A Primary User Authentication Scheme for Secure Cognitive TV Spectrum Sharing

Fatty M. Salem[1], Maged H. Ibrahim[2] and I. I. Ibrahim[3]

**[1,2,3]Department of Electronics, Communications and Computers, Helwan University
Cairo, 02012, Egypt**

Abstract

Cognitive radio is being intensively investigated by regulatory bodies as the enabling technology for opportunistic access to the TV white spaces. The successful deployment of cognitive radio networks and the realization of their benefits depend on the assignment of essential security challenges to resist misuse of the systems. In this paper, we propose a primary user authentication scheme in the presence of attackers. Our system is based on the deployment of multiple stages of "helper" nodes, helper nodes in the first stage are fixed and close to primary user, while helper nodes in the next stages are placed within the primary user's coverage area. Helper nodes are responsible for sensing the spectrum based on the received signal power detection scheme, and broadcasting the spectrum information to secondary users. Compared to prior work, our system can provide a stricter requirement for probability of false alarm and probability of missing.

Keywords: *Cognitive Radio Networks, Dynamic Spectrum Access, Opportunistic Spectrum Sensing, Primary User Emulation, Byzantine Failure.*

1. Introduction:

Dynamic Spectrum Access (DSA) refers to communication techniques that exploit the temporal variations of the licensed channels making them suitable candidates for secondary access by unlicensed wireless devices.

Cognitive Radio [1] (CR) can be seen as one possible approach of implementing DSA especially on Software Defined Radio (SDR) platforms. Originally CR referred to software radios extended with a self-awareness about their characteristics and requirements, in order to determine an appropriate radio protocol to be used. However, since then the research has focused especially on the DSA sub-problem of cognitive radio. Indeed, cognitive radio has become a general research term for radio technology where the radios are trying to use the holes of the licensed spectrum. A CR needs to carry out spectrum sensing to identify fallow spectrum bands. Ensuring the trustworthiness of the spectrum sensing process is important in the Opportunistic Spectrum Sensing (OSS) paradigm. In the OSS paradigm, Secondary Users (SUs) equipped with CRs opportunistically utilize fallow bands after identifying them via spectrum sensing. SUs are permitted to operate in licensed bands only on a noninterference basis to the Primary Users (PUs). A SU that detects the presence of primary signals in the current band must immediately switch to another band.

In a *Primary-User Emulation* (PUE) attack, the attacker can emulate the PU, and can thus convince other SUs that the PU is using the spectrum when it is not. This can be achieved by mimicking characteristics of primary signal. The potential impact of a PUE attack depends on the legitimate SUs' ability to distinguish the attacker's signals and actual primary signals.
Hence, It is necessary to have a secure PU detection method that can authenticate the PU in the presence of attackers. At first glance, a cryptographic signature seems to be a good candidate for this task. Unfortunately, Federal Communications Commission (FCC) states that "no modification to the incumbent system (i.e., primary user) should be required to accommodate opportunistic use of the spectrum by secondary users" [2]. As a result, any solution that requires changes to PUs is not desirable.

Another security threat is closely related to spectrum sensing. This security problem threatens the reliability of the distributed spectrum sensing (DSS) process. In distributed spectrum sensing, individual nodes send their local sensing data to a fusion center (or data collector), which processes the data to determine the final sensing decision. Many proposed approaches suggest that DSS enhances sensing accuracy and reduces the need for very sensitive sensing technology, which can be costly [3, 4, 5], when compared with individual spectrum sensing. However, DSS raises a security concern: Byzantine failures. Byzantine failures may be caused by either malfunctioning sensing terminals or spectrum sensing data falsification (SSDF) attacks (where a malicious SU intentionally sends falsified local spectrum sensing report to the data collector). In either case, incorrect spectrum sensing data is reported to the fusion center, which can affect the accuracy of the sensing decision.

CR is being intensively investigated by regulatory bodies as the enabling technology for opportunistic access to the so-called TV white spaces (TVWS). White space is the term used by the FCC for TV white space spectrum. This VHF and UHF spectrum provides superior propagation and building penetration compared to other unlicensed spectrum in other bands. However, realization of this networks depends on the assignment of essential security challenges. The FCC rules specify a number of requirements on these cognitive radio networks.

