Int. J. Electron. Commun. (AEÜ) 68 (2014) 520–527

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

journal homepage: www.elsevier.com/locate/aeue

# Cooperative spectrum sensing for cognitive radio networks in the presence of smart malicious users

Maryam Haghighat, Seyed Mohammad Sajad Sadough*

*Cognitive Telecommunication Research Group, Faculty of Electrical and Computer Engineering, Shahid Beheshti University, 1983963113 Tehran, Iran*

ARTICLE INFO

*Article history:*
Received 27 March 2013
Accepted 20 December 2013

*Keywords:*
Cognitive radio
Cooperative spectrum sensing
Malicious users
Primary user emulation attack

ABSTRACT

Cognitive radio (CR) signaling imposes some threats to the network. One of these common threats is commonly referred to as *primary user emulation attack*, where some *malicious* users try to mimic the primary signal and deceive secondary users to prevent them from accessing vacant frequency bands. In this paper, we introduce a *smart* primary user emulation attacker (PUEA) that sends fake signals similar to the primary signal. We assume a smart attacker, in the sense that it is aware of its radio environment and may choose different transmission strategies and then, we compare it to an *always present attacker*. In the proposed smart attacker strategy, the occurrence of fake signal is adjusted according to the primary user activity. First, we investigate the received signal at the CR users under such attackers. Then, we formulate and derive cooperative spectrum sensing (CSS) rules for a cognitive network operating in the presence of a PUEA and propose a new spectrum sensing scheme based on energy detection. Simulation results show that our proposed method can mitigate the destructive effect of PUEA in spectrum sensing, compared to conventional energy detection spectrum sensing.

## 1. Introduction

Cognitive radio (CR) [1] has been widely studied as an approach for increasing spectrum efficiency by allowing dynamic spectrum access of vacant bands through spectrum sensing process. In CR terminology, a licensed user is called primary user (PU) and unlicensed users are referred to as secondary (SU) or CR users. Unlicensed users are allowed to use licensed frequency bands to the PU, whenever PU is not present in the radio environment. To implement this efficient procedure and for exploiting unused frequency bands, a kind of spectrum sensing is needed to be performed in the CR network. In spectrum sensing, CR users sense the radio environment and try to find spectrum holes. The primary signal received in CR spectrum sensing unit is susceptible to the attenuation caused by fading, shadowing or other impairments. Therefore, the detection of primary signal in CR network by a single CR user may not be very reliable. So, cooperative spectrum sensing (CSS) [2] by means of multiple CRs is suggested which leads to more accurate detection of primary signals [1,2]. However, this dynamic manner to sense and exploit the spectrum in the CR network imposes some *threats* and provides an opportunity for some *malicious* users to intrude to the network and disrupt the performance of CR spectrum sensing [3]. One of these threats is referred to as primary user emulation (PUE) attack which benefits from CR responsibility to vacate bands occupied by the primary signal. In this type of attack, malicious users send fake signals with properties similar to the primary signal over the licensed frequency bands, leading true SUs to vacate the spectrum [3,4]. Then, malicious users can abuse this provided situation to perform their transmission or start an illegal transmission activity on free bands. As these malicious users try to prevent CRs from accessing frequency bands, they can be referred as a kind of competitive users for CRs.

Several approaches have been advocated in the literature to combat PUE attacks. For instance, a location based scheme which performs received signal strength (RSS) measurements is proposed in [5]. In [4], the authors investigate an advanced PUE attack and an advanced countermeasure by using estimation techniques and learning methods to obtain the key information of the environment. In [6], an analytical model is proposed to obtain a lower bound on the probability of a successful PUE attack on a SU by a set of cooperating malicious users. A new RSS-based defense strategy against the PUE attack in CR wireless networks using belief propagation of location information is proposed in [7]. Ref. [8] proposes a CSS that considers PUE attacker (PUEA), but the attacker is assumed to be always present, which is not a practical assumption. However, although there are lots of efforts from the research community to combat PUEA, CSS in the presence of such attackers has not been investigated sufficiently [8].

