Modeling Primary User Emulation Attacks and Defenses in Cognitive Radio Networks

Zesheng Chen, Todor Cooklev, Chao Chen, and Carlos Pomalaza-Ráez
Indiana University - Purdue University Fort Wayne
Fort Wayne, IN 46805

Abstract—**Primary user emulation attacks are a potential security threat to cognitive radio networks. In this work, we attempt to characterize an advanced primary user emulation attack and an advanced countermeasure against such an attack. Specifically, we show that both the attacker and the defender can apply estimation techniques and learning methods to obtain the key information of the environment and thus design better strategies. We further demonstrate that the advanced attack strategy can defeat the naive defense technique that focuses only on the received signal power, whereas the advanced defense strategy that exploits the invariant of communication channels can counteract the advanced attack effectively.**

I. Introduction

Cognitive radio networks are emerging wireless networks and a new paradigm in communications, aiming at resolving the spectrum crisis and allowing secondary spectrum licensing [1], [22]. In a cognitive radio network, a licensed user is called the *primary user*, whereas an unlicensed user is named the *secondary user*. If secondary users sense that primary users do not transmit, they can then use the spare spectrum for communications; otherwise, secondary users detect the presence of primary users and will restrain from transmitting. In this way, secondary users can make use of precious spectrum without interfering with the transmission of primary users.

The success of cognitive radio networks, however, strongly depends on counteracting potential security threats and attacks. There are mainly two physical security attacks against cognitive radios: primary user emulation attacks and machine learning algorithm attacks [4], [5], [6]. A primary user emulation attack exploits the intrinsic characteristic of secondary users that avoids interfering with the transmission of the primary user, whereas a machine learning algorithm attack compromises the ability of secondary users to learn the environment.

In this paper, we focus on primary user emulation attacks. When primary users do not transmit, an attacker sends jamming signals that emulate those from primary users, so that normal secondary users believe that a primary user is transmitting and are prevented from using the spare spectrum. Such attacks are a new type of denial-of-service attacks against normal secondary users.

Primary user emulation attacks and defenses have been studied in previous work [5], [2], [12]. For example, Chen *et al.* proposed to use the location of the primary user to identify the primary user emulation attack [5]. Moreover, Jin *et al.* applied Wald's sequential probability ratio test to detect the attack [12]. The previous work, however, assumes that the transmit power of the attacker is fixed so that the underlying probability distributions of the received signal power from the primary user and the attacker are fundamentally different [12], [2]. In this paper, we consider more *advanced* attacks that can *adapt* the transmit power to effectively jam the victim. We also show that a *naive* defense strategy that focuses only on the probability distribution of received signal power cannot counteract such advanced attacks.

The goal of this work is to characterize an advanced primary user emulation attack and an advanced countermeasure against such an attack. Specifically, we emphasize that both the attacker and the defender can potentially apply estimation techniques to obtain the key information of the environment from the received signals and use the information to design better strategies. For example, we show that an attacker can employ a *maximum likelihood estimator* [13] to infer the transmit power of the primary user and a channel parameter, and use the inferred parameters and a *mean-field approach* [17] to generate primary user emulation signals against a secondary user. On the other hand, we propose an advanced defense strategy against the designed attack. We call such a defense strategy the *variance detection* method. The key observation of variance detection is that an advanced attacker can potentially emulate many characteristics of the primary user, such as modulation methods and cyclostationary features, but will find it difficult to emulate the feature of a communication channel. Since signals from the primary user and the attacker may go through different channels, the channel parameters are different and can be applied as the *signatures* of the primary user and the attacker. Therefore, we propose to estimate the *invariant* of a communication channel, *i.e.,* the channel parameter, to detect the advanced primary user emulation attack.

Our research work makes several contributions as follows:

- We design an advanced primary user emulation attack that applies an estimation technique and a learning method, and show that such an attack can defeat a naive defense strategy that focuses only on the received signal power.
- We propose a defense strategy that exploits the invariant of a communication channel and estimates the channel parameter, and demonstrate that such a defense mechanism can counteract the advanced attack effectively.
- We find that under the designed attack and defense strategies, the performance metrics (*i.e.,* the probabilities of false positives and false negatives) are independent of

the transmit power of the primary user, the geometric locations of all entities, and the path loss exponent.

- We illustrate the tradeoff between the performance and the overhead. For the variance detection method, the defense performance improves as the number of spectrum sensing increases.

Detecting the primary user emulation attack belongs to a more general research problem that identifies radio-frequency (RF) fingerprints [3]. The solutions to this problem can broadly be classified into two categories: (1) exploiting transmitter-specific characteristics [15], [3], and (2) using channel-specific features [7], [16], [18]. Our solution belongs to the category of using channel features. Different from most existing work that focuses on the location distinction [18], [5], our work contributes to the field by exploiting the fundamental characteristics of communication channels with the path loss and the log-normal shadowing in cognitive radio networks.

The remainder of this paper is structured as follows. Section II introduces the problem setup. Section III gives a naive defense strategy against traditional primary user emulation attacks. Section IV presents an advanced primary user emulation attack against the naive defense strategy, whereas Section V proposes an advanced defense method based on the invariant of communication channels. Section VI further shows the numerical results. Finally, Section VII concludes this paper.

II. Problem Setup

In this section, we introduce a network model, a spectrum sensing method, a channel model, and performance metrics for studying the problem of primary user emulation attacks and defenses.

A. Network Model

Figure 1 shows a simplified cognitive radio network model. An attacker attempts to emulate a primary user to fool a victim (*i.e.,* a secondary user or a defender), whereas the victim endeavors to distinguish between the signals from the primary user and those from the attacker. Specifically, when the primary user is transmitting, both the victim and the attacker cannot use the spectrum. When the primary user is not transmitting, however, the attacker can send jamming signals into the channel to emulate the primary user so that the victim is prevented from using the free spectrum. On the other hand, when the victim receives a signal, it needs to determine whether the signal is from the primary user (*i.e.,* normal) or from the attacker (*i.e.,* anomalous), in a manner similar to an intrusion detection system [21], [10].