FCC RULES:

The main features of the FCC rules are as follows:

- The Commission provides for the operation of unlicensed radio transmitters in Part 15 of its rules. Under these rules, unlicensed devices are allowed to operate on frequencies shared with authorized services at relatively low power, *i.e*., at output power levels of 1 watt or less. Operation under Part 15 is subject to the condition that a device does not cause harmful interference to authorized services, and that it must accept any interference received. The rules adopted in the *Second Report and Order* [6] permit unlicensed devices to operate on TV channels that are not in use in their vicinity, subject to specific technical requirements that are intended to prevent interference to TV broadcasting and other authorized users of the TV bands.
- The broadcast television service operates under Part 73 of the Commission's rules. Full service TV stations operate on six-megahertz channels designated 2 to 51 in four bands of frequencies in the VHF and UHF regions of the radio spectrum (54-72 MHz, 76-88 MHz, 174-216 MHz and 470-698 MHz). To avoid interference between TV stations, stations on the same and adjacent channels must comply with a number of technical provisions that effectively require that significant distances be maintained between co-channel and adjacent channel stations. The service range of a TV station is shorter than its interference range, so there are areas between stations that are outside of TV station service areas where channels are unused. In addition, television stations operate with relatively high antennas and high power so that their signals can propagate to, and serve viewers at, significant distances.
- The devices operating according to these rules are referred to as TV Band Devices (TVBDs) by the FCC. There are two classes of TV band devices: fixed and personal/portable. The portable devices are further divided into Mode I and Mode II devices.
- The Commission is limiting the maximum antenna height of fixed unlicensed TVBDs to 30 meters above ground level and find that this will appropriately balance the needs of unlicensed fixed TVBDs to achieve adequate service range while minimizing the range at which those operations could impact licensed services.
- Fixed devices are permitted to transmit up to 30 dBm (1 watt) with up to 6 dBi antenna gain, while portable devices are permitted to transmit up to 20 dBm (100 mw) with no antenna gain. Fixed devices are permitted to use a higher gain antenna as long as the transmit power is decreased dB-for-dB for any antenna gain above 6 dBi.
- The White Space Coalition argues that it is not necessary for the Commission to specify a channel availability minimum sensing period because the optimum check time will be dictated by the algorithms implemented by each manufacturer to meet the minimum detection threshold. It also submits that because of the "always on" nature of services in the TV bands, a re-check interval of one minute is more appropriate than 10 seconds, because the shorter 10 second interval would reduce the throughput of TV band devices. The White Space Coalition states that a period of 10 seconds after detecting a station is sufficient and appropriate for a device to vacate a channel, and that it is unnecessary to specify a nonoccupancy period because devices would be required to confirm that a channel is unoccupied before commencing operation. IEEE 802.18 recommends that we require that TV band devices check for the presence of wireless microphones every two seconds, but states that a recheck interval of 10 seconds or longer is adequate for Digital TV (DTV) signals.

2. Previous Work:

Cognitive radio has an important property that it detects the unused spectrum and shares it without harmful interference to PUs. The spectrum sensing enables the cognitive radio to detect the spectrum holes. Transmitter detection technique is further classified into energy detection, matched filter detection and cyclostationary feature detection.

Energy detection: In energy detection, the output signal of a bandpass filter with bandwidth W is squared and integrated over the observation interval T. The output would be the measure of primary signal's presence, which can be compared with a detection threshold to decide whether a licensed user is present or not. Implementation with nyquist sampling A/D converter, square-law device and integrator [7], [8]. An energy detector can be implemented similar to a spectrum analyzer by averaging frequency bins of a FFT. This technique has the advantages that it has low complexity, ease of implementation and faster decision making probability. In addition, energy detection is the optimum detection if the PU's signal is not known. It also has disadvantages: (1) The threshold used in energy selection depends on the noise variance. (2) Inability to differentiate the interference from other SUs sharing the same channel and with the PU. (3) It has poor performance under low SNR conditions. This is because the noise variance is not accurately known at the low SNR, and the noise uncertainty may render the energy detection useless.

Matched filter detection: it is the optimum method for detection of PUs when the transmitted signal is known [9]. The main advantage of matched filtering is the short time to achieve a certain probability of false alarm or probability of misdetection [10].

This technique has the advantage that it requires less detection time because it requires less time for higher processing gain. However, matched-filtering requires cognitive radio to demodulate received signals. Hence, it requires perfect knowledge of the PU's signaling features. Moreover, since cognitive radio needs receivers for all signal types, the implementation complexity of sensing unit is impractically large [11]. Another disadvantage is large power consumption as various receiver algorithms need to be executed for detection.

Cyclostationary feature detection: It has been introduced as a complex technique for recognition of modulated signals in the presence of noise and interference [11]. To identify the received primary signal, it exploits periodicity of modulated signals couple with sine wave carriers, hopping sequences, cyclic prefixes, etc. Due to the periodicity, these cyclostationary signals exhibit the features of periodic statistics and spectral correlation, which is not found in stationary noise and interference [12], [13].

The main advantage of the feature detection is that it can differentiate between the noise energy and the modulated signal energy. Furthermore, cyclostationary feature detection can detect the signals with low SNR. This technique also has disadvantages that the detection requires long observation time and higher computational complexity [12], [14]. In addition, feature detection needs the prior knowledge of the PUs.

A centralized architecture is proposed where a central controller is responsible for allocation of bandwidth to intended users. In order to obtain complete information of unused frequency (spectrum hole), sensing is considered to be decentralized. In each SU, one transceiver is dedicated for control and second a SDR based which scans the availability of spectra in its vicinity and forwards the information of these spectrum holes to the master/controller in case the SUs form an infrastructure less network or to the base station in case of infrastructure based network. The bandwidth is allocated to SU based on the number of availability of unoccupied channels [15].

