Energy Detection Based Sensing for Secure Cognitive Spectrum Sharing in the Presence of Primary User Emulation Attack

Fatty M. Salem, Maged H. Ibrahim, and I. I. Ibrahim

Department of Electronics, Communications, and Computers, Faculty of Engineering, Helwan University / Cairo, Egypt
{fatty4com, mhii72}@hotmail.com, iiibrahim@softhome.net

***** Corresponding Author: Fatty M. Salem

Received July 14, 2013; Revised July 29, 2013; Accepted September 12, 2013; Published December 31, 2013

** Regular Paper*

***Abstract*:** Spectrum sensing, as a fundamental functionality of Cognitive Radio (CR), enables Secondary Users (SUs) to monitor the spectrum and detect spectrum holes that could be used. Recently, the security issues of Cognitive Radio Networks (CRNs) have attracted increasing research attention. As one of the attacks against CRNs, a Primary User Emulation (PUE) attack compromises the spectrum sensing of CR, where an attacker monopolizes the spectrum holes by impersonating the Primary User (PU) to prevent SUs from accessing the idle frequency bands. Energy detection is often used to sense the spectrum in CRNs, but the presence of PUE attack has not been considered. This study examined the effect of PUE attack on the performance of energy detection-based spectrum sensing technique. In the proposed protocol, the stationary helper nodes (HNs) are deployed in multiple stages and distributed over the coverage area of the PUs to deliver spectrum status information to the next stage of HNs and to SUs. On the other hand, the first stage of HNs is also responsible for inferring the existence of the PU based on the energy detection technique. In addition, this system provides the detection threshold under the constraints imposed on the probabilities of a miss detection and false alarm.

***Keywords*:** Energy detection, Spectrum sensing, Cognitive radio networks, Primary user emulation, Authentication

1. Introduction

The rapid increase in wireless applications and the need to better utilize scarce spectrum have led the Federal Communications Commission (FCC) to revisit the problem of spectrum management. The FCC is considering opening up the licensed bands to unlicensed operations on a non-interference basis to licensed users. In this new paradigm, unlicensed users (secondary users) detect the fellow licensed bands and use them without interfering with the licensed users (primary or incumbent users), thereby increasing the efficiency of spectrum utilization. This method of sharing is often called Dynamic Spectrum Access (DSA).

CR offers the promise of intelligent radio that can learn from and adapt to the environment using Software Defined Radio (SDR) terminal [1], which may be regarded as a programmable radio transceiver whereby the user equipment can reconfigure itself in terms of its capability, functionality and behavior to dynamically accommodate the needs of the user. Therefore, CR is seen as an enabling technology for DSA.

The current research and standardization efforts suggest that one of the first applications of CR technology will be its use for DSA of the fellow TV spectrum bands. The FCC is considering opening up the TV bands for DSA because the TV bands often experience lower and less dynamic utilization compared to other PUs networks, such as cellular networks [2].

The most important challenge for a CR system is to identify the presence of PUs over a wide range of spectra. Therefore, reliable and effective spectrum sensing is the key of CR deployment. On the other hand, in practice, ideal spectrum sensing without miss detection or false alarm of the spectrum holes is impossible due to background noise and wireless fading. A miss detection of

PU is defined as detecting a spectrum hole when the PU's signal is transmitted. On the other side, a false alarm is defined as detecting the presence of a PU when the PU's signal is not transmitted, which would lead to a spectrum usage shortage because the spectrum resources are not utilized by PUs.

The most popular sensing techniques are energy detection [3-5], matched filter [6], and cyclostationary feature detection [7]. Previous studies have examined the performance of such techniques as a conventional detection problem, but none of them considered the effects of a PUE attack [8, 9] on their performance. In a PUE attack, due to the reconfigurability of CRs, it is possible for an adversary to modify the radio software of a CR to change its emission characteristics (i.e. modulation, frequency, power, etc.) so that the emission characteristics resemble those of a PU. The potential impact of a PUE attack depends on the ability of a legitimate SU to distinguish the attacker's signal from the actual PU's signals while conducting spectrum sensing. Such an attack can have severe effects on the normal operation of CR networks [10], representing a great security threat that must be contained effectively in a real deployment of CRNs.

Fig. 1 shows a SU sensing the spectrum in the presence of a PUE attacker. Assume that a total of 10 channels are available to the legacy system, and that channels (1, 4) and (2, 3, 5) are occupied by two PUs within the range of the SU. In a non-adversarial environment, the SU would have sensed the channels (6, 7, 8, 9, 10) as idle. On the other hand, in the presence of a PUE attacker, the set of idle channels sensed by the SU is limited to (6, 10).

This study examined the effects of a PUE attack on the performance of energy detection-based [5] spectrum sensing technique over an Additive White Gaussian Noise (AWGN) channel at the first stage of the helper nodes in the framework. In addition, a complete system was introduced to determine the threshold of the detector to obtain stricter requirements of the probability of a false alarm and the probability of miss detection. In the present management framework, multiple stages of stationary "helper" nodes should be distributed over the coverage area of PUs. The HNs in the first stage are close to PUs, whereas the HNs in the next stages are placed within the PU's coverage area. The HNs in the first stage are responsible for sensing the spectrum relying on an energy detection-based sensing technique, and securely broadcasting the spectrum status information to the next stage of the HNs and/or to the SUs inside their coverage area. On the other hand, the HNs in the next stages are responsible only for forwarding the spectrum status information to the next stage of the HNs and/or to the SUs inside their coverage area.

This paper is organized in six sections as follows: Section 2 summarizes previous works proposed in the area of spectrum sensing. The system characteristics and the model are described in section 3. The performance of the energy detector in the presence of PUE attack is analyzed in section 4. The complete system is described in section 5. Finally, we conclude this paper in section 6.