This paper aims at illustrating the non-efficiency of the approach considered for PUEA in [8], in which, an “always present attacker” is considered. Obviously, an always present attacker leads to a waste

* Corresponding author. Tel.: +98 2129904187.
*E-mail addresses:* s_sadough@sbu.ac.ir, sajad.sadough@gmail.com (S.M.S. Sadough).

1434-8411/$ – see front matter © 2013 Elsevier GmbH. All rights reserved.
http://dx.doi.org/10.1016/j.aeue.2013.12.010

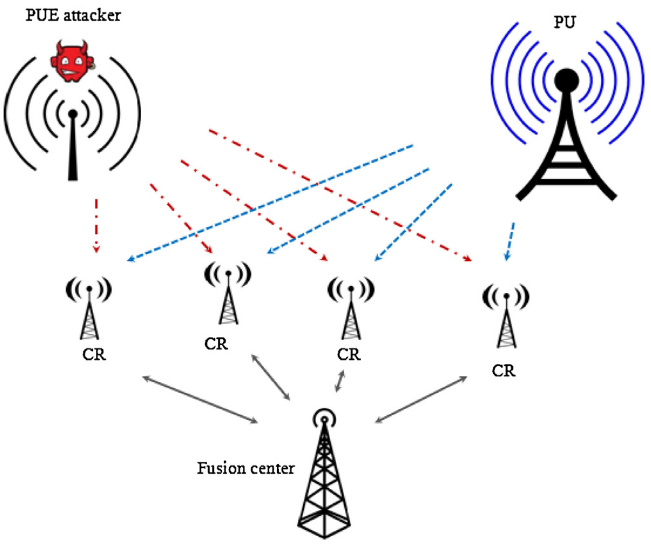

**Fig. 1.** System model for the considered network.

of energy and cannot be a practical assumption. We intend to show that starting from a predefined power budget, the proposed PUEA scheme has more destructive effects on CR spectrum sensing performance than the always present scheme. We consider a smart PUEA in the sense that the attacker is aware of its radio environment and performs its own spectrum sensing similar to a CR. The attacker sends fake signals with desired signal occurrence over licensed frequency bands. We assume a perfect spectrum sensing by the PUEA, i.e., the attacker is able to distinguish exactly between occupied and unoccupied frequency bands allocated to the PU. We investigate CSS rules performed in a CR network using logic data fusion rules of OR/AND in the presence of a PUEA. Moreover, applying energy detection, we propose a new scheme for local spectrum sensing performed in every CR user to detect spectrum holes. Every CR user will declare a hard decision about PU activity and sends it to the fusion center (FC). The FC receives these decisions from its distributed CR users and fuse them using logic OR/AND rules to make a global decision about presence or absence of the primary signal in the radio environment.

This paper extends and generalizes our initial results in [9]. More precisely, in [9], the fake signal occurrence in the presence of the primary signal was considered equal to zero, i.e., the PUEA was solely operating on vacant frequency bands where the PU was absent. In this work, we consider a more general and practical framework for PUEA strategy, i.e., we assume that the PUEA performs a kind of spectrum sensing and hence it may transmit fake signals in both vacant and occupied primary bands. Obviously, due to the generalized scenario considered here, the problem formulation and the probability of detection differ from what we derived in [9] and new results and conclusions are obtained due to the more general system model. Moreover, in contrast to [9], we separately show the effect of fake signal occurrences under presence and under absence of PU in CR spectrum sensing. Then, we investigate the spectrum sensing rules under such smart PUEA.

In contrast to [9], in this work we compare the performance of OR fusion rule with AND fusion rule under considered attacker, and derive appropriate conclusions.

The rest of this paper is organized as follows. Section 1 introduces the considered system model. In Section 3, spectrum sensing in CR network employing OR/AND fusion rules is investigated by taking into account the presence of a PUEA. In Section 4, we combine the considered CSS under PUEA with energy detection spectrum sensing and a new formulation and scheme is proposed to be used in local spectrum sensing of every CR user. Section 5 discusses practical considerations through the paper and proposes a scheme to justify assumptions. Simulation results and discussions are presented in Section 6 and finally, Section 7 concludes the paper.

