}$, is finally transmitted through a multipath channel $h_m(n,l)$. Because of CP, the transmitted data have the following characteristics: if $n_2 \neq n_1$ and $n_2 \neq n_1 + N$, then the correlation of $x_m(n)$ is $E[x_m(n_1)\, x_m^*(n_2)] = 0$; otherwise $E[x_m(n_1)\, x_m^*(n_2)] = \sigma_x^2$, where σ_x^2 is the signal power on the transmitter side.

B. Channel-Tap Power Estimation

From [3], on the receiver (SU) side, the correlation between the received sampled current data $\tilde{x}_m(n)$ and separated-by-N data $\tilde{x}_m(n+N)$ can be written is a vector form as

$$\mathbf{r} = \sigma_x^2 J_0(\beta N)\mathbf{D}\mathbf{p} = \mu\mathbf{D}\mathbf{p} \quad (2)$$

where $\mathbf{p} = \left[\sigma^2_{h_m(0)}, \sigma^2_{h_m(1)}, \cdots, \sigma^2_{h_m(L)}\right]^T$ is the transpose vector of channel tap-powers; $\mathbf{D}$ is a matrix with unity and zero elements [3], and $\mu = \sigma_x^2 J_0(\beta N)$ is a constant when the coherence time is larger than the symbol duration. From (2), the channel-tap power estimation of Tx, $\hat{\mathbf{p}}$, can be obtained

$$\hat{\mathbf{p}} = \mu^{-1}\mathbf{D}^\dagger\hat{\mathbf{r}} \quad (3)$$

where $\mathbf{D}^\dagger$ denotes the pseudo-inverse of $\mathbf{D}$ and $\hat{\mathbf{r}}$ is the maximum likelihood estimate of $\mathbf{r}$ with Gaussian distribution [3]. Since the estimate (3) is a linear combination of $\hat{\mathbf{r}}$, $\hat{\mathbf{p}}$ is also Gaussian distribution with

$$\hat{\mathbf{p}} \sim \mathcal{N}_r(\bar{\mathbf{p}}, \mathbf{C}) \quad (4)$$

where $\bar{\mathbf{p}} \equiv \mu^{-1}E\left[\mathbf{D}^\dagger\hat{\mathbf{r}}\right]$ and $\mathbf{C} \equiv \mu^{-2}\mathrm{Cov}\left(\mathbf{D}^\dagger\hat{\mathbf{r}}\right)$ are the mean vector and covariance matrix of $\hat{\mathbf{p}}$, respectively, and $\mathcal{N}_r$ represents the Gaussian distribution for a real random variable.

III. PROPOSED CROSS-LAYER AUTHENTICATION

A. Constructing Fingerprint Databases for Identification

The mobility of Tx and SU pairs leads to variation of channel-tap powers; however, its statistical parameters $(\bar{\mathbf{p}}, \mathbf{C})$ do not change within the channel coherent time interval, which are utilized as the RFs to detect PUs and PUEAs. To initialize RF databases, the SU utilizes the higher-layer authentication in [5] to identify PUs and PUEAs accurately. Then the SU determines $\hat{\mathbf{p}}$ of PUs and PUEAs using (3) and records their statistics in PU and PUEA databases, respectively. The PU and PUEA databases compose of the FPs of all PUs and PUEAs, i.e. $\left(\bar{\mathbf{p}}_j^I, \mathbf{C}_j^I\right)$ and $\left(\bar{\mathbf{p}}_k^A, \mathbf{C}_k^A\right)$, respectively, where $j = 1, ..., J$, $k = 1, ..., K$, J and K are the numbers of PUs and PUEAs, and superscripts I and A refer to PU and PUEA, respectively. For simplicity, $\mathbf{C}_j^I \approx \mathbf{C}_k^A \equiv \mathbf{C}$ in low signal-to-noise ratio (SNR). These databases are initially established by higher layer authentication, updated and tracked by PHY layer.