The geometric locations of the primary user, the attacker, and the victim are shown in Figure 1. That is, the distance between the victim (or the attacker) and the primary user is r_1 (or r_2), whereas the victim is r_3 away from the attacker. In many cases, the attacker is close to the victim [5], [2], *i.e.,* $r_3 << r_1$ and $r_3 << r_2$. In this work, we assume that the locations of all entities are fixed.

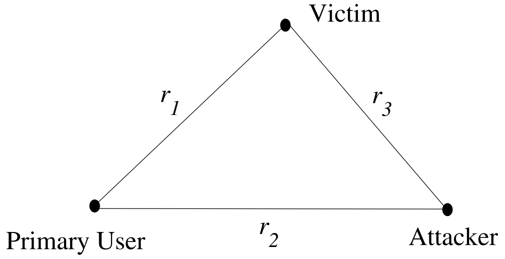

Fig. 1. A simplified cognitive radio network.

B. Spectrum Sensing and Channel Model

A secondary user can use different methods to sense the presence of the primary user in the spectrum, such as matched filter detection, cyclostationary feature detection, and energy detection [1], [22], [14]. In this work, we consider energy detection for three reasons. First, the energy detection method is most widely used and can be easily implemented [1], [14]. Second, an intelligent attacker can potentially generate a signal with the features similar to those of the primary user, such as modulation schemes and cyclostationary characteristics. Hence, a victim cannot distinguish between the primary user and the attacker based only on matched filter and cyclostationary spectrum sensing methods. Last, the anomaly detection method proposed in this paper under the energy sensing (*i.e.,* variance detection) can easily be extended to other spectrum sensing methods.

The energy detection method measures the energy of the received signal and determines whether or not such a signal is from the primary user. To model the relationship between the transmit signal power and the received signal power, in this paper we consider the path loss and the log-normal shadowing of a communication channel. Specifically, it is assumed that a path loss exponent of α is used, *i.e.,* the received signal energy P_r is proportional to $r^{-\alpha}$, where r is the distance between the transmitter and the receiver. Moreover, P_r is also proportional to a shadowing random variable G. Here, $G = 10^{\frac{\beta}{10}} = e^{a\beta}$, where $a = \frac{\ln 10}{10}$ and β follows a normal distribution $\beta \sim N(0, \sigma^2)$. It is noted that the moment generating function of normal random variable β [20] is

$$\psi(t) = \mathrm{E}\left(e^{t\beta}\right) = e^{\frac{1}{2}\sigma^2 t^2}, \tag{1}$$

which leads to

$$\mathrm{E}(G) = \mathrm{E}\left(e^{a\beta}\right) = e^{\frac{1}{2}a^2\sigma^2} \tag{2}$$

$$\mathrm{Var}(G) = \mathrm{E}\left(G^2\right) - \mathrm{E}^2(G) = e^{a^2\sigma^2}\left(e^{a^2\sigma^2} - 1\right). \tag{3}$$

Hence, if a transmitter uses energy P_t to send signals, then the received signal energy at the receiver is

$$P_r = P_t \cdot r^{-\alpha} \cdot G = P_t \cdot r^{-\alpha} \cdot e^{a\beta}. \tag{4}$$

Such a channel model is described in detail in [9] and has been applied in [2], [12]. Note that if a signal is from the primary user, from the view of the receiver (either the victim or the attacker), $G = G_p$, $\beta = \beta_p$, and $\sigma^2 = \sigma_p^2$; otherwise, if the signal is from the attacker, $G = G_s$, $\beta = \beta_s$, and $\sigma^2 = \sigma_s^2$. Since the primary user and the attacker may be at different locations, σ_p^2 and σ_s^2 may be very different. Moreover, according to [9], $2 \leq \alpha \leq 8$, and $4 < \sigma^2 < 12$ from the empirical study.

C. Performance Metrics

Most existing work on cognitive sensing focuses on performing a hypothesis testing to decide the presence of the primary user [1], [22], [14], [11]. In this paper, we attempt to characterize the interaction between the attacker and the defender. As a result, in our work a victim (or a defender) performs a hypothesis testing to decide whether a signal is from the primary user or from the attacker, as shown in the following two hypotheses:

$$\begin{aligned} \mathcal{H}_0: &\quad \text{the signal is from the primary user} \\ \mathcal{H}_1: &\quad \text{the signal is from the attacker.} \end{aligned}$$

We are particularly interested in two performance metrics:

- Probability of false positives (P_{FP}) or probability of false alarm (P_{FA}): When the signal is from the primary user, the probability that the victim falsely classifies it as from the attacker, *i.e.,*

$$\mathrm{P}_{\mathrm{FP}} = \mathrm{P}_{\mathrm{FA}} = \Pr(\mathcal{H}_1 | \mathcal{H}_0). \tag{5}$$

- Probability of false negatives (P_{FN}) or probability of misdetection (P_{MD}): When the signal is from the attacker, the probability that the victim falsely classifies it as from the primary user, *i.e.,*

$$\mathrm{P}_{\mathrm{FN}} = \mathrm{P}_{\mathrm{MD}} = \Pr(\mathcal{H}_0 | \mathcal{H}_1). \tag{6}$$

Note that another widely used metric is the probability of detection (P_{D}), and

$$\mathrm{P}_{\mathrm{D}} = 1 - \mathrm{P}_{\mathrm{MD}} = 1 - \mathrm{P}_{\mathrm{FN}} = \Pr(\mathcal{H}_1 | \mathcal{H}_1). \tag{7}$$

The goal of the attacker is to make P_{FP} or P_{FN} as large as possible, whereas the aim of the defender is to make both P_{FP} and P_{FN} as small as possible. In the area of statistical signal processing, a widely used plot is the receiver operating characteristics (ROCs) that are based on P_{D} and P_{FA} [13]. In this work, we will also use ROCs to demonstrate the performance of strategies used by the attacker and the defender.