A spectrum sensing technique using group intelligence is proposed where multiple users can learn from the group's information to reach a correct conclusion. It is proposed an adaptive threshold based on group intelligence accuracy of the spectral occupancy has improved by training the SU. This training is done with the help of the global decision derived from other SUs in the network. This approach is suitable in two ways. (1) To indicate the presence or absence of the PU, separate training signal are not required. Training can be done continually, not limited to the training signal. (2) Training signal derived from spatially diverse SUs should be robust and less sensitive to local channel fading. Together the SUs are expected to reach a common decision, which should be correct in all situations [16].

The approach in [17] thus proposes a secure trust-based authentication approach for Cognitive Radio Networks (CRNs). A SU's trust value is determined from its previous trust behavior in the network and depending on this trust value, it is decided whether or not this CR node will obtain access to the PU's free spectrum. Many other cooperative sensing schemes are proposed in [18, 19, 20]. These approaches have the disadvantage of attacks on location privacy of SUs. It is expected to compromise SUs' location privacy by correlating their sensing reports and their physical locations.

3. The Model

Now, we aim to describe the system and the adversary model.

3.1 System Model

Entities in CRs are classified into three categories:

Primary Users: Primary users are the licensed users who are assigned with certain channels. However, following the FCC rules, no any modification to PUs to provide secure communication in CRNs.

Secondary Users: Secondary users are the unlicensed users who are allowed to use the channels assigned to a PU only when they do not cause any harmful interference to the PU.

Helper Nodes: They are fixed nodes serving as “bridges”. They can detect the presence of the PU, and enable SUs to verify the cryptographic signatures included in their signals. In our proposed protocol, we classified the helper nodes into two levels. Helper nodes in the first level are close to the PU and responsible for detecting the presence of the primary signals. Helper nodes in the second level are distributed over the coverage area of the PU and responsible for delivering the spectrum information to SUs. Finally, to securely communicate with SUs, helpers are initialized with public/private keys and certificates from a trusted authority.

3.2 Adversary Model

In the adversary model, the objective of the adversary is to deny using licensed spectrum to other SUs in CRN by emulating primary user signals. A PUE attack can be classified as either a selfish PUE attack or a malicious PUE attack:

Selfish PUE attacks: In this attack, an attacker’s objective is to maximize its own spectrum usage. When selfish PUE attackers detect a fallow band, they prevent other SUs from using that band by transmitting signals that emulate the signal characteristics of primary-user signals.

Malicious PUE attacks: The objective of this attack is to obstruct the dynamic spectrum access process of legitimate SUs; that is, prevent legitimate SUs from using fallow licensed spectrum bands, causing denial of service. Unlike a selfish attacker, a malicious attacker does not necessarily use fallow spectrum bands for its own communication purposes. Both attacks could have disruptive effects on CRNs.

4. Existing Tools:

The Byzantine failure problem can be caused by malfunctioning sensing terminals or spectrum sensing data falsification (SSDF) attacks. Each case could affect the accuracy of the sensing decision. We suggest the Weighted Sequential Probability Ratio Test (WSPRT) [21] to improve robustness against Byzantine failures.

4.1 Weighted Sequential Probability Ratio Test (WSPRT):

WSPRT is composed of two steps. The first step is a reputation maintenance step, and the second step is the actual hypothesis test. In the reputation maintenance step, a sensing terminal’s reputation ratings are allocated based on the accuracy of a sensing terminal’s sensing. The reputation value is set to zero at the beginning; whenever its local spectrum sensing report is consistent with the final sensing decision, its reputation is incremented by one; otherwise it is decremented by one. Under this rule, assuming N_i’s reputation value is r_i, the last sensing report N_i sent to data collector N_0 is u_i, and the final decision is u, then r_i is updated according to the following relation: $r_i \leftarrow r_i + (-1)^{u_i + u}$.

The hypothesis test step of WSPRT is based on Sequential Probability Ratio Test (SPRT) [22]. The idea of WSPRT is to modify the likelihood ratio used in the SPRT so that the decision variable also takes a sensing terminal’s reputation into consideration. The new decision variable is:

$$W_n \leftarrow \prod_{i=0}^{n} \left(\frac{P[u_i \mid H_1]}{P[u_i \mid H_0]} \right)^{w_i} \qquad (1)$$

Where w_i is defined as the weight of N_i and is a function of r_i : $w_i = f(r_i)$. The function of w_i and $f(\cdot)$ is as follows:

$$w_i = f(r_i) = \begin{cases} 0 & r_i \le -g \\ \dfrac{r_i + g}{\max(r_i) + g} & r_i > -g \end{cases} \qquad (2)$$

The variable g(> 0) is used to ensure that enough weight is allocated to a sensing terminal that has a slightly negative reputation value.