Owing to the time-varying property of wireless channels that become uncorrelated after the channel coherence time [6], the use of out-of-date RFs in the databases raises the false alarm probability of the channel-based detection method. Therefore, we use a timer for each record, and delete the out-of-date RFs of PU and PUEA in the databases. Once the timer exceeds the maximum lifetime, which should be less than the channel coherence time, the SU will estimate a new channel-tap power and compute $(\bar{\mathbf{p}}, \mathbf{C})$. The maximum lifetime is configured as approximately the inverse of Doppler frequency [6].

The fingerprint of PUEA k in the database is $\bar{\mathbf{p}}_k^A$, which is a vector including N_{CP} elements, namely $\bar{p}_k^A(i), i = 0, 1, \ldots, N_{CP} - 1$. If we denote b as the number of bits used to quantize each element $\bar{p}_k^A(i)$, then the memory size of each fingerprint is $b \times N_{CP}$ bits, where $\times$ denotes the multiplication. Hence, the memory capacity for PUEA database at the SU is $K \times b \times N_{CP}$ bits. Similarly, the memory capacity for PU database is $J \times b \times N_{CP}$ bits. Thus, the overall memory capacity is linearly proportional to the number of PUs and PUEAs, i.e. $b \times N_{CP} \times (J + K)$ bits.

B. Resemblance Test Using Channel-Tap Power Estimation

After the SU determines $\hat{\mathbf{p}}$, it checks whether PU and PUEA databases exist fingerprints of PUs and PUEAs that resemble the property of $\hat{\mathbf{p}}$. The resemblance test for the PUEA database is similar to that for the PU database. To check whether the property of $\hat{\mathbf{p}}$ resembles RFs of PUEAs stored in its database, say PUEA k with RF $\bar{\mathbf{p}}_k^A$, the SU correlates $\hat{\mathbf{p}}$ with $\bar{\mathbf{p}}_k^A$ by a threshold κ. Let a transformation be applied to each entry,

$$\hat{\mathbf{p}}_t = \mathbf{C}^{-1/2}(\hat{\mathbf{p}} - \bar{\mathbf{p}}_k^A) \quad (5)$$

where $\mathbf{C}^{-1/2}$ is the inverse matrix of $\mathbf{C}^{1/2}$ that is given by $\mathbf{C} = \mathbf{C}^{1/2}\left(\mathbf{C}^{1/2}\right)^T$. The channel length is assumed to be N_{CP} without any need to estimate L, such that $\hat{\mathbf{p}}_t$ has N_{CP} uncorrelated elements that are normally distributed. An element in $\hat{\mathbf{p}}_t$, say $\hat{p}_t(i)$, belongs to the PUEA k with a confidence interval $P(|\hat{p}_t(i)| < \kappa) = \nu$, where $P(\cdot)$ denotes the probability, $\kappa = Q^{-1}((1-\nu)/2)$, and $Q^{-1}(\cdot)$ is the inverse Q function. Since $\hat{\mathbf{p}}_t$ has N_{CP} i.i.d elements, the probability that $\hat{\mathbf{p}}_t$ belongs to the PUEA k is

$$\begin{aligned} &P(|\hat{p}_t(0)| < \kappa, |\hat{p}_t(1)| < \kappa, \ldots, |\hat{p}_t(N_G - 1)| < \kappa) \\ &\qquad = \prod_{i=0}^{N_{CP}-1} P(|\hat{p}_t(i)| < \kappa) = \nu^{N_{CP}} \end{aligned} \quad (6)$$

If $|\hat{p}_t(i)| < \kappa, \forall i$, $\hat{\mathbf{p}}$ passes the resemblance test for the PUEA k, which means that Tx resembles the PUEA k. The set of all users in the PUEA database passing (6) is denoted by $\mathcal{A}_{pass}$.