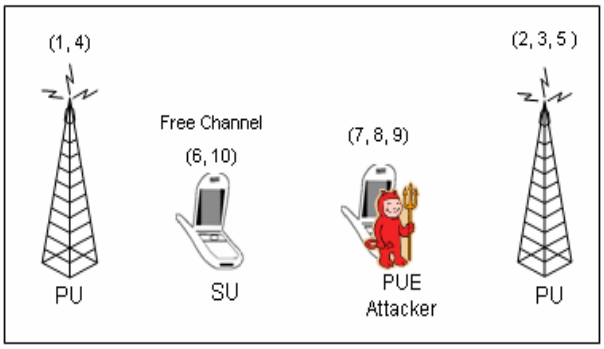

Fig. 1. Primary user emulation attack scenario.

2. Related Work

The present literature for spectrum sensing is still in its early stages of development. A number of different methods for identifying the presence of signal transmissions have been proposed. The spectrum sensing techniques are classified broadly into three main types, transmitter detection or non cooperative sensing, cooperative sensing and interference based sensing.

2.1 Non Cooperative Sensing

This form of spectrum sensing occurs when a CR acts on its own. Transmitter detection techniques are classified further into energy detection, matched filter detection and cyclostationary feature detection [11].

Energy Detection: Energy detection (ED) is a non coherent detection method that detects the PU's signal based on the sensed energy [12]. ED is the most popular sensing technique in cooperative sensing because of its simplicity and no requirement for a priori knowledge of the PU's signal [13].

The ED is said to be a blind signal detector because it ignores the structure of the signal. The ED estimates the presence of a signal by comparing the received energy with a known threshold derived from the statistics of the noise.

On the other hand, ED is always accompanied by a number of disadvantages: i) the sensing time taken to achieve a given probability of detection may be high; ii) detection performance is subject to the uncertainty of noise power; and iii) ED cannot be used to detect the spread spectrum signals [14].

Matched Filter: Matched-filtering is the optimal method for detecting PUs when the transmitted signal is known. The main advantage of matched filtering is the short time to achieve a certain probability of a false alarm or the probability of miss detection compared to other methods. The required number of samples grows as O(1/SNR) for a target probability of a false alarm at low SNRs for matched-filtering [6].

On the other hand, matched-filtering requires a CR to demodulate the received signals. Therefore, it requires perfect knowledge of the signaling features of PUs, such as bandwidth, operating frequency, modulation type and

order, pulse shaping, and frame format. Moreover, because CR needs receivers for all signal types, the implementation complexity of the sensing unit is impractically large [15]. Another disadvantage of matched filtering is the large power consumption by various receiver algorithms needed for detection.

Cyclostationary Feature Detection: Cyclostationary feature detection [7] exploits the periodicity in the received primary signal to identify the presence of the PU's signal. The periodicity is commonly embedded in sinusoidal carriers, pulse trains, spreading code, hopping sequences, or cyclic prefixes of the primary signals. Because of the periodicity, these cyclostationary signals exhibit the features of periodic statistics and spectral correlation, which are not found in stationary noise and interference.

Therefore, cyclostationary feature detection is robust to noise uncertainty and performs better than ED in low SNR regions. Although it requires a priori knowledge of the signal characteristics, cyclostationary feature detection is capable of distinguishing CR transmissions from various types of PUs' signals [15].

On the other hand, this method has its own shortcomings because of its high computational complexity and long sensing time. Because of these issues, this detection method is less common than ED in cooperative sensing.

2.2 Cooperative Sensing

In this approach, the PU's signals are detected reliably by interacting or cooperating with other users. This method can be implemented as either centralized access to the spectrum coordinated or distributed approach [16].

Centralized Access: In centralized cooperative sensing [17, 18], the fusion center (FC) controls the processes of cooperative sensing. All cooperating CR users report their sensing results via the control channel. The FC combines the received local sensing information, determines the presence of PUs, and diffuses the decision back to the cooperating CR users. For local sensing, all CR users are tuned to the selected licensed channel or frequency band where a physical point-to-point link between the PU transmitter and each cooperating CR user for observing the PU's signal is called a sensing channel. For data reporting, all CR users are tuned to a control channel where a physical point-to-point link between each cooperating CR user and FC for sending the sensing results is called a reporting channel. In centralized networks, a base station (BS) is naturally the FC. Alternatively, in CRNs, where a BS is not present, any CR user can act as a FC to coordinate cooperative sensing and combine the sensing information from the cooperating neighbors.

Distributed Cooperative-Sensing: Unlike centralized cooperative-sensing, distributed cooperative-sensing [19] does not rely on a FC to make a cooperative decision. In this case, CR users communicate among themselves and converge to a unified decision on the presence or absence of PUs by iterations. Based on the distributed algorithm, each CR user sends its own sensing data to other users, combines its data with the received sensing data, and determines whether or not the PU is present using a local criterion. If the criterion is not satisfied, the CR users send their combined results to the other users again and repeat this process until the algorithm converges and a decision is reached. In this manner, this distributed scheme may take several iterations to reach a unanimous cooperative decision.

On the other hand, distributed sensing is more advantageous than centralized sensing because there is no need for a backbone infrastructure and it has reduced cost.

2.3 Interference Based Detection

For interference-based spectrum sensing techniques, there are two proposed methods, Interference Temperature Management and Primary Receiver Detection.

Interference Temperature Management: The interference temperature is a measure of the RF power available at a receiving antenna to be delivered to a receiver, reflecting the power generated by the other emitters and noise sources [20].

Primary Receiver Detection: In this method, the interference and/or spectrum opportunities are detected based on the primary receiver's local oscillator leakage power [21].

2.4 Other Techniques

Many other techniques are proposed to enhance the detection of PU's signals in CRNs. As an example, covariance-based detection [22] exploits space-time signal correlation that does not require knowledge of the noise and signal power. This is unlike the energy detection method, which suffers from noise uncertainty problems. Furthermore, hybrid detection methods [23, 24] are proposed to exploit the advantages of covariance-based and energy detection methods for detecting a licensed user.

3. The System Characteristics and Model

This section describes the system characteristics and the model in this design.