The fusion decision is based on the following criterion:

$$\begin{cases} W_n \ge \eta_1 \Rightarrow \text{accept } \mathrm{H}_1 \\ W_n \le \eta_0 \Rightarrow \text{accept } \mathrm{H}_0 \\ \eta_0 < W_n < \eta_1 \Rightarrow \text{take another observation} \end{cases} \qquad (3)$$

The values of η_1 and η_0 are decided by $\eta_1 = \frac{1 - P_{01}}{P_{10}}$ and $\eta_0 = \frac{P_{01}}{1 - P_{10}}$. Where P_{01} and P_{10} are the tolerated false alarm probability and the tolerated miss detection probability, respectively.

5. Our System Characteristics:

Now, we will describe the operating characteristics of our system.

5.1. PU Characteristics (TV Tower):

In the United States, the antenna Height Above Average Terrain (HAAT) and Average Effective Radiated Power

(AERP) for DTV stations operated by existing licenses is designed to provide equivalent noise-limited coverage to a distance equal to the present NTSC (National Television System Committee) grade B service contour. The maximum permissible power for new DTV stations in the UHF band is 316 kW. The maximum antenna height is 2000 ft above average terrain. For HAATs below this value, higher AERP is permitted to achieve equivalent coverage. The maximum AERP is 1000 kW regardless of HAAT.

We consider the case of Georgia for our study, which is covered by WCTV Television Tower. WCTV is the CBS-affiliated television station for southwest Georgia and Tallahassee, Florida that is licensed to Thomasville, Georgia. Owned by Gray Television, the station has studios on Halstead Boulevard in Tallahassee along I-10. It operates the area's MyNetworkTV affiliate on a second digital sub-channel as well as Comcast digital cable channels 14 and 227.

it 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 is 609.6 meters (2000 ft) high. It’s transmitter power is 1,000 kW. This could provide city-grade coverage of Tallahassee and north central Florida as well as southwestern Georgia (Tallahassee is the capital of the U.S. state of Florida with area of 103.1 sq mi (267.029 km^2)).

5.2. Helper Node Characteristics:

We suggest the dipole antenna for receiving and transmitting signals at helper nodes, which is the simplest TV antenna. Variations on the dipole are the bowtie (which has wider bandwidth), the folded-dipole (which can solve an efficiency problem) and the loop (variation on the folded dipole). Dipole antennas have the same gain and the same radiation field. The gain is generally 2.15 dBi. “dBi” means “dB of improvement over an isotropic radiator”, which is an antenna that radiates equally in all directions. An antenna will have the same gain when receiving as when transmitting, and also the same radiation pattern. Following the FCC rules, we assume that the height of the antenna of helper nodes in our system is 20 meter.

6. PU Authentication System:

In this section, we describe the two steps of the spectrum authentication mechanism, i.e., the authentication of the PU signal at the helper nodes in the first stage and the interaction between CR’s entities for secure broadcasting of spectrum status information.

6.1 PU Signal Authentication at Helper Nodes (First Stage):

Our goal is to provide SUs with the ability to determine whether a received signal is from a PU or not in the presence of attackers. A key component of our approach is a helper nodes placed close to a PU which is a TV tower in our system. Though we cannot modify any PU due to the FCC constraint, we can put necessary mechanisms on each helper node, including the use of cryptographic signatures.

We consider a network of SUs distributed over a large area. In the case of our study, WCTV tower could provide city-grade coverage of Tallahassee (with area of 103.1 sq mi (267.029 km2)). Helper nodes in the first stage measure the power of the received signal using energy detectors due to their simplicity, efficiency, and widespread use [23]. The outcome of sensing by helper node N_i is P_r , which represents an estimate of the received primary power at node N_i. In dB, this is written as $P_r = P_t - PL$ where P_t is the transmitting power and PL is the pass loss.

The average large-scale path loss for an arbitrary transmitter-receiver (T-R) separation *d*, is expressed as a function of the path loss at a reference distance d_0 by using a path loss exponent, *n*. Measurements have shown that at any value of *d*, the path loss PL(*d*) (in dB) at a particular location is random and distributed log-normally about the mean distance-dependent value. That is:

$$PL(d)\ \ dB = \overline{PL}(d_0) + 10n\log(d/d_0) + X_\sigma \qquad (4)$$

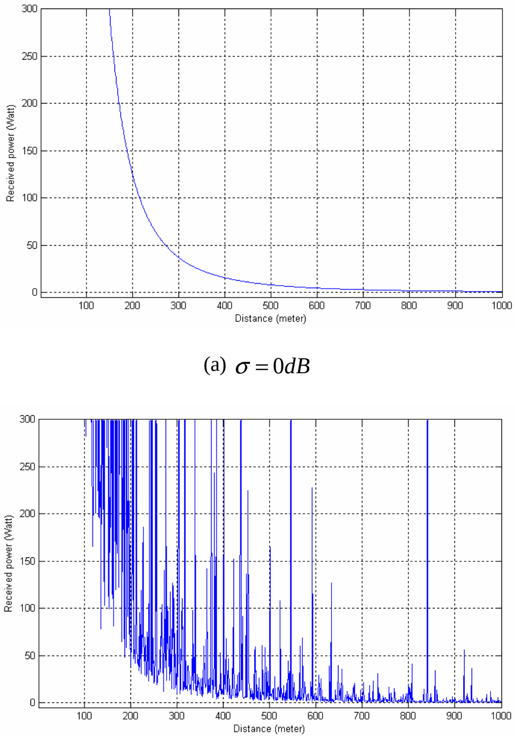
Where X_σ is a zero-mean Gaussian distributed random variable (in dB) with standard deviation σ (also in dB). σ is a parameter that typically range between 2 – 6 dB and the path loss exponent *n* depends on the environments as shown in table.1.

Table. 1 Pass Loss Exponents for Different Environments

Environment	***Pass loss exponent, n***
Free space	2
Urban area cellular radio	2.7 to 3.5
Shadowed Urban cellular radio	3 to 5
In building line of sight	1.6 to 1.8
Obstructed in building	4 to 6
Obstructed in factories	2 to 3

We assume that the received power at close-in-reference distance from transmitter is 0dBm and the close-in-reference distance is d_0 =10m. For urban area cellular radio, we consider the path loss exponent is *n*=3. Thus, according to the log-normal path loss, the relation between the power of the received signal and the distance (between the first level of helper nodes and the PU) is shown in Fig. 1 at different values of standard deviation.

The helper nodes detect the power level of the received signals. If the power level exceeds a certain threshold γ, helper nodes decide that the received signal is that of the primary user. Otherwise, helper nodes decide the presence of attacker.



(a) $\sigma = 0dB$

(b) $\sigma = 4dB$

Fig. 1 The received signal power vs. the distance at (a) $\sigma = 0dB$, and (b) $\sigma = 4dB$.

Now, we need to determine the distance between the PU and the helper nodes at the first stage, and the threshold of the received signal power level, based on the requirements of probability of false alarm (i.e., an idle channel is detected as busy), and probability of missing (i.e., a busy channel is detected as idle).

Algorithm Evaluation:

To evaluate our proposed scheme, we first give the mathematical model of the received signal power, and then show the performance of the proposed authentication scheme in terms of the probability of false alarm and the probability of missing.

According to the log-normal path loss model in Eq. (4), since *PL(d)* is a random variable with a normal distribution in dB about the distance-dependent mean, so is $\overline{P_r}(d)$, and the Q-function or error function (*erf*) may be used to determine the probability that the received signal level exceed (or fall below) a particular level. The Q-function is defined as:

$$Q(z) = \frac{1}{\sqrt{2\pi}} \int_{z}^{\infty} \exp(-\frac{x^2}{2})dx = \frac{1}{2}\left[1 - erf(\frac{z}{\sqrt{2}})\right] \qquad (5)$$

The probability of detection (i.e., the PU's signal is correctly identified) is the probability that the received signal power level exceeds a certain value which can be calculated from the cumulative density function as:

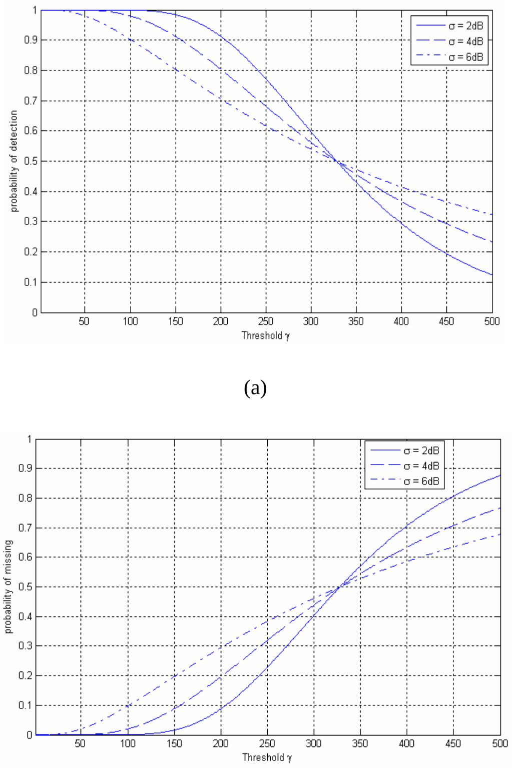
$$\begin{aligned} P_D &= \Pr\left[P_r(d) \geq \gamma\right] = Q\left[\frac{\gamma - \overline{P_r}(d)}{\sigma}\right] \\ &= \frac{1}{2} - \frac{1}{2} erf\left[\frac{\gamma - \overline{P_r}(d)}{\sigma\sqrt{2}}\right] \\ &= \frac{1}{2} - \frac{1}{2} erf\left[\frac{\gamma - \left[P_t - (\overline{PL}(d_0) + 10n\log(d/d_0))\right]}{\sigma\sqrt{2}}\right] \qquad (6) \end{aligned}$$

The probability of missing can be calculated from:

$$\begin{aligned} P_M &= \Pr\left[P_r(d) < \gamma\right] = 1 - P_D \\ &= \frac{1}{2} + \frac{1}{2} erf\left[\frac{\gamma - \left[P_t - (\overline{PL}(d_0) + 10n\log(d/d_0))\right]}{\sigma\sqrt{2}}\right] \qquad (7) \end{aligned}$$

When placing the helper nodes (in the first stage) at distance d = 145m, the relations between the threshold γ and the probability of detection, and the probability of missing are shown in Fig. 2.