Similarly, the resemblance test for the PU j can be obtained as (6) by replacing $\bar{\mathbf{p}}_k^A$ in (5) with $\bar{\mathbf{p}}_j^I$ that is fingerprint of the PU j stored in the PU database. The set of all users in the PU database passing (6) is denoted by $\mathcal{I}_{pass}$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LCOMM.2015.2399920, IEEE Communications Letters

C. Tx Authentication and Database Update

Figure 1 illustrates the proposed cross-layer assisted decision flow. After the SU performs the resemblance test for the Tx by correlating $\hat{\mathbf{p}}$ with the fingerprint of all users stored in the PU and PUEA databases, it makes a binary decision D^I and $D^A \in \{0, 1\}$, respectively, as follows,

$$D^I = \begin{cases} 1, \text{if } \mathcal{I}_{pass} \neq \emptyset \\ 0, \text{otherwise} \end{cases} \tag{7}$$

where $\emptyset$ is an empty set, which denotes that no RFs of users in the PU database pass (6). When $D^I = 1$, the SU must find a PU that best matches the Tx. This PU is chosen by searching over RFs of PUs in the $\mathcal{I}_{pass}$ and satisfied the condition

$$j^* = \underset{\{\forall j \in \mathcal{I}_{pass}\}}{\arg\min} \left| \bar{\mathbf{p}}_j^I - \hat{\mathbf{p}} \right| \tag{8}$$

The RF of the best match of PU j^* is $\bar{\mathbf{p}}_{j^*}^I$. Similarly, when $D^A = 1$, the SU finds a PUEA that best matches the Tx,

$$k^* = \underset{\{\forall k \in \mathcal{A}_{pass}\}}{\arg\min} \left| \bar{\mathbf{p}}_k^A - \hat{\mathbf{p}} \right| \tag{9}$$

The RF of the best match of PUEA k^* is $\bar{\mathbf{p}}_{k^*}^A$. Next, the SU combines D^I and D^A to decide the use of higher layer authentication or PHY layer detection as follows,

$$D^I D^A = \begin{cases} 00, \text{perform higher layer authentication} \\ 01, \text{Tx is determined as the PUEA } k^* \\ 10, \text{Tx is determined as the PU } j^* \\ 11, \text{perform the channel-based detection} \end{cases} \tag{10}$$

There are 4 possible outcomes. 1) $D^I D^A = 01$, only $\mathcal{A}_{pass} \neq \emptyset$. The PHY layer decides the Tx as the PUEA k^* and updates the fingerprint of PUEA k^* by fingerprint of Tx. 2) $D^I D^A = 10$, only $\mathcal{I}_{pass} \neq \emptyset$. The PHY layer decides the Tx as the PU j^* and updates the fingerprint of PU j^* by fingerprint of Tx. 3) $D^I D^A = 00$, $\mathcal{I}_{pass} = \emptyset$ and $\mathcal{A}_{pass} = \emptyset$, the property of $\hat{\mathbf{p}}$ doesn't resemble any fingerprint of users stored in both PU and PUEA databases. The SU invokes higher layer authentication [5] to accurately identify Tx as a PU or a PUEA and stores the updated statistics of $\hat{\mathbf{p}}$ in the PU or PUEA databases, respectively. Hence, for subsequent detection, as the property of $\hat{\mathbf{p}}$ resembles the fingerprint stored in the databases, the SU only uses the PHY layer detection method without the need to invoke higher layer authentication again. 4) Otherwise, the SU uses channel-based detection by PHY layer to detect the Tx as the PUEA k^* or the PU j^* introduced in the next subsection. Similarly, PHY layer also stores the update-to-date statistics of $\hat{\mathbf{p}}$ in the PU or PUEA databases, enabling the variation of wireless channels to be tracked.

By using the cross-layer design, the SU can significantly reduce the workload of the higher layer authentication. Moreover, the PHY layer can completely detect Tx as a PUEA or a PU because RF of new Txs is supplemented in the detection databases established by the higher layer authentication.