3.1 System Characteristics

PU Characteristics (TV Tower): A number of TV towers are transmitting their signals with an Effective Radiated Power of 1000 kW (like WCTV and KTVY towers). The case of Georgia was considered in this study, which is covered by the WCTV Television Tower. The tower broadcasts a high definition digital signal on UHF channel 46 (662-668 MHz) from a transmitter in Metcalf along the Georgia and Florida state line. This TV tower is 609.6 meters (2000 ft) high.

Helper Node and Attacker Characteristics: This section assumes the dipole antenna for receiving and transmitting signals at HNs and at the attacker. Dipole antennas have the same gain and same radiation field. The gain is generally 2.15 dBi. An antenna will have the same gain when receiving as when transmitting, and also the same radiation pattern.

Following the FCC rules [2], the height of the antenna of HNs (and attacker) in the proposed system was assumed to be 30 m because the commission is limiting the maximum antenna height of fixed unlicensed TV Band Devices (TVBDs) to 30 meters above ground level. This will appropriately balance the needs of unlicensed fixed TVBDs to achieve an adequate service range while minimizing the range at which those operations could impact licensed services.

3.2 The Model

System Model: The entities in CRNs are classified into three categories:

Primary Users: They are the legitimate users who have a license to use a specific band. On the other hand, there is no modification of the PUs to accommodate the opportunistic use of the spectrum by SUs.

Secondary Users: These are the unlicensed users allowed to access the licensed frequency bands without interfering with the licensed users to realize more effective and reliable communication.

Helper Nodes: They are stationary nodes distributed over the coverage area of the PUs to enable the SUs to verify the cryptographic signatures included in their signals. In the proposed approach, HNs are distributed in multiple stages. HNs in the first stage are close to the PU and are responsible for (a) detecting the presence of the PU's signals relying on the energy detection-based sensing technique and (b) delivering the spectrum status information to HNs in the next stage and/or SUs inside their coverage areas. The HNs in the next stages are distributed over the coverage area of the PU and are responsible only for forwarding the spectrum status information to the HNs in the next stage and/or SUs inside their coverage areas. Finally, to securely communicate with the SUs, the HNs are initialized with the public/private keys and certificates from a trusted authority.

Adversary Model: In the adversary model, the objective of the adversary is to deny licensed spectrum use to the SUs in CRNs by emulating the PU's signals. Depending on the motivation behind the attack, a PUE attack can be classified as a selfish PUE attack and a malicious PUE attack [25]. The objective of a selfish PUE attacker is to maximize its own spectrum usage by preventing other SUs from competing for that band, whereas a malicious user launching an attack in the same manner is more interested in obstructing the whole dynamic spectrum access process of legitimate SUs rather than monopolizing the utilization of the frequency spectrum resource.

4. Energy Detector in the Presence of PUE Attack

The case of interest is one in which a PUE attack exists. Here, H_p indicates that a PU exists, H_A indicates that PUE attacker exists, and H_0 indicates that PU and PUE attacker are absent. The received signal $y(t)$ is denoted by [5]:

$$y(t)=\begin{cases} n(t), & H_0 \\ h\times s_P(t)+n(t), & H_P \\ h\times s_A(t)+n(t), & H_A \end{cases} \quad (1)$$

where $s_P(t)$ is the PU's signal and $s_A(t)$ is the PUE attacker's signal $n(t)$ is additive white Gaussian noise with a zero mean and variance $N_0 W$ [5], and h is the amplitude gain of the channel. The receiver lets the band-pass filter (BPF) pass to filter the out-of-band noise and adjacent signals, and then pass the A/D converter, squarer and summation device. The test statistic is obtained from [26]:

$$y(t)=\begin{cases} \chi^2_{2TW} & H_0 \\ \chi^2_{2TW}(2\gamma_P) & H_P \\ \chi^2_{2TW}(2\gamma_A) & H_A \end{cases} \quad (2)$$

where γ_P and γ_A are the instantaneous PU's and attacker's signals to noise ratio at the helper nodes in the first stage, respectively. TW is the product of the observation time and interested bandwidth, and is usually written as $m=TW$, where m is an integer. As shown in (2), when a PU and PUE attacker are absent, $y(t)$ obeys the central chi-square distribution with $2m$ degrees of freedom, but when a PU is present, $y(t)$ obeys the noncentral chi-square distribution with $2m$ degrees of freedom and a non-centrality parameter, $2\gamma_P$, and when the PUE attacker is present, $y(t)$ obeys the noncentral chi-square distribution with $2m$ degrees of freedom and a non-centrality parameter $2\gamma_A$.

χ^2_{2TW} is a central Chi-square distribution, whereas $\chi^2_{2TW}(2\gamma_P)$ and $\chi^2_{2TW}(2\gamma_A)$ are noncentral Chi-square distributions. Therefore, the probability of a density function is as follows [27]:

$$f_Y(y)=\begin{cases} \dfrac{1}{2^m\Gamma(m)}y^{(m-1)}e^{-\frac{y}{2}}, & H_0 \\ \dfrac{1}{2}\left(\dfrac{y}{2\gamma_P}\right)^{\frac{(m-1)}{2}}e^{-\frac{(2\gamma_P+y)}{2}}I_{(m-1)}(\sqrt{2\gamma_P y}), & H_P \\ \dfrac{1}{2}\left(\dfrac{y}{2\gamma_A}\right)^{\frac{(m-1)}{2}}e^{-\frac{(2\gamma_A+y)}{2}}I_{(m-1)}(\sqrt{2\gamma_A y}), & H_A \end{cases} \quad (3)$$

where $I_{(m-1)}(\cdot)$ is the $(m-1)^{th}$ order-modified Bessel function of the first kind, and $\Gamma(u)$ is a gamma function defined as: $\Gamma(u)=\int_0^\infty t^{u-1}e^{-t}dt$. On the other hand , $\Gamma(a,b)$ is the incomplete gamma function [28] defined as $\Gamma(a,b)=\int_b^\infty t^{a-1}e^{-t}dt$.