III. Defense Strategy: Naive Detection

In this section, we give a simple defense strategy that is based on the received signal power. Such a strategy is called *naive detection* and is similar to the defense strategy used in [2]. The main difference between the naive detection method and the strategy in [2] is that the naive detection method estimates the mean and the variance of the received power from the primary user, whereas the strategy in [2] focuses on the successful attack probability without estimation. Specifically, a defender attempts to identify the main range of the received power from the primary user and takes the following two steps:

- Estimate the mean and the variance of the received power from the primary user.
- Determine whether a received signal is from the primary user or from the attacker.

A. Estimation

The defender receives signals from the primary user with energies $y_1^{(v)}$, $y_2^{(v)}$, $\cdots$, $y_n^{(v)}$, where n is the number of observed signals. Then, $y_1^{(v)}$, $y_2^{(v)}$, $\cdots$, $y_n^{(v)}$ are i.i.d. and follow the same distribution as $P_r^{(v)}$, where

$$P_r^{(v)} = P_t \cdot r_1^{-\alpha} \cdot G_p = P_t \cdot r_1^{-\alpha} \cdot e^{a\beta_p}. \tag{8}$$

Here, r_1 is the distance between the defender (*i.e.,* the victim) and the primary user, α is the path loss exponent, and $\beta_p \sim N(0,\, \sigma_p^2)$. Note that the mean and the variance of $P_r^{(v)}$ are

$$u_r = \mathrm{E}\left(P_r^{(v)}\right) = P_t r_1^{-\alpha} e^{\frac{1}{2}a^2\sigma_p^2} \tag{9}$$

$$\sigma_r^2 = \mathrm{Var}\left(P_r^{(v)}\right) = P_t^2 r_1^{-2\alpha} e^{a^2\sigma_p^2}\left(e^{a^2\sigma_p^2} - 1\right) \tag{10}$$

from Equations (2) and (3). Thus, the problem is to estimate u_r and σ_r^2 based on $y_1^{(v)}$, $y_2^{(v)}$, $\cdots$, $y_n^{(v)}$. Here, we consider a well-known unbiased estimator [13]

$$\hat{u_r} = \frac{1}{n}\sum_{i=1}^{n} y_i^{(v)} \tag{11}$$

$$\hat{\sigma_r^2} = \frac{1}{n-1}\sum_{j=1}^{n}\left(y_j^{(v)} - \frac{1}{n}\sum_{i=1}^{n} y_i^{(v)}\right)^2. \tag{12}$$

When n is large, u_r and σ_r^2 can be estimated accurately.

B. Determination

After estimating u_r and σ_r^2 accurately, a defender decides whether a received signal is from the primary user or not as follows:

$$\begin{cases} \text{If } |P_r - \hat{u_r}| \leq k\sqrt{\hat{\sigma_r^2}}, & \text{signal is from primary user } (\mathcal{H}_0) \\ \text{If } |P_r - \hat{u_r}| > k\sqrt{\hat{\sigma_r^2}}, & \text{signal is from attacker } (\mathcal{H}_1), \end{cases} \tag{13}$$

where P_r is the received power, and k ($k > 0$) is a constant that controls the threshold of determination and is called the *threshold factor*.

IV. Advanced Attack Strategy

In this section, we model an advanced strategy used by the attacker, which can defeat the naive detection method given in the last section. We assume that an attacker knows the distances between all entities (*i.e.,* r_1, r_2, and r_3), path loss exponent α, and σ_s^2. To emulate the transmission of the primary user, the attacker needs to generate a signal that from the victim's viewpoint has the energy similar to that from the primary user. To achieve this, the attack consists two steps:

- Estimate primary user transmit power P_t and channel parameter σ_p^2.
- Design a primary user emulation attack with transmit power P_s so that the received signal energy at the victim from the attacker $P_r^{(s)}$ is as similar as possible to that from the primary user $P_r^{(v)}$.

A. Estimation

The attacker receives signals from the primary user with energies $y_1^{(a)}$, $y_2^{(a)}$, $\cdots$, $y_n^{(a)}$, where n is the number of observed signals. Then, the problem of estimation can be stated as follows: Given $y_1^{(a)}$, $y_2^{(a)}$, $\cdots$, $y_n^{(a)}$, what is the best estimate of P_t and σ_p^2?

Note that $y_1^{(a)}$, $y_2^{(a)}$, $\cdots$, $y_n^{(a)}$ are independent and identically distributed (i.i.d.) and follow the same distribution as $P_r^{(a)}$, where

$$P_r^{(a)} = P_t \cdot r_2^{-\alpha} \cdot G_p = P_t \cdot r_2^{-\alpha} \cdot e^{a\beta_p}. \tag{14}$$

Here, r_2 is the distance between the attacker and the primary user, α is the path loss exponent, and $\beta_p \sim N(0,\, \sigma_p^2)$. Then,

$$\ln P_r^{(a)} = \ln P_t - \alpha \ln r_2 + a\beta_p. \tag{15}$$

Hence, we have $\ln P_r^{(a)} \sim N(P,\, a^2\sigma_p^2)$, where $P = \ln P_t - \alpha \ln r_2$. Since α and r_2 are known to the attacker, the problem of estimating P_t is equivalent to estimating P.