D. Channel-based detection by PHY layer

As $D^I D^A = 11$, the PHY layer employs the hypothesis test to determine whether the Tx is the PU j^* or the PUEA k^*,

$$\begin{cases} \mathcal{H}_0 : \hat{\mathbf{p}} \text{ belongs to the PU } j^* \\ \mathcal{H}_1 : \hat{\mathbf{p}} \text{ belongs to the PUEA } k^* \end{cases} \tag{11}$$

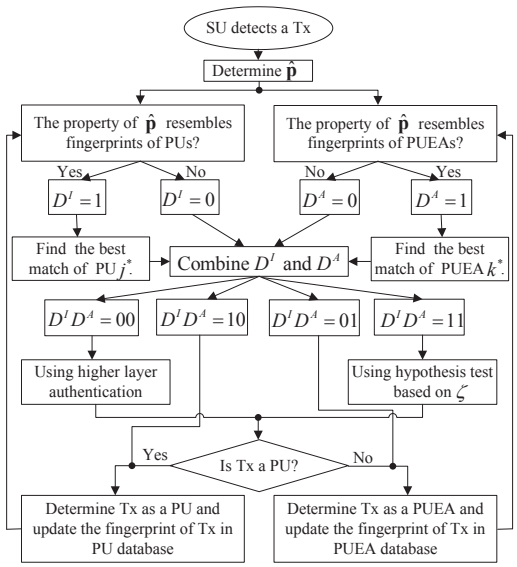

Fig. 1. Cross-layer assisted decision flow used in PU and PUEA detection.

From (4), the properties of the hypotheses are

$$\begin{cases} \mathcal{H}_0 : \hat{\mathbf{p}} & \sim & \mathcal{N}_r \left(\bar{\mathbf{p}}_{j^*}^I, \mathbf{C} \right) \\ \mathcal{H}_1 : \hat{\mathbf{p}} & \sim & \mathcal{N}_r \left(\bar{\mathbf{p}}_{k^*}^A, \mathbf{C} \right) \end{cases} \tag{12}$$

The SU utilizes the log-likelihood ratio (LLR) test of $\hat{\mathbf{p}}$ in [3] to differentiate Tx as the PU or PUEA as follows,

$$\begin{aligned} \zeta = & \ \hat{\mathbf{p}}^T \mathbf{C}^{-1} \left(\bar{\mathbf{p}}_{k^*}^A - \bar{\mathbf{p}}_{j^*}^I \right) \\ & - \frac{1}{2} \left(\bar{\mathbf{p}}_{k^*}^A + \bar{\mathbf{p}}_{j^*}^I \right)^T \mathbf{C}^{-1} \left(\bar{\mathbf{p}}_{k^*}^A - \bar{\mathbf{p}}_{j^*}^I \right) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta \end{aligned} \tag{13}$$

where η is a decision threshold. Since ζ is a linear combination of $\hat{\mathbf{p}}$, so according to (12), it is distributed as

$$\begin{cases} \mathcal{H}_0 : \zeta \sim \mathcal{N}_r \left(m_0, \sigma_\zeta^2 \right) \\ \mathcal{H}_1 : \zeta \sim \mathcal{N}_r \left(m_1, \sigma_\zeta^2 \right) \end{cases} \tag{14}$$

where

$$\begin{aligned} m_0 &= \frac{1}{2} \left(\bar{\mathbf{p}}_{j^*}^I - \bar{\mathbf{p}}_{k^*}^A \right)^T \mathbf{C}^{-1} \left(\bar{\mathbf{p}}_{k^*}^A - \bar{\mathbf{p}}_{j^*}^I \right) \\ m_1 &= \frac{1}{2} \left(\bar{\mathbf{p}}_{k^*}^A - \bar{\mathbf{p}}_{j^*}^I \right)^T \mathbf{C}^{-1} \left(\bar{\mathbf{p}}_{k^*}^A - \bar{\mathbf{p}}_{j^*}^I \right) \\ \sigma_\zeta^2 &= \left(\bar{\mathbf{p}}_{k^*}^A - \bar{\mathbf{p}}_{j^*}^I \right)^T \mathbf{C}^{-1} \left(\bar{\mathbf{p}}_{k^*}^A - \bar{\mathbf{p}}_{j^*}^I \right) \end{aligned} \tag{15}$$