By comparing $y(t)$ with a pre-set threshold, λ, the receiver can determine if PU is present. If $y(t)$ is beyond a given threshold λ , then PU is existing, otherwise PU is absent and uses the spectrum holes for some its own communications. The threshold is selected to achieve a given probability of a false alarm P_F (i.e. an idle channel

is detected as busy), and the probability of a miss detection P_M (i.e. a busy channel is detected as idle). Therefore, the probability of detection can be calculated from

$$\begin{aligned} P_D &= P(y > \lambda \mid H_P) \\ P_D &= \int_{\lambda}^{\infty} \frac{1}{2} \left(\frac{y}{2\gamma_P}\right)^{\frac{(m-1)}{2}} e^{-\frac{(2\gamma_P + y)}{2}} I_{(m-1)}(\sqrt{2\gamma_P y}) dy \\ P_D &= Q_m(\sqrt{2m\gamma_P}, \sqrt{\lambda}) \end{aligned} \tag{4}$$

where $Q_m(..)$ is the generalized Marcum Q function [29] that is defined as:

$$Q_m(a,b) = \int_{b}^{\infty} \frac{x^m}{a^{m-1}} e^{-\frac{(x^2+a^2)}{2}} I_{(m-1)}(ax) dy \tag{5}$$

The probability of missing is expressed as

$$P_M = 1 - P_D \tag{6}$$

On the other hand, the total probability of a false alarm results in the noise and PUE attack presence. Therefore, the total probability of a false alarm can be expressed as

$$P_F = P_{F0}.P(0) + P_{FA}.P(A) \tag{7}$$

where $P(0)$ is the priori probability of the noise, $P(A)$ is the priori probability of the PUE attackers, and P_{F0} can be defined as:

$$\begin{aligned} P_{F0} &= P(y > \lambda \mid H_0) \\ P_{F0} &= \int_{\lambda}^{\infty} \frac{1}{2^m \Gamma(m)} y^{(m-1)} e^{-\frac{y}{2}} dy \\ P_{F0} &= \frac{\Gamma(m, \lambda/2)}{\Gamma(m)} \end{aligned} \tag{8}$$

and,

$$\begin{aligned} P_{FA} &= P(y > \lambda \mid H_A) \\ P_{FA} &= \int_{\lambda}^{\infty} \frac{1}{2} \left(\frac{y}{2\gamma_A}\right)^{\frac{(m-1)}{2}} e^{-\frac{(2\gamma_A + y)}{2}} I_{(m-1)}(\sqrt{2\gamma_A y}) dy \\ P_{FA} &= Q_m(\sqrt{2m\gamma_A}, \sqrt{\lambda}) \end{aligned} \tag{9}$$

Therefore,

$$P_F = \frac{\Gamma(m, \lambda/2)}{\Gamma(m)}.P(0) + Q_m(\sqrt{2m\gamma_A}, \sqrt{\lambda}).P(A) \tag{10}$$

The threshold λ can be determined based on the requirement for the probability of miss detection or the probability of a false alarm. For practical applications, the IEEE 802.22 standard suggests both probabilities of a false alarm and missing of less than 0.1 in terms of detecting the PUs [30]. Herein, a stricter requirement that P_M and $P_F \leq$ 0.02 were assumed, and from Figs. 2 and 3 at γ_P *=15dB*, the threshold λ could be determined to be *314 Joule* to obtain the probability of detection of 0.9801. Therefore, the probability of miss detection will be less than 0.02. On the other hand, Fig. 4 shows that the probability of a false alarm due to noise at λ *=314 Joule* will be $4.47x10^{-62}$.

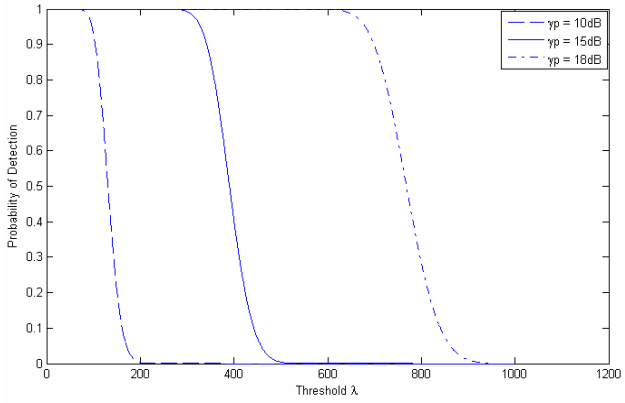

Fig. 2. Probability of detection versus threshold λ.

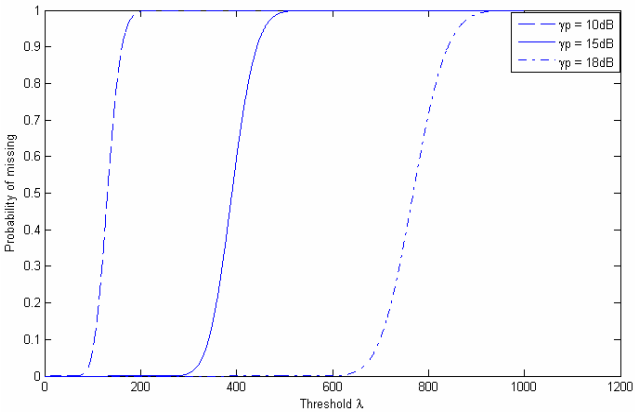

Fig. 3. Probability of missing versus threshold λ.

To determine the total probability of a false alarm, Fig. 5 shows the probability of a false alarm due to the PUE attack versus γ_A. To obtain $P_{FA} = 0.01961$, γ_A should be 19.57. Therefore, the total probability of a false alarm will be less than 0.01. Fig. 6 shows the Receiver Operating Characteristic (ROC) curve.

As a result, a stricter requirements of the probability of a false alarm and the probability of miss detection in the presence of PUE attack can be obtained. The protocols in [22-24] studied the performance of their detectors in a non-adversarial environment but none of them considered the presence of a PUE attack.

This work can be applied to a matched filter but matched-filtering requires the CR to demodulate the received signals. Therefore, it requires perfect knowledge of the PUs' signaling features. Moreover, because CR requires the receivers for all signal types, the implementation complexity of the sensing unit is impractically large [15].