The threshold γ can be determined based on the requirement for the probability of missing P_M or the probability of false alarm P_f. For practical applications, the IEEE 802.22 standard suggests both probabilities of false alarm and missing be less than 0.1 in terms of detecting PUs [24]. Herein, we assume a stricter requirement that $P_M \leq 0.02$, and thus from Fig. 2, the threshold γ can be determined to be 100 watt. Hence, the probability of detection is 0.98 and the probability of missing is 0.02 (at $\sigma = 4dB$).



(a)

(b)

Fig. 2 The threshold γ vs. (a) the probability of detection, and (b) the probability of missing.

Assuming that the minimum distance between the helper nodes in the first stage and the attacker is 50m, the relation between the probability of false alarm, the threshold γ, and the transmitting power at the attacker is shown in Fig. 3. At threshold γ = 100 watt, the relation between the probability of false alarm and the transmitting power at the attacker is shown in Fig. 4.

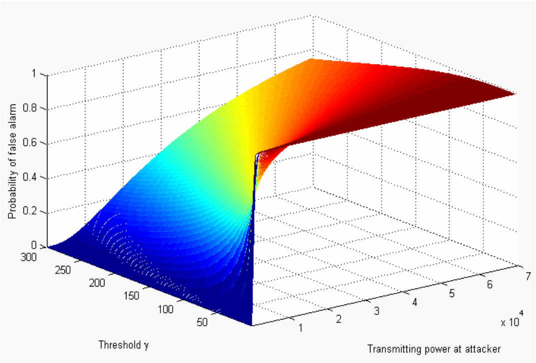


Fig. 3 The probability of false alarm and the threshold γ vs. the transmitting power at the attacker.

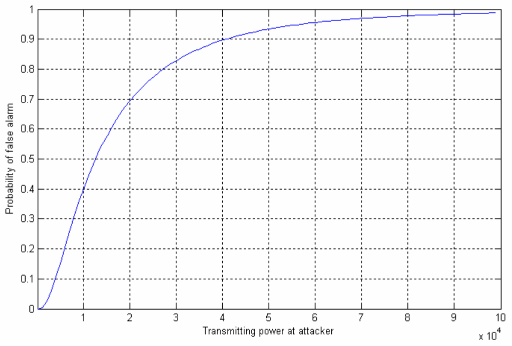


Fig. 4 The probability of false alarm vs. the transmitting power at the attacker at γ =100 watt

Herein, we assume a stricter requirement that $P_f \leq 0.02$, and thus from Fig. 4, when the attacker is placed at the minimum distance d = 50m, the attacker should have the capability to send its signal with a power greater than 1885 watt, which is a very strong assumption where the attacker is assumed to have a maximum transmission output power that is within the range from a few hundred milliwatts to a few watts.

For more generality, Fig. 5 shows the relation between probability of false alarm and the transmitting power at the attacker for different minimum distances between the attacker and the helper nodes in the first stage.

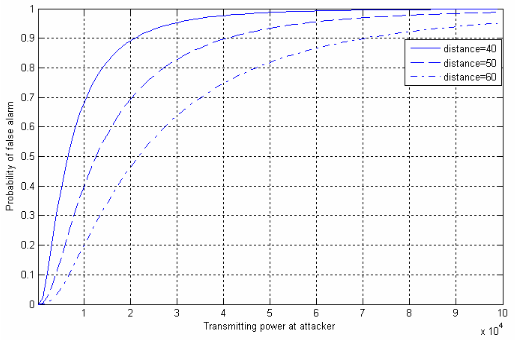


Fig. 5 Probability of false alarm vs. the transmitting power at the attacker for different distances

6.2 Interaction between CR's Entities in Our System:

Our proposed PU authentication scheme is depending on a first stage of helper nodes placed physically close to a PU, but the helper nodes are physically bound to PU which is a TV tower with thousands of watts of transmission power [25]. Hence, helper node is NOT able to deliver spectrum information directly to all SUs in the coverage area of the tower due to the power constraint mandated by the FCC.

To solve this problem, we propose to distribute helper nodes in next stages over the coverage area of the TV tower. Helper nodes in the first stage are responsible for (1) authenticating the PU's signal based on the power level detection, and (2) broadcasting spectrum status information to helper nodes in the next stages and to SUs. Helper nodes in the next stages act as repeaters to serve the SUs inside their coverage area.