Next, we apply *maximum likelihood estimation* to obtain the estimates of P and σ_p^2. Note that the likelihood function based on the observations is given by the following product

$$\begin{aligned} \mathrm{L}\left(P, \sigma_p^2\right) &= \prod_{i=1}^{n} \Pr\left(\ln y_i^{(a)}; P, \sigma_p^2\right) &(16)\\ &= \left(\frac{1}{\sqrt{2\pi}a\sigma_p}\right)^n e^{-\frac{1}{2a^2\sigma_p^2}\sum_{i=1}^{n}\left(\ln y_i^{(a)}-P\right)^2} &(17)\end{aligned}$$

We then design a maximum likelihood estimator (MLE), *i.e.,*

$$\left(\hat{P}, \hat{\sigma_p^2}\right)_{\text{MLE}} = \arg\max_{P,\sigma_p^2} \mathrm{L}\left(P, \sigma_p^2\right). \tag{18}$$

Rather than maximizing $\mathrm{L}\left(P, \sigma_p^2\right)$, we choose to maximize its logarithm $\ln \mathrm{L}\left(P, \sigma_p^2\right)$. That is,

$$\frac{d}{dP} \ln \mathrm{L}\left(P, \sigma_p^2\right) = 0 \tag{19}$$

$$\frac{d}{d\sigma_p^2} \ln \mathrm{L}\left(P, \sigma_p^2\right) = 0, \tag{20}$$

which lead to

$$\hat{P}_{\text{MLE}} = \frac{1}{n}\sum_{i=1}^{n} \ln y_i^{(a)} \tag{21}$$

$$\left(\hat{\sigma_p^2}\right)_{\text{MLE}} = \frac{1}{na^2}\sum_{j=1}^{n}\left(\ln y_j^{(a)} - \frac{1}{n}\sum_{i=1}^{n}\ln y_i^{(a)}\right)^2. \tag{22}$$

Moreover, from Equation (21), we obtain the MLE of P_t

$$\left(\hat{P_t}\right)_{\text{MLE}} = r_2^{\alpha} e^{\frac{1}{n}\sum_{i=1}^{n}\ln y_i^{(a)}}. \tag{23}$$

It can further be derived based on the techniques in [13] that

$$\hat{P}_{\text{MLE}} \sim N\left(P, \frac{a^2\sigma_p^2}{n}\right) \tag{24}$$

$$\left(\hat{\sigma_p^2}\right)_{\text{MLE}} \sim N\left(\frac{n-1}{n}\sigma_p^2, \frac{2(n-1)}{n^2}\sigma_p^4\right). \tag{25}$$

This indicates that when n is large, P_t and σ_p^2 can be estimated accurately.

B. Design

After estimating P_t and σ_p^2 accurately, the attacker designs a signal with power P_s to confuse the victim. Here, we apply a *mean-field* approach [17] to derive a solution of P_s. Specifically, the mean-field method focuses on the averages of the received signal power, ignoring fluctuations. Note that the received power at the victim from the primary user, $P_r^{(v)}$, is given by

$$P_r^{(v)} = P_t \cdot r_1^{-\alpha} \cdot G_p = P_t \cdot r_1^{-\alpha} \cdot e^{a\beta_p}, \tag{26}$$

where r_1 is the distance between the victim and the primary user, α is the path loss exponent, and $\beta_p \sim N(0,\, \sigma_p^2)$. Similarly, the received power at the victim from the attacker, $P_r^{(s)}$, is given by

$$P_r^{(s)} = P_s \cdot r_3^{-\alpha} \cdot G_s = P_s \cdot r_3^{-\alpha} \cdot e^{a\beta_s}, \tag{27}$$

where r_3 is the distance between the victim and the attacker, and $\beta_s \sim N(0,\, \sigma_s^2)$. Then, we consider the mean values of $P_r^{(v)}$ and $P_r^{(s)}$, *i.e.,*

$$\mathrm{E}\left(P_r^{(v)}\right) = P_t \cdot r_1^{-\alpha} \cdot e^{\frac{1}{2}a^2\sigma_p^2} \tag{28}$$

$$\mathrm{E}\left(P_r^{(s)}\right) = P_s \cdot r_3^{-\alpha} \cdot e^{\frac{1}{2}a^2\sigma_s^2} \tag{29}$$

by applying Equation (2). Therefore, one goal of the attacker is to make $\mathrm{E}\left(P_r^{(v)}\right) = \mathrm{E}\left(P_r^{(s)}\right)$, which leads to

$$P_s = P_t \left(\frac{r_3}{r_1}\right)^{\alpha} e^{\frac{1}{2}a^2\left(\sigma_p^2 - \sigma_s^2\right)}. \tag{30}$$

In the above equation, the attacker can use the estimated $\left(\hat{P_t}\right)_{\text{MLE}}$ and $\left(\hat{\sigma_p^2}\right)_{\text{MLE}}$ to obtain P_s.

C. Performance Evaluation

To evaluate the performance of the advanced attack strategy, we study the probabilities of false positives and false negatives (*i.e.,* P_{FP} and P_{FN}) for the naive detection method. Since when n is large, the attacker can estimate P_t and σ_p^2 accurately, we assume $(\hat{P_t})_{\text{MLE}} = P_t$ and $(\hat{\sigma_p^2})_{\text{MLE}} = \sigma_p^2$. Similarly, we assume $\hat{u_r} = u_r$ and $\hat{\sigma_r^2} = \sigma_r^2$ for the defender.