The cyclostationary signals exhibit the features of periodic statistics and spectral correlation, which were not

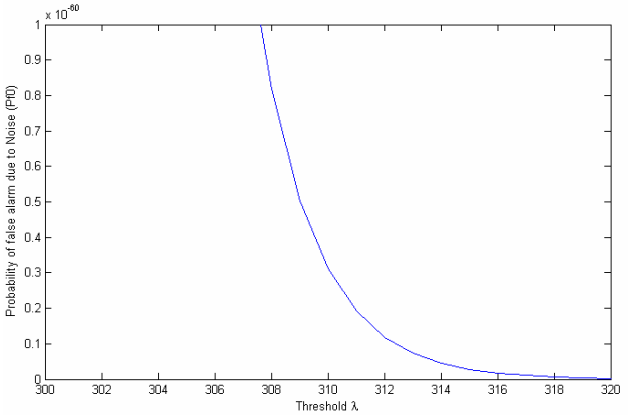

Fig. 4. Probability of false alarm due to noise versus threshold λ.

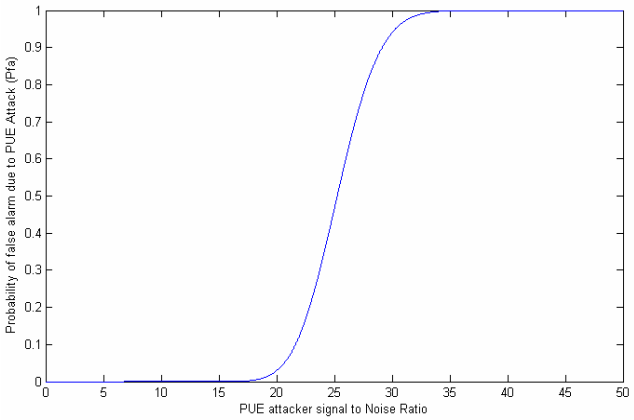

Fig. 5. Probability of false alarm due to PUE attack versus PUE attacker's signal to noise ratio γ_A.

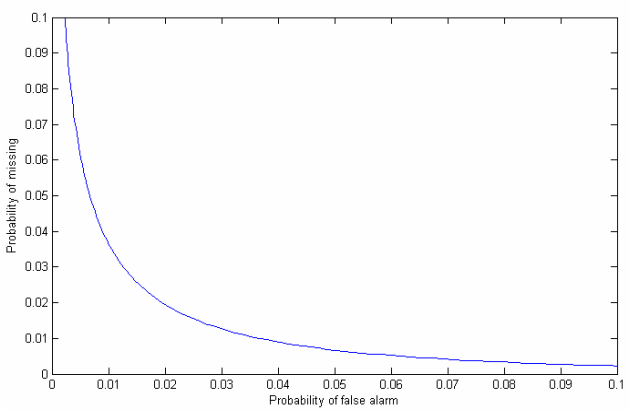

Fig. 6. Receiver operating characteristics curve.

found in stationary noise and interference. Therefore, a cyclostationary feature detector provides a way of separating the desired signals from noise. On the other hand, PUE may modify the radio software of a CR to change its emission characteristics, so that the emission characteristics and cyclostationary feature resemble those of a PU. As a result, a hybrid energy detection and cyclostationary feature detection may be used to enhance the algorithm to detect the free spectrum.

5. The Complete System

In this section, we determine the distance between HNs in the first stage and PU are determined, the interaction between CR entities is described, and the cost of the HNs and the optimal number of HNs in the proposed system are evaluated.

5.1 Distance between HNs in the First Stage and PU

To determine the distance between the HNs in the first stage and the PU, this study considered a ground reflection (two-ray) model for calculating the power level of a received signal over a distance, d. The received power level is given by [31]:

$$P_r(d) = P_t G_t G_r \frac{h_t^2 h_r^2}{d^4 L} \tag{11}$$

where P_t is the transmitted power, $P_r(d)$ is the received power, which is a function of the T-R separation, G_t, h_t are the transmitter gain and height, respectively, G_r, h_r are the receiver antenna gain and height, respectively, d is the T-R separation distance in meters, and L is the system loss factor not related to propagation ($L \geq 1$).

Fig. 7 plots, using matlab, the received power versus the distance between the HNs in the first stage and PU. Fig. 8, however, plots the SNR γ_P versus the distance between the HNs in the first stage and PU at different values of noise variance.

Finally, following the FCC rules, the unlicensed users were assumed to have a maximum transmission output power that is within the range from a few hundred milliwatts to a few watts [2]. Therefore, Fig. 9 shows the probability of a false alarm versus the minimum distance between the attacker and HNs in the first stage at an attacker's transmitting power of 4 watts and a noise variance of *10 dBm*.

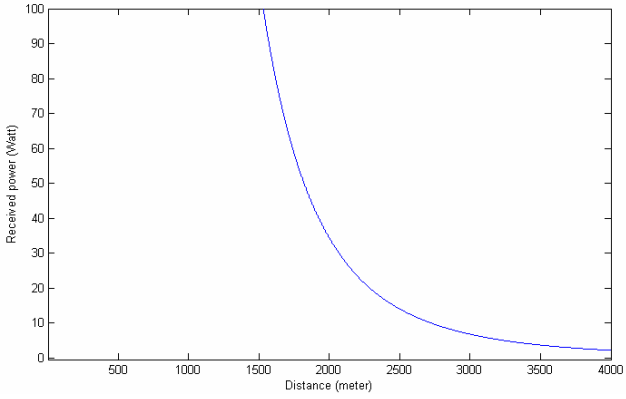

Fig. 7. Received power at HN versus distance between HNs in the first and the PU.