The Neyman-Pearson detector is adopted to achieve a constant false alarm rate, P_{fa}, which is given by

$$P_{fa} = P \left(\zeta \geq \eta | \mathcal{H}_0 \right) = \frac{1}{2} \text{erfc} \left(\frac{\eta - m_0}{\sqrt{2}\sigma_\zeta} \right) \tag{16}$$

where $\text{erfc}(\cdot)$ is the complementary error function. Therefore, the threshold at the detector can be calculated as

$$\eta = \sqrt{2}\sigma_\zeta \text{erfc}^{-1} \left(2P_{fa} \right) + m_0 \tag{17}$$

Let S denote the event that Tx is identified as a PUEA. The probability of PUEA detection using the hypothesis test,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LCOMM.2015.2399920, IEEE Communications Letters

$P(S|D^I D^A = 11) \equiv P_d$, is given by

$$P_d = P\left(\zeta \geq \eta | \mathcal{H}_1\right) = \frac{1}{2}\text{erfc}\left(\frac{\eta - m_1}{\sqrt{2}\sigma_\zeta}\right) \tag{18}$$

E. Probability of Detection Using Cross-layer

The overall PUEA detection probability using cross-layer is

$$\begin{aligned} P(S) = & P(D^I D^A = 00)P(S|D^I D^A = 00) \\ & + P(D^I D^A = 11)P(S|D^I D^A = 11) \\ & + P(D^I D^A = 01)P(S|D^I D^A = 01) \\ & + P(D^I D^A = 10)P(S|D^I D^A = 10) \end{aligned} \tag{19}$$

where $P(S|D^I D^A = 00)$ and $P(S|D^I D^A = 01)$ are the probability of PUEA detection using higher layer authentication and PHY layer detection that $\hat{\mathbf{p}}$ only resembles fingerprints of users in PUEA database, respectively, which are equal 1. $P(S|D^I D^A = 10)$ refers to the P_{fa}. The priori probabilities $P(D^I D^A = 00)$, $P(D^I D^A = 11)$, $P(D^I D^A = 10)$, and $P(D^I D^A = 01)$ are obtained by numerical simulations.

IV. PERFORMANCE EVALUATION

Monte Carlo simulations are conducted to evaluate the performance of the detector. 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 and $N = 64$, $N_{CP} = 16$. We use $b = 16$ bits to assess the performance. The Doppler effect is verified using vehicular test environment of International Mobile Telecommunications-2000 (IMT-2000) standard with recommendation ITU-R M.1225 [7]. The parameters of channel B from table 5 in [7] with the number of taps $(L+1) = 6$ and velocity of the mobile node equal to 70 km/h are utilized. All the results are obtained by averaging over 5000 simulation runs with the confidence interval $\nu = 90\%$.

To compare the performance of the proposed mechanism with that of PHY layer detection in [3], Fig. 2 plots $P(S)$ against P_{fa} under various SNRs. As shown, $P(S)$ approaches 1 rapidly as SNR increases, which means that the proposed method can reliably detect PUEA. Figure 3 plots $P(S)$ versus P_{fa} for various M's at SNR=-2 dB. For $P_{fa} = 0.1$, $P(S) = 0.9673$ can be achieved with $M = 30$, and $P(S) = 0.6147$ can be achieved with $M = 8$ using the cross-layer design. Meanwhile, using only PHY layer, probabilities of detection are 0.868 and 0.516 for $M = 30$ and $M = 8$, respectively. As shown, the performance of the proposed approach based on the cross-layer design can be improved compared to that using only the PHY layer detection. However, the detection time of [3] using only the PHY layer is faster than the proposed method. Notably, the performance can be improved by increasing M but the detection time also increases. Comparing Fig. 2 with Fig. 3 it reveals the trade-off between M and SNR. The influence of M on $P(S)$ is greater than SNR on $P(S)$; therefore, increasing M is a good strategy for operating in the low SNR environment. Furthermore, the results also reveal that the simulation values of $P(S)$ and P_{fa} are close to the analytical results. This indicates that, the proposed design is very promising for future mobile CR networks.