1) False Positives: From Equations (9) and (10), $\sigma_r = u_r\sqrt{e^{a^2\sigma_p^2}-1} = cu_r$, where $c = \sqrt{e^{a^2\sigma_p^2}-1}$. When the signal is from the primary user, $P_r = P_r^{(v)}$. Thus, from the determination criteria of the naive detection in (13), the probability of false positives can be calculated as

$$\begin{aligned} \mathrm{P}_{\text{FP}} &= \mathrm{Pr}\left(\left|P_r^{(v)} - u_r\right| > k\sigma_r\right) && (31) \\ &= \mathrm{Pr}\left(P_r^{(v)} > (1+kc)u_r\right) \\ &\quad + \mathrm{Pr}\left(P_r^{(v)} < (1-kc)u_r\right). && (32) \end{aligned}$$

Using Equations (8) and (9) and applying $\beta_p \sim N(0, \sigma_p)$, we have that if $kc < 1$,

$$\begin{aligned} \mathrm{P}_{\text{FP}} &= \mathrm{Pr}\left(\frac{\beta_p}{\sigma_p} > \frac{1}{2}a\sigma_p + \frac{1}{a\sigma_p}\ln(1+kc)\right) \\ &\quad + \mathrm{Pr}\left(\frac{\beta_p}{\sigma_p} < \frac{1}{2}a\sigma_p + \frac{1}{a\sigma_p}\ln(1-kc)\right) && (33) \\ &= 1 + Q\left(\frac{1}{2}a\sigma_p + \frac{1}{a\sigma_p}\ln(1+kc)\right) \\ &\quad - Q\left(\frac{1}{2}a\sigma_p + \frac{1}{a\sigma_p}\ln(1-kc)\right); && (34) \end{aligned}$$

otherwise, if $kc \geq 1$,

$$\begin{aligned} \mathrm{P}_{\text{FP}} &= \mathrm{Pr}\left(\frac{\beta_p}{\sigma_p} > \frac{1}{2}a\sigma_p + \frac{1}{a\sigma_p}\ln(1+kc)\right) && (35) \\ &= Q\left(\frac{1}{2}a\sigma_p + \frac{1}{a\sigma_p}\ln(1+kc)\right), && (36) \end{aligned}$$

where $Q(\tau) = \int_\tau^\infty \frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}dx$. Note that P_{FP} only depends on σ_p and k, and is independent of P_t, r_1, and α.

2) False Negatives: When the signal is from the attacker, $P_r = P_r^{(s)}$. From the determination criteria in (13) and $\sigma_r = cu_r$, the probability of false negatives can be calculated as

$$\begin{aligned} \mathrm{P}_{\text{FN}} &= \mathrm{Pr}\left(\left|P_r^{(s)} - u_r\right| \leq k\sigma_r\right) && (37) \\ &= \mathrm{Pr}\left(1 - kc \leq \frac{P_r^{(s)}}{u_r} \leq 1 + kc\right). && (38) \end{aligned}$$

Using Equations (27), (30), and (9), we have that if $kc < 1$,

$$\begin{aligned} \mathrm{P}_{\text{FN}} &= \mathrm{Pr}\left(\frac{a\sigma_s}{2} + \frac{\ln(1-kc)}{a\sigma_s} \leq \frac{\beta_s}{\sigma_s} \leq \frac{a\sigma_s}{2} + \frac{\ln(1+kc)}{a\sigma_s}\right) \\ &= Q\left(\frac{1}{2}a\sigma_s + \frac{1}{a\sigma_s}\ln(1-kc)\right) \\ &\quad - Q\left(\frac{1}{2}a\sigma_s + \frac{1}{a\sigma_s}\ln(1+kc)\right), && (39) \end{aligned}$$

otherwise, $kc \geq 1$,

$$\begin{aligned} \mathrm{P}_{\text{FN}} &= \mathrm{Pr}\left(\frac{\beta_s}{\sigma_s} \leq \frac{1}{2}a\sigma_s + \frac{1}{a\sigma_s}\ln(1+kc)\right) && (40) \\ &= 1 - Q\left(\frac{1}{2}a\sigma_s + \frac{1}{a\sigma_s}\ln(1+kc)\right). && (41) \end{aligned}$$

Note that P_{FN} only depends on σ_p, σ_s, and k, and is independent of P_t, r_1, r_3, and α. When $\sigma_s = \sigma_p$, $\mathrm{P}_{\text{FP}} + \mathrm{P}_{\text{FN}} = 1$. Moreover, when threshold factor k increases from 0 to infinity, P_{FP} decreases from 1 to 0, whereas P_{FN} increases from 0 to 1.

As will be shown in Section VI (Numerical Results), the designed advanced attack strategy can defeat the naive defense method. That is, the advanced attack causes the naive defense to have a high probability of false alarm or a low probability of detection. Therefore, in the next section we study an advanced defense strategy.

V. Advanced Defense Strategy: Variance Detection

To better counteract the advanced attack, we propose another defense strategy. Instead of focusing on the first order of the received power, a defender can look into more detailed information about the received signals to design better detection methods. One of such methods is based on the variance (or the second order) of the received signal power, which indeed reflects the channel parameter σ^2. Note that σ^2 is a time-invariant of a communication channel and is difficult for an attacker to emulate. We call such a method *variance detection*. Similar to the naive detection method, the variance detection strategy consists of two steps:

- Estimate the variance of the received power from the primary user, *i.e.,* channel parameter σ_p^2.
- Determine whether a received signal is from the primary user or from the attacker.