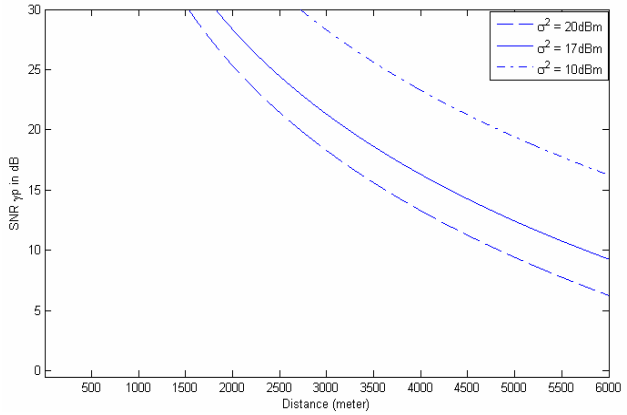

Fig. 8. SNR γ_P at HNs versus distance between HNs in the first stage and the PU.

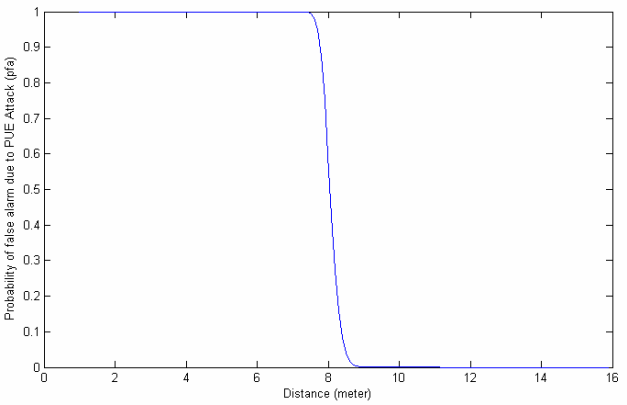

Fig. 9. Probability of a false alarm due to a PUE attack versus the minimum distance between the PUE attacker and HNs at the first stage.

To obtain the target probability of detection (calculated previously at $\gamma_P = 15dB$), the HNs in the first stage can be positioned *4310* meters away from the PU to achieve the required signal to noise ratio ($\gamma_P = 15dB$). Therefore, the maximum possible distance between HNs in the first stage and the PU than that of the scheme in [32] can be increased to obtain the same probabilities of detection and less probability of false alarm.

At a low typically value of the noise variance (10 dBm) (i.e. at the maximum typically SNR γ_A), to keep γ_A less than 19.57 and keeping the total probability of false alarm less than 0.02, the distance between the attacker and HNs in the first stage must be larger than 8.5 m.

5.2 Interactions between CR Entities

HNs at the first stage are responsible for first detecting the presence of the PU's signal and then forwarding the spectrum status information to the HNs in next stages and/or SUs in their coverage area. When the signal received at HNs at the first stage exceeds the threshold, λ, it is detected as the PU's signal, otherwise, it is either due to noise or a PUE attack.

On the other hand, as the HNs are assumed to have a maximum transmission output power that is within the range of a few hundred milliwatts to a few watts [2], HNs in the first stage are unable to deliver the spectrum information directly to all the SUs existing in the wide coverage area of the PUs. Therefore, it is an essential need for the multiple next stages of HNs.

To broadcast the spectrum status information to the HNs in the next stage and/or to the SUs within their coverage area, each HN_i in the first stage transmits the following information periodically: $m_i \,||\, sig_i(m_i)$, where $||$ denotes concatenation, m_i is an k-bits occupancy vector indicating the set of k-channels where legitimate PUs are active, whereas $sig_i(m_i)$ denotes the cryptographic signature of HN_i on the message m_i.

When receiving the spectrum information, HNs in the next stage or/and SUs will verify the authenticity and integrity of the received message m_i by verifying the validity of the cryptographic signature $sig_i(m_i)$. Message m_i, which fails to be authenticated, is discarded. If the message is verified, the SUs will accept the contents of the message, whereas each HN_j in the next stage will retransmit the received spectrum information to the subsequent stages of the HNs as follows: $m_i \,||\, sig_j(m_i)$, where $sig_j(m_i)$ denotes the cryptographic signature of HN_j on the message m_i.

5.3 Cost of the Helper Nodes

Helper nodes in the proposed approach can be classified into the following:

Helper nodes at the first stage: They are responsible for sensing the spectrum based on the energy detection method and forwarding the signed spectrum information to HNs in the next stages.

In the energy detection-based spectrum-sensing method, the signal is passed through the band pass filter of the bandwidth W and is integrated over the time interval. The output from the integrator block is then compared with a predefined threshold. This method has the advantage of low implementation and computational complexities compared to the matched filter and cyclostationary feature detection methods. When considering the general purpose of spectrum sensing with low complexity, the energy detection technique is decidedly the most feasible spectrum sensing scheme for detecting the spectrum [33]. This explains why this paper focuses on spectrum sensing using energy detection.

As the cryptographic algorithms take a significant amount of time if the algorithms are implemented in software, the current advancements in technologies provide hardware cryptographic coprocessors for use in securing financial applications, e-commerce and SSL (Secure Socket Layer) transactions. These cryptographic coprocessors can perform 1250 Digital Signature Algorithms (DSA) per second and 620 DSA signature verifications per second [34]. Therefore, the signing at the first stage of HNs will take 8×10^{-4} *s*.

Helper Nodes at the next stages: They are responsible only for verifying the spectrum information received from the previous stage and signing the verified spectrum information to be forwarded to the next stage of the HNs. Therefore, HNs in the next stage performs one signature and one signature verification, which will take 24.13×10^{-4} *s*.

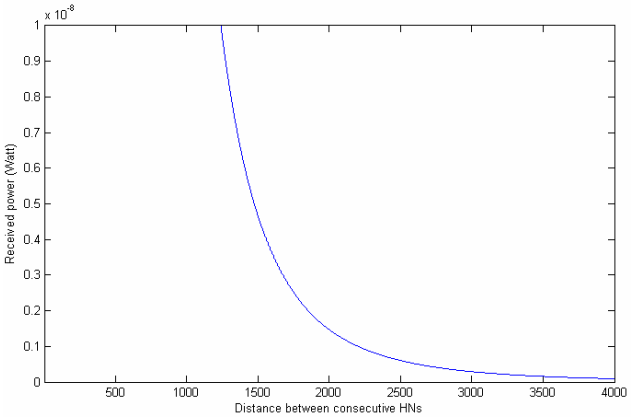

Fig. 10. Received power versus distance between consecutive HNs.