Using power level detection, each helper node N_i in the first stage constructs an occupancy vector V_i indicating the set of channels where legitimate PUs are active. V_i is an m-bit vector (m is the number of channels of the system). The j^{th} bit of V_i is set to one if channel j is currently occupied. Otherwise, it is set to zero. The TV spectrum sensing process is repeated at the helpers at the frequency mandated by the FCC (e.g., every 2 seconds [6]).

Secure broadcasting of authentic spectrum information to helper nodes in the next stages: Helper nodes in the first stage are responsible for broadcasting spectrum information to helper nodes in the next stage and to SUs in their coverage area. Each helper node N_i periodically transmits the following information: $m_i \,||\, sig_i(m_i)$ where $m_i : V_i$. Here, $sig_i(m_i)$ denotes the cryptographic signature of helper node N_i on the message m_i.

Secure broadcasting of authentic spectrum information to SUs: Helper nodes in the next stages are responsible for delivering spectrum information to the SUs and to helper nodes in the next stage far from the PU.
First, the helper nodes in the next stage 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 that fails to be authenticated is discarded. If the message is verified, each helper node N_j in the next stage will retransmit the received spectrum information as follows: $m_j \,||\, sig_j(m_j)$ where $m_j : V_i$.

Secondary Users: SU will receive spectrum information form helper nodes where this SU is located in their coverage area. Helper nodes may be those in the first stages or in one of the next stages. The SU will verify the authenticity and integrity of each received message m_j. Message m_j that fails to be authenticated is discarded.

Finally, it is possible for a helper node to falsely detect a PU because of noise or interference in the wireless environment. Additionally, attacker may corrupt helper nodes and enforce them to send false spectrum sensing data. Many proposed schemes indicate that these problems can be addressed by distributing spectrum sensing. In DSS, each helper node acts as a sensing terminal that conducts local spectrum sensing. The local results are reported to a data collector. In our system, when a SU needs to conduct spectrum sensing, it becomes a data collector, collects local sensing reports from the nearby helper nodes, and executes data fusion and determines the final spectrum sensing result.

We suggest the WSPRT data fusion technique, that is more robust against Byzantine failures than the "OR" fusion rule, the "AND" fusion rule, and the "Majority" fusion rule [26, 27]. SPRT may collect multiple reports from corrupted helper nodes, which amplifies the effect of the attack. However, WSPRT makes a favorable tradeoff between data collection overhead and robustness of data fusion. Specifically, WSPRT improves the robustness of data fusion (against Byzantine failures) at the cost of requiring an increased number of local sensing reports.

7. Determining the Number of Next Stages:

Helper nodes in the next stages are responsible for delivering spectrum information to SUs inside their coverage area and to helper nodes in the next stage far from the PU. Hence, the spectrum information have to be delivered to the helper nodes in the last stage before 2 *sec*, as mandated by the FCC, to serve all SUs in the coverage area of the PU. To determine the number of next stages, we need to determine the processing time and the delay at each helper node.

In general, cryptographic algorithms take a significant amount of time if the algorithms are implemented in software. To speed up the processing time, 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 Algorithm (DSA) per second and 620 DSA signature verifications per second [28]. This means that each helper node in the next stages requires 2.4 *msec* for broadcasting the authentic spectrum information; 1.6 *msec* for verification of the received message and 0.8 *msec* for signing the retransmitted spectrum information. However, helper nodes in the first stage require only 0.8 *msec* for signing the occupancy vector.

Additionally, multipath fading in a wireless system is the result of multiple signals from the same RF source arriving at the receive site via many unique paths. Essentially, as an RF signal is radiated from an antenna, it strikes many objects such as walls, buildings, towers, the earth, etc. After striking these objects, the RF signal is time delayed, attenuated, reflected or diffracted and arrives at the receive site at a different amplitude, phase and perhaps time sequence than the directly received signal. At any given instant in time, the total signal received by the antenna is the vector sum of the direct signal and all of all the multipath signals. The measured delay for urban area cellular radio is within 3 μsec.

As a result, each helper node in the next stages requires a total processing time of 2.403 msec. However, all helper nodes in the same stage receive the signed message and perform the signing and the verification process at the same time as we proposed helper nodes to be distributed in circles over the coverage area of the PU. Hence, the total processing time per one stage is 2.403 *msec*. Because the spectrum sensing process remains within the mandated period of 2 seconds, the maximum number of next stages in our system is 831 stages, which ensures that each SU can find a number of helper nodes to provide him with the spectrum information.