A. Estimation

Similar to the technology used by the attacker, the defender can first estimate the channel parameter σ_p^2 when the primary user is transmitting, and then use the estimated information to detect the presence of the primary user or the attacker. In Section IV-A, an attacker uses MLE in Equation (22) to infer σ_p^2. Here, we can consider a similar, but unbiased estimator for estimating σ_p^2. Specifically, if the sequence of the received signal power at the defender from the primary user is $y_1^{(v)}$, $y_2^{(v)}$, $\cdots$, $y_n^{(v)}$, where n is the number of observations, then an unbiased estimator for σ_p^2 is

$$\left(\hat{\sigma_p^2}\right)_{\text{D}} = \frac{1}{(n-1)a^2}\sum_{j=1}^{n}\left(\ln y_j^{(v)} - \frac{1}{n}\sum_{i=1}^{n}\ln y_i^{(v)}\right)^2. \quad (42)$$

Note that $\frac{1}{n-1}$ is used in the above equation, whereas $\frac{1}{n}$ is used in Equation (22). Therefore, it can further be derived that

$$\left(\hat{\sigma_p^2}\right)_{\text{D}} \sim N\left(\sigma_p^2, \frac{2}{n-1}\sigma_p^4\right). \quad (43)$$

When n is large, σ_p^2 can be estimated accurately.

B. Determination

From Equation (43), we can design a new detection method as follows: When the defender receives a sequence of the signal power (no matter from the primary user or the attacker), *i.e.,* y_1, y_2, $\cdots$, y_m, where m is the number of sensing attempts, the defender first estimates the channel parameter by

$$\left(\hat{\sigma^2}\right)_{\mathrm{D}} = \frac{1}{(m-1)a^2}\sum_{j=1}^{m}\left(\ln y_j - \frac{1}{m}\sum_{i=1}^{m}\ln y_i\right)^2, \qquad (44)$$

and then determines whether the signals are from the primary user or the attacker as follows:

$$\begin{cases} \text{If } \left|\left(\hat{\sigma^2}\right)_{\mathrm{D}} - \left(\hat{\sigma_p^2}\right)_{\mathrm{D}}\right| \le k\left(\hat{\sigma_p^2}\right)_{\mathrm{D}}, \\ \qquad \text{then the signal is from the primary user } (\mathcal{H}_0) \\ \text{If } \left|\left(\hat{\sigma^2}\right)_{\mathrm{D}} - \left(\hat{\sigma_p^2}\right)_{\mathrm{D}}\right| > k\left(\hat{\sigma_p^2}\right)_{\mathrm{D}}, \\ \qquad \text{then the signal is from the attcker } (\mathcal{H}_1), \end{cases} \qquad (45)$$

where k ($k > 0$) is the threshold factor that controls the threshold of determination.

C. Performance Evaluation

Similar to the naive detection, we study the probabilities of false positives and false negatives (*i.e.,* P_{FP} and P_{FN}) under the advanced attack for the variance detection. Here, we assume that the defender can estimate σ_p^2 accurately, *i.e.,* $\left(\hat{\sigma_p^2}\right)_{\mathrm{D}} = \sigma_p^2$.

1) False Positives: When the signals are from the primary user,

$$\left(\hat{\sigma^2}\right)_{\mathrm{D}} = \hat{\sigma_p^2} \sim N\left(\sigma_p^2, \frac{2}{m-1}\sigma_p^4\right), \qquad (46)$$

which is similar to the result in Equation (43). Thus, setting $l = \sqrt{\frac{2}{m-1}}$, we can derive the probability that the defender incorrectly classifies them as from the attacker:

$$\begin{aligned} \mathrm{P}_{\mathrm{FP}} &= \Pr\left(\left|\hat{\sigma_p^2} - \sigma_p^2\right| > k\sigma_p^2\right) & (47) \\ &= \Pr\left(\frac{\left|\hat{\sigma_p^2} - \sigma_p^2\right|}{\sigma_p^2/l} > kl\right) & (48) \\ &= 2Q(kl). & (49) \end{aligned}$$

2) False Negatives: When the signals are form the attacker,

$$\left(\hat{\sigma^2}\right)_{\mathrm{D}} = \hat{\sigma_s^2} \sim N\left(\sigma_s^2, \frac{2}{m-1}\sigma_s^4\right). \qquad (50)$$

Therefore, using $\frac{\hat{\sigma_s^2} - \sigma_s^2}{\sigma_s^2/l} \sim N(0,\,1)$, we can obtain the probability that the defender incorrectly classifies them as from the primary user:

$$\begin{aligned} \mathrm{P}_{\mathrm{FN}} &= \Pr\left(\left|\hat{\sigma_s^2} - \sigma_p^2\right| \le k\sigma_p^2\right) & (51) \\ &= 1 - Q\left(l(k-1)\left(\frac{\sigma_p}{\sigma_s}\right)^2 + l\right) \\ &\quad - Q\left(l(k+1)\left(\frac{\sigma_p}{\sigma_s}\right)^2 - l\right). & (52) \end{aligned}$$

Note that when $\sigma_p = \sigma_s$, $\mathrm{P}_{\mathrm{FN}} = 1 - 2Q(kl) = 1 - \mathrm{P}_{\mathrm{FP}}$.

It can be seen that similar to the naive detection, both P_{FP} and P_{FN} of the variance detection are independent of primary user transmit power P_t, the geometric locations of entities (*i.e.,* r_1, r_2, and r_3), and path loss exponent α. Indeed, P_{FP} only depends on threshold factor k and the number of sensing m, whereas P_{FN} only depends on the number of sensing m, threshold factor k, and channel parameters σ_p^2 and σ_s^2. Moreover, when threshold factor k increases from 0 to infinity, P_{FP} decreases from 1 to 0, whereas P_{FN} increases from 0 to 1.

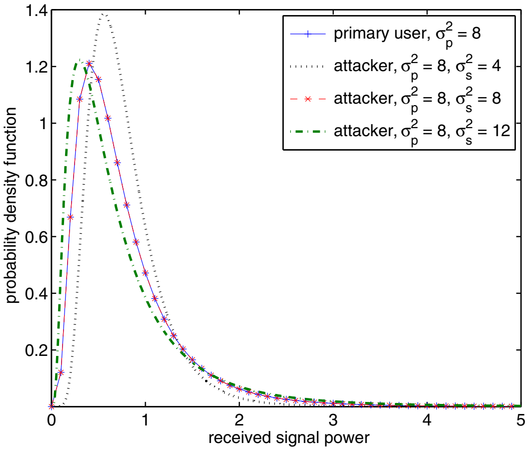

Fig. 2. Probability density functions of the received signal power at the victim.