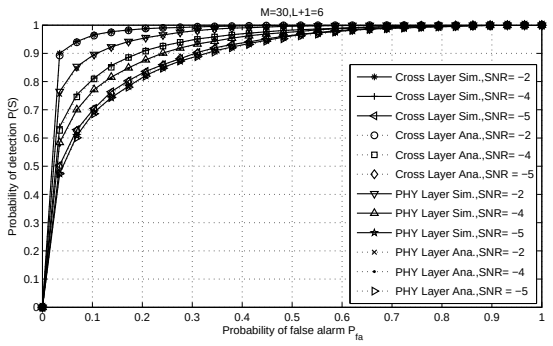

Fig. 2. Probability of detection as a function of P_{fa} for various SNRs.

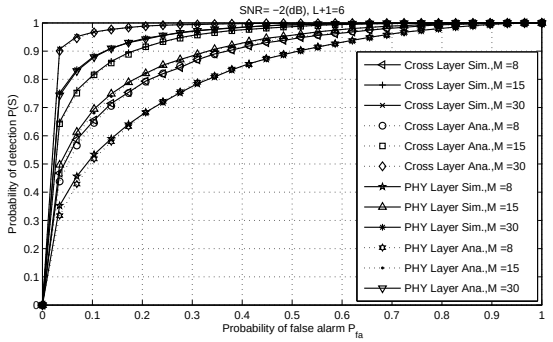

Fig. 3. Probability of detection versus P_{fa} for various M's.

V. CONCLUSIONS

The uniqueness of channel-tap powers between the SU and Txs is utilized as a RF to detect PUEA and PU in mobile CR networks. In addition, this letter proposes cross-layer design to completely detect PUEA and PU based on detection databases established by seamlessly combining the accuracy of higher layer authentication with the quick detection of PHY layer. Simulations demonstrate that the proposed technique greatly enhances detection efficiency of PHY layer.

REFERENCES

[1] H. Shokri-Ghadikolaei and R. Fallahi, "Intelligent sensing matrix setting in cognitive radio networks," *IEEE Commun. Lett.*, vol. 16, no. 11, pp.1824-1827, Nov. 2012.

[2] Z. Chen, C. Chen, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in *Proc. 2009 IEEE 28th International Performance Computing and Communications Conference*, pp. 208-215, Dec. 2009.

[3] W. L. Chin, T. N. Le, C. L. Tseng, W. C. Kao, C. S. Tsai and C.W. Kao, "Cooperative detection of primary user emulation attacks based on channel-tap power in mobile cognitive radio networks," in *Int. J. Ad Hoc and Ubiquitous Computing*, Vol. 15, No. 4, pp. 263-274, May 2014.

[4] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *Proc. the 2010 IEEE Symposium on Security and Privacy*, pp. 286-301, May 2010.

[5] C. N. Mathur and K. P. Subbalakshmi, "Digital signatures for centralized DSA networks," in *First IEEE Workshop on Cognitive Radio Networks*, pp. 1037-1041, Jan. 2007.

[6] A. Goldsmith, *Wireless Communications*, Cambridge University Press, Cambridge, 2005.

[7] International Telecommunication Union, " Guidelines for evaluation of radio transmission technologies for IMT-2000," *Recommendation ITU-R M.1225*, 1997.