## 2. System model

As shown in Fig. 1, the system model consists of a PU co-existing with a CR network composed of $N$ CR users and a FC. A malicious user (also referred to as PUEA) is present in the environment with the aim of deceiving the CR network. The PUEA is aware of the radio environment and tries to send fake signals to disrupt CR network activity over licensed bands. It is assumed that the cognitive network applies energy detection for local spectrum sensing in CR users and employs OR/AND fusion rules to make a global decision at the FC.

Let $\sqrt{P_P}x_P^k$ be the signal transmitted by the PU, where, $\sqrt{P_P}$ is a power coefficient and $x_P$ is assumed to be independently and identically distributed (i.i.d.) complex Gaussian random variable with zero mean and a constant known variance $\sigma_P^2$. Since the PUEA makes effort to send signals similar to the PU signal, we assume $x_E$ multiplied by a power coefficient of $\sqrt{P_E}$ is transmitted from the malicious unit and, $x_E$ follows a complex Gaussian distribution with zero mean and a known variance $\sigma_E^2$, as well.

Also $y_i^k$ is defined as the signal received at the $i$th CR user in $k$th time instant. We indicate the presence and absence of the primary signal by $H_1$ and $H_0$, respectively, and the presence and absence of fake PUEA signal by $E_1$ and $E_0$.

Depending on the presence or absence of the PU and PUEA in our model, there would be four possible cases to express the received signal at the $i$th CR users as: $\{E_1, H_1\}$, $\{E_0, H_1\}$, $\{E_1, H_0\}$ and $\{E_0, H_0\}$,

$$y_i^k = \begin{cases} \sqrt{P_P}x_P^k h_{P,i}^k + \sqrt{P_E}x_E^k h_{E,i}^k + n_i^k, & \text{under}\,\{E_1, H_1\}, \\ \sqrt{P_P}x_P^k h_{P,i}^k + n_i^k, & \text{under}\,\{E_0, H_1\}, \\ \sqrt{P_E}x_E^k h_{E,i}^k + n_i^k, & \text{under}\,\{E_1, H_0\}, \\ n_i^k, & \text{under}\,\{E_0, H_0\}, \end{cases} \tag{1}$$

where $n_i^k$ is the additive white Gaussian noise at the $i$th CR user with zero mean and variance $\sigma_{n,i}^2$. $h_{P,i}^k$ is channel gain between PU and $i$th CR user at $k$th time instant, and $h_{E,i}^k$ is channel gain between PUEA and $i$th CR user at $k$th time instant. We assume block fading channels with channel coefficients that can be assumed constant in every detection cycle. Thereby, $k$ can be omitted from $h_{P,i}^k$ and $h_{E,i}^k$.

Then, according to (1), $y_i^k$ will be a complex Gaussian random variable under $\{E_j, H_k\}$ for $j, k \in \{0, 1\}$ as below.

$$y_i^k = \begin{cases} \mathcal{CN}(0, \sigma_{1,i}^2) & \textit{under}\,\{E_1, H_1\}, \\ CN(0, \sigma_{2,i}^2) & \textit{under}\,\{E_0, H_1\}, \\ CN(0, \sigma_{3,i}^2) & \textit{under}\,\{E_1, H_0\}, \\ CN(0, \sigma_{4,i}^2) & \textit{under}\,\{E_0, H_0\}, \end{cases} \tag{2}$$

where one can easily verify that

$$\sigma_{1,i}^2 = P_P\sigma_P^2|h_{P,i}|^2 + P_E\sigma_E^2|h_{E,i}|^2 + \sigma_{n,i}^2,$$

$$\sigma_{2,i}^2 = P_P\sigma_P^2|h_{P,i}|^2 + \sigma_{n,i}^2,$$

$$\sigma_{3,i}^2 = P_E\sigma_E^2|h_{E,i}|^2 + \sigma_{n,i}^2,$$

$$\sigma_{4,i}^2 = \sigma_{n,i}^2.$$