VI. Numerical Results

As a motivating example, Figure 2 shows the probability density functions (PDFs) of signal power received by the victim when the primary use or the attacker is transmitting. Here, the attacker applies the advanced strategy as designed in Section IV. Specifically, we assume that the transmit power of the primary user is $P_t = 10$, the distance between the primary user and the victim is $r_1 = 2$, and the path loss exponent is $\alpha = 4$. Moreover, when the primary user is transmitting, the channel parameter is $\sigma_p^2 = 8$; whereas when the attacker is transmitting, the channel parameter is $\sigma_s^2 = 4$, 8, or 12. Figure 2 demonstrates that when $\sigma_s^2 = \sigma_p^2$, the PDFs of signal power received from the primary user and the attacker are identical. That is, we cannot distinguish the distributions under this case. Furthermore, although when $\sigma_s^2 \neq \sigma_p^2$, the PDFs are different, all curves in the figure have the same mean of 0.77. This indicates that the advanced attack can potentially jam effectively the victim who only focuses on the received signal power to detect the attacker.

For the numerical analysis of the performance of the advanced attack and defense, we plot the receiver operating characteristics (ROCs) of both naive detection and variance detection. We obtain the different values of the probability of false alarm P_{FA} and the probability of detection P_{D} in the range [0, 1] by varying threshold factor k. Specifically, for a given k, we can calculate both P_{FP} and P_{FN}, and plot the point (P_{FA}, P_{D}) in the figure, where $\mathrm{P}_{\mathrm{FA}} = \mathrm{P}_{\mathrm{FP}}$ and $\mathrm{P}_{\mathrm{D}} = 1 - \mathrm{P}_{\mathrm{FN}}$. If a detection method has a good performance, its ROCs will show that when P_{FA} is small, P_{D} has a large value. An ideal (but not realistic) detection would result in that when $\mathrm{P}_{\mathrm{FA}} = 0$,

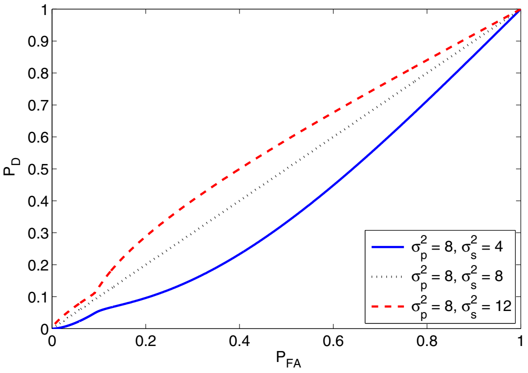

Fig. 3. Receiver operating characteristics (ROCs) of naive detection with $\sigma_p^2 = 8$ and different σ_s^2.

$P_D = 1$. In the experiments, since $4 < \sigma^2 < 12$ [9], we choose $\sigma_p^2 = 8$, $\sigma_s^2 = 4$, 8, or 12.

Figure 3 shows the ROCs of naive detection. It can be seen that $P_D = P_{FA}$ when $\sigma_p^2 = \sigma_s^2$, which is reflected by the diagonal line in the figure. When $\sigma_p^2 < \sigma_s^2$, $P_D > P_{FA}$, but P_D is still close to P_{FA}. Moreover, when $\sigma_p^2 > \sigma_s^2$, $P_D < P_{FA}$, indicating that the attacker can deceive the victim with a very high probability if the victim wants to detect the primary user with a high probability. Therefore, naive detection cannot counteract the advanced strategy used by the attacker.

Figure 4 demonstrates the ROCs of variance detection, when the number of spectrum sensing $m = 20$. It can be seen that when $\sigma_p^2 = \sigma_s^2$, $P_D = P_{FA}$. When $\sigma_p^2 \neq \sigma_s^2$, however, $P_D > P_{FA}$. Compared with naive detection, variance detection can achieve a much higher value of P_D for a given P_{FA} ($0 < P_{FA} < 1$) when $\sigma_p^2 \neq \sigma_s^2$. Therefore, variance detection has a much better performance against the advanced attack than naive detection. That is, when $\sigma_p^2 \neq \sigma_s^2$, variance detection can reliably distinguish between the legitimate primary user and the attacker disguised as the primary user.

Note that such a performance improvement comes from the overhead on the number of spectrum sensing. Naive detection uses only one-time sensing, while variance detection needs m sensing attempts. To further demonstrate the tradeoff between the performance and the overhead, in Figure 5 we show how ROCs vary with the number of sensing (*i.e,* $m = 10$, 20, and 30), when $\sigma_p^2 = 8$ and $\sigma_s^2 = 4$. As expected, the performance of variance detection improves as m increases.

VII. Conclusions

In this paper, we propose and model some advanced strategies used by the attacker and the defender in cognitive radio networks. We have shown that the estimation techniques (*e.g.,* maximum likelihood estimation) and the learning methods (*e.g.,* mean-field approach) can be exploited by the attacker and the defender. We have evaluated the performance of naive detection and variance detection methods against the advanced primary user emulation attack. We have found that while the naive detection cannot counteract the attack, the variance detection that focuses on the invariant of communication channels performs much better than the naive detection to mitigate the attack.