5.4 Optimal Number of Helper Nodes

To determine the number of stages, it is important to establish the maximum acceptable distance between any two consecutive HNs. To guarantee good quality, the power of the transmitted signal should be in balance at the edge of the cell. The main idea behind the power budget calculations is to receive the output power level of transmitter as a function of the receiver sensitivity levels. Therefore a ground reflection (two-ray) model was considered for calculating the power level of a received signal at the HNs over a distance *d*.

According to the FCC specifications, the fixed TVBDs operate from a known, fixed location, and can use a transmit power of up to 4W EIRP. Fig. 10 plots the received power as a function of the distance between the consecutive HNs at a transmitting power of 4W EIRP.

At a 3000 m separation, the received power will be 3×10^{-10} watt, which means that the HN sensitivity levels will range from -65 to -70 dBm, which is a practical level. In the laboratory tests of the TV signals, the Phase II prototype devices can detect a ‘‘clean,’’ i.e. unfaded, DTV signal on a single channel at levels in the range of -116 to -126 dBm. The detection threshold sensitivity of the devices ranged from -106 to -128 dBm when the recorded off-air DTV signals were used.

As the IEEE 802.22 standard is designed to provide broadband wireless access services over a large area (typically 33km radius), 10 levels of HNs need to be distributed over the coverage area of PU. On the other hand, the number of HNs in each level will be increased when moving away from the PU because the HNs were proposed to be distributed in circles over the coverage area of the PU.

As an example, if the first stage of HNs is located at a distance 4300 m away from the PU, the fourth stage is located at 13300 m away from the PU. Therefore, the circumference of this level is 83600 m, which requires approximately 28 HNs with a 3000 m coverage area.

6. Conclusion

This paper introduced an approach for authenticating the PUs’ signals in CRNs to maximize a SU’s transmission opportunity while minimizing the interference that may be introduced to the PU by the SUs. This approach integrated the cryptographic signatures and energy detection based spectrum sensing technique to enable PU detection in a hostile environment. The HNs distributed over the coverage area of the PUs serve as a bridge to enable the SUs to verify the cryptographic signature carried by the HNs’ signals, whereas the HNs authenticate the PU’s signals relying on the energy detection-based spectrum sensing technique. A key contribution in this paper is an investigation of the performance of the energy detection-based spectrum sensing technique in the presence of PUE attacks. The proposed scheme showed significant performance advantages in terms of the probability of miss detection and the probability of a false alarm. In addition, this approach successfully accommodated the opportunistic use of the spectrum by SUs without modification to the PUs, which conforms to the FCC’s requirements.

References

[1] Ulversoy Tore, “Software defined radio: Challenges and opportunities,” IEEE Communications Surveys & Tutorials, vol. 12, no. 4, pp. 531 – 550, 2010. Article (CrossRef Link)

[2] Federal Communications Commission, “Facilitating opportunities for flexible, efficient, and reliable spectrum use employing spectrum agile radio technologies,” ET Docket No. 03-108, December, 2003. Article (CrossRef Link)

[3] Tanuja S. Dhope (Shendkar), Dina Simunic and Antun Kerner, “Analyzing the performance of spectrum sensing algorithms for IEEE 802.11 af standard in cognitive radio network,” Studies in Informatics and Control, vol. 21, no. 1, pp. 93-100, 2012. Article (CrossRef Link)

[4] Lehtomäki Janne, “Analysis of energy based signal detection,” PhD. dissertation, University of Oulu, Finland, December, 2005. Article (CrossRef Link)

[5] H. Urkowitz, “Energy detection of unknown deterministic signals,” in the Proc. of IEEE, vol. 55, no. 4, pp. 523–531, 1967. Article (CrossRef Link)

[6] R. Tandra and A. Sahai, “Fundamental limits on detection in low SNR under noise uncertainty,” in Proc. of IEEE International Conference on Wireless Networks, Communication and Mobile Computing, pp. 464–469, June, 2005. Article (CrossRef Link)

[7] A. Al-Dulaimi, N. Radhi, N., H. S. Al-Raweshidy, “Cyclostationary detection of undefined secondary users,” Third International Conference on Next Generation Mobile Applications, Services and Technologies, pp. 230 – 233, 2009. Article (CrossRef Link)

[8] R. Chen, J.-M. Park, and J. H. 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, 2008. Article (CrossRef Link)

[9] T. Newman and T. Clancy: 'Security threats to cognitive radio signal classifiers," in Proc. of the Virginia Tech Wireless Personal Communications Symposium, June 2009. Article (CrossRef Link)

[10] A Sethi, TX Brown, "Hammer model threat assessment of cognitive radio denial of service attacks," 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, pp. 1–12, 2008. Article (CrossRef Link)

[11] D. Bhargavi and C.R. Murthy, "Performance comparison of energy, matched-filter and cyclostationarity-based spectrum sensing," IEEE Eleventh International Workshop of Signal Processing Advances in Wireless Communications (SPAWC), pp. 1-5, June, 2010. Article (CrossRef Link)

[12] A. Shahzad, "Comparative analysis of primary transmitter detection based spectrum sensing techniques in cognitive radio systems," Australian Journal of Basic and Applied Sciences, INSInet Publication, vol 4, no. 9, pp. 4522-4531, 2010. Article (CrossRef Link)

[13] D. Cabric, A. Tkachenko, and R. Brodersen, "Spectrum sensing measurements of pilot, energy, and collaborative detection," in Proc. of IEEE Military Communication Conference, pp. 1–7, October, 2006. Article (CrossRef Link)

[14] Ian F. Akyildiz and Brandon F. Lo, Ravikumar, "Cooperative spectrum sensing in cognitive radio networks: A survey," Physical Communication (Elsevier), vol. 4, no. 1, pp: 40-62, 2011. Article (CrossRef Link)

[15] D. Cabric, S. Mishra and R. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in Proc. of Asilomar Conference on Signals, Systems and Computers, pp. 772–776, November, 2004. Article (CrossRef Link)

[16] I. F. Akyildiz, W. Y. Lee, M. C. Vuranand S. Mohanty, "NeXt generation / dynamic spectrum access / cognitive radio wireless networks: A survey," Computer Networks Journal (Elsevier), vol. 50, no. 13, pp. 2127–2159, September, 2006. Article (CrossRef Link)

[17] C. Sun, W. Zhang and K. B. Letaief, "Cooperative spectrum sensing for cognitive radios under bandwidth constraints," in Proc. of IEEE Wireless Communication and Networking Conference, pp. 1–5, March, 2007. Article (CrossRef Link)

[18] J. Lund´en, V. Koivunen, A. Huttunen and H. V. Poor, "Spectrum sensing in cognitive radios based on multiple cyclic frequencies," in Proc. of IEEE International Conference on Cognitive Radio Oriented Wireless Networks and Communication (Crowncom), July-August, 2007. Article (CrossRef Link)

[19] M. Gandetto and C. Regazzoni, "Spectrum sensing: A distributed approach for cognitive terminals," IEEE Journal on Selected Areas in Communications, vol. 25, no. 3, pp. 546–557, April, 2007. Article (CrossRef Link)

[20] O. Simeone, J. Gambini, U. Spagnolini and Y. Bar-Ness, "Cooperation and cognitive radio," in Proc. of IEEE CogNet Workshop, pp. 6511 – 6515, August, 2007. Article (CrossRef Link)

[21] B. Wild and K. Ramchandran, "Detecting primary receivers for cognitive radio applications," in Proc. of IEEE New Frontiers in Dynamic Spectrum Access Networks DySPAN, pp. 124–130, December, 2005. Article (CrossRef Link)

[22] T. Dhope and D. Simunic, "Performance analysis of covariance based detection in cognitive radio," in Proc. Of 35th Jubilee International Convention MIPRO, pp. 737 - 742, May, 2012. Article (CrossRef Link)

[23] T. Dhope and D. Simunic, "Hybrid detection method for cognitive radio," 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp: 1-5, September, 2011. Article (CrossRef Link)

[24] T. Dhope and D. Simunic, "Hybrid detection method for spectrum sensing in cognitive radio," 35th Jubilee International Convention MIPRO, pp. 765 – 770, May, 2012. Article (CrossRef Link)

[25] R. Chen and J. M. Park, "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks," IEEE Workshop on Networking Technologies for Software Defined Radio Networks, pp. 110-119, 2006. Article (CrossRef Link)

[26] T. Yand and H. Arslan, "A survey of spectrum sensing algorithms for Cognitive Radio applications," IEEE Communications Surveys and Tutorials, vol. 11, no. 1, pp. 116-130, May, 2009. Article (CrossRef Link)

[27] Kostylev, "Energy detection of a signal with random amplitude," in Proc. of IEEE International Conference on Communication, pp. 1606 - 1610, August, 2002. Article (CrossRef Link)

[28] I. S. Gradshteyn and I. M. Ryzhik, Table of integrals, series, and products, Academic Press, 5th edition. 1996. Article (CrossRef Link)

[29] A. H. Nuttall, "Some integrals involving the QM function," IEEE Transactions on Information Theory, vol. 21, no. 1, pp. 95-96, January, 1975. Article (CrossRef Link)

[30] C. Cordeiro, K. Challapali and M. Ghosh, "Cognitive phy and mac layers for dynamic spectrum access and sharing of tv bands," in Proc. of the first international workshop on Technology and policy for accessing spectrum, ACM, 2006. Article (CrossRef Link)

[31] Theodore S. Rappaport, Wireless communications principles and practice, Prentice Hall, 2nd edition. 2002. Article (CrossRef Link)

[32] Fatty M. Salem, Maged Hamada Ibrahim and I. I. Ibrahim, "A primary user authentication scheme for secure cognitive TV spectrum sharing," International Journal of Computer Science Issue, vol. 9, no. 4, pp. 157-166, July 2012. Article (CrossRef Link)

[33] Takeshi Ikuma and Mort Naraghi-Pour, "A comparison of three classes of spectrum sensing

techniques," IEEE GLOBECOM proceeding, pp. 1-5, November, 2008. Article (CrossRef Link)
[34] SafeXcel-1841 Product Brief, SafeNet Inc., Belcamp, MD, 2005. Article (CrossRef Link)

Fatty M. Salem Received her B.Sc. degree in communications and computers engineering from Helwan University, Cairo, Egypt, in 2007. She received her M.S. degree in network security from Helwan University, in 2010. She is currently working toward a PhD degree in network security at Helwan University. She is a Teaching Assistant in Helwan University. Her main interests include systems, cryptography, and network security.

Maged Hamada Ibrahim He received his BSc in communications and computers engineering from Helwan University, Cairo; Egypt, in 1995. He received his MSc and PhD in engineering cryptography and network security systems from Helwan University in 2001 and 2005 respectively. Currently, he is an associate professor since 2013 at Helwan University and also joining several network security projects in Egypt. His main interest is engineering cryptography and communications security. More specifically, working on the design of efficient and secure cryptographic algorithms and protocols, in particular, secure distributed multiparty computations, public key infrastructures, digital signatures, digital rights management protocols and non-cryptographic solutions to communication security problems. Other things that interest him are number theory and the inspection of mathematics for designing secure and efficient cryptographic schemes.

I. I. Ibrahim Received his B.Sc. degree with honor in communications engineering from Helwan University, Cairo, Egypt, in 1976. He received his M.S. in communications from Cairo University, Cairo, Egypt in 1983 and PhD in communications from Queen University, Belfast, UK in 1987. since 2001, he has been a full professor of electronics and communications engineering at Helwan University. He has more than eighty scientific publications in the field of digital signal processing and wireless communications.