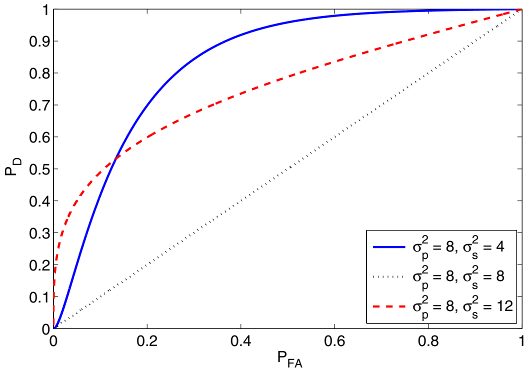

Fig. 4. Receiver operating characteristics (ROCs) of variance detection with $m = 20$, $\sigma_p^2 = 8$, and different σ_s^2.

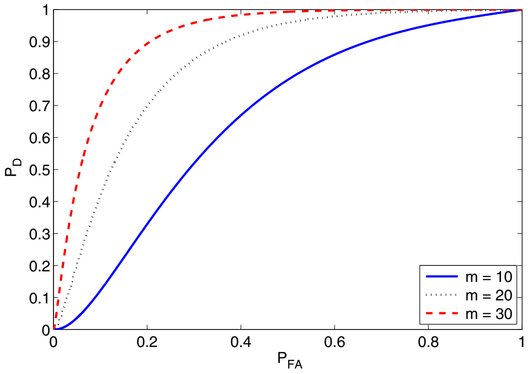

Fig. 5. Receiver operating characteristics (ROCs) of variance detection with $\sigma_p^2 = 8$, $\sigma_s^2 = 4$, and different numbers of spectrum sensing.

As part of our on-going work, we plan to study effective defense strategies when $\sigma_p^2 = \sigma_s^2$. We will also extend the simplified network model to include more attackers and defenders [8], [19] and to consider the mobility of entities.

References

[1] I. F. Akyildiz, W. Lee, M. C. Vuran, and S. Mohanty, “NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey,” *Computer Networks*, vol. 50, 2006, pp. 2127-2159.

[2] S. Anand, Z. Jin, and K. P. Subbalakshmi, “An analytical model for primary user emulation attacks in cognitive radio networks,” in *IEEE DySPAN*, Oct. 2008.

[3] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, “Wireless device identification with radiometric signatures,” in *14th Annual International Conference on Mobile Computing and Networking (MobiCom’08)*, Sept. 2008, pp. 116-127.

[4] J. L. Burbank, “Security in cognitive radio networks: The required evolution in approaches to wireless network security,” in *Third International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, May 2008.

[5] R. Chen, J. Park, and J. H. Reed, “Defense against primary user emulation attacks in cognitive radio networks,” *IEEE Journal on Selected Areas in Communications, Special Issue on Cognitive Radio Theory and Applications*, vol. 26, no. 1, Jan. 2008.

[6] T. C. Clancy and N. Goergen, “Security in cognitive radio networks: Threats and mitigation,” in *Third International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, May 2008.

[7] D. Faria and D. Cheriton, “Detecting identity-based attacks in wireless networks using signalprints,” in *Proc. of the Fifth ACM Wireless Security Workshop (WiSe’06)*, Los Angeles, CA, Sept. 2006, pp. 43-52.

[8] G. Ganesan and Y. Li, “Cooperative spectrum sensing in cognitive radio networks,” in *IEEE DySPAN*, Baltimore, MD, Nov. 2005, pp. 137-143.

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

[10] P. Helman and G. Liepins, “Statistical foundations of audit trail analysis for the detection of computer misuse,” *IEEE Transactions on Software Engineering*, vol. 19, no. 9, Sept. 1993, pp. 886-901.

[11] S. Hong, M. H. Vu, and V. Tarokh, “Cognitive sensing based on side information,” in *IEEE Sarnoff Symposium*, Princeton, NJ, April 2008.

[12] Z. Jin, S. Anand, and K. P. Subbalakshmi, “Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing,” in *ACM Mobile Computing and Communications Review, Special Issue on Cognitive Radio Technologies and Systems*, vol. 13, no. 2, April 2009, pp. 74-85.

[13] S. Kay, *Fundamentals of Statistical Signal Processing, Vol. I - Estimation Theory*. Prentice Hall, 1993.

[14] H. Kim and K. G. Shin, “In-band spectrum sensing in cognitive radio networks: Energy detection or feature detection?” in *14th Annual International Conference on Mobile Computing and Networking (MobiCom’08)*, Sept. 2008, pp. 14-25.

[15] T. Kohno, A. Broido, and K. C. Claffy, “Remote physical device fingerprinting,” *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 2, April-June 2005, pp. 93-108.

[16] Z. Li, W. Xu, R. Miller, and W. Trappe, “Securing wireless systems via lower layer enforcements,” in *Proc. of the Fifth ACM Wireless Security Workshop (WiSe’06)*, Los Angeles, CA, Sept. 2006, pp. 33-42.

[17] M. Opper and D. Saad (Eds.), *Advanced Mean Field Methods, Theory and Practice*. MIT Press, Feb. 2001.

[18] N. Patwari and S. K. Kasera, “Robust location distinction using temporal link signatures,” in *13th Annual ACM International Conference on Mobile Computing and Networking (MOBICOM’07)*, Sept. 2007, pp. 111-122.

[19] E. Peh and Y. Liang, “Optimization for cooperative sensing in cognitive radio networks,” in *Wireless Communications and Networking Conference*, Hong Kong, Mar. 2007, pp. 27-32.

[20] S. M. Ross, *Introduction to Probability Models*, Ninth Edition. Academic Press, 2007.

[21] A. Sundaram, “An introduction to intrusion detection,” *ACM Crossroads, Special Issue on Computer Security*, vol. 2, no. 4, April 1996, pp. 3-7.

[22] T. Yucek and H. Arslan, “A survey of spectrum sensing algorithms for cognitive radio applications,” *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, 2009.