8. Conclusion:

In this paper, we proposed a scheme for authenticating PU’s signals in CRNs, which conforms to FCC’s requirement. Our proposed protocol integrates cryptographic signatures and power detection algorithm to enable PU detection in the presence of attackers. Our system relies on the deployment of a network of helper nodes located close to PU for verifying the availability of idle spectrum and for broadcasting the spectrum information to helper nodes in the next stages and to SUs. Distributing helper nodes in next stages ensures the delivery of the spectrum information to each SU in the coverage area of the PU. Our scheme can provide a stricter requirements of probability of false alarm and probability of missing. Compared to prior work, our system can accommodate mobile SUs and can be implemented with relatively low-power helper nodes. Additionally, we can improve the robustness of data fusion against Byzantine failures depending on helper nodes for delivering spectrum sensing reports to the data fusion without any dependence on SUs. Hence, we can preserve the SUs’ location privacy in our proposed scheme.

9. References:

[1] J. Mitola III. Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio. PhD thesis, KTH Royal Institute of Technology, 2000.

[2] Federal Communications Commission. Facilitating opportunities for flexible, efficient, and reliable spectrum use employing spectrum agile radio technologies. ET Docket, (03-108), Dec. 2003.

[3] T. A. Weiss, and F. K. Jondral, "Spectrum pooling: An innovative strategy for the enhancement of spectrum efficiency", IEEE Communications Magazine, 2004.

[4] S. Mishra, A. Sahai, and R. Brodersen, "Cooperative sensing among cognitive radios", in Proceedings of the IEEE International Conference on Communications, June 2006.

[5] S. Shankar, C. Cordeiro, and K. Challapali, "Spectrum agile radios: Utilization and sensing architectures", in Proceedings of the IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, Nov. 2005, pp. 160–169,.

[6] Second Report and Order and Memorandum Opinion and Order In the Matter of Unlicensed Operation in the TV Broadcast Bands, Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3 GHz Band, Federal Communication Commission, Document 08-260, Nov. 14, 2008.

[7] S. Shankar, C. Cordeiro, and K. Challapali, "Spectrum Agile Radios: Utilization and Sensing Architectures", in Proc. IEEE Int. Symposium on New Frontiers in Dynamic Spectrum Access Networks,2006, Baltimore, Maryland, USA, pp.160–169.

[8] D. Cabric, A. Tkachenko, and R. Brodersen, "Spectrum Sensing Measurements of Pilot, Energy and Collaborative Detection", in Proc. IEEE Military Communication Conf., 2006, Washington, D.C., USA, pp 1–7.

[9] J. G. Proakis, Digital Communications, McGraw-Hill, 2001,4th ed.

[10] R. Tandra and A. Sahai, "Fundamental Limits on Detection in Low SNR Under Noise Uncertainty", in Proc. IEEE Int. Conf. Wireless Networks, Communication and Mobile Computing, 2005, vol. 1, Maui, HI, pp 464–469.

[11] W. A. Gardner, "Signal Interception: A Unifying Theoretical Framework for Feature Detection", IEEE Trans. on Communications, , vol. 36, No. 8, 1988.

[12] D. Cabric, S. Mishra, and R. Brodersen, "Implementation Issues in Spectrum Sensing for Cognitive Radios", in Proc. Asilomar Conference on Signals, Systems and Computers,2006,vol.1,PacificGrove,California, USA,, pp 772–776.

[13] K. Kim, I. A. Akbar, K. K. Bae, J.-S. Um, C. M. Spooner, and J. H. Reed, "Cyclostationary Approaches to Signal Detection and Classification in Cognitive Radio", in Proc. IEEE Int. Symposium on New Frontiers in Dynamic Spectrum Access Networks, Dublin, Ireland,2007, pp 212–215.

[14] I. F. Akyildiz, "Next Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A survey", Elsevier Computer Networks, Vol. 50, 2006, pp 2127-2159.

[15] Prabhjot Kaur, and Arun Khosla, "Markovian Queuing Model for Dynamic Spectrum Allocation in Centralized

Architecture for Cognitive Radios", IACSIT, Vol. 3, no. 1, pp 1-4.

[16] Rajagopal Sreenivasan, Sasirekha GVK, and Jyotsna Bapat, "Adaptive Cooperative Spectrum Sensing Using Group Intelligence", IJCNC, Vol.3 ,No.3, 2011, pp 1-7.

[17] S. Parvin, Song Han, Biming Tian, and F.K Hussain, "Trust-Based Authentication for Secure Communication in Cognitive Radio Networks", IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC), 2011, 589 – 596.

[18] Tengyi Zhang, Tsang, and D.H.K., "Optimal Cooperative Sensing Scheduling for Energy-efficient Cognitive Radio Networks", In IEEE proceeding of INFOCOM, 2011, 2723 – 2731.

[19] Weng-Chon Ao, Shin-Ming Cheng, and Kwang-Cheng Chen, "Connectivity of Multiple Cooperative Cognitive Radio Ad Hoc Networks", IEEE Journal on Selected Areas in Communications 30, 2012, pp. 263-270.

[20] Y ali Zhu, Di Suo, and Zehua Gao, "Secure Cooperative Spectrum Trading in Cognitive Radio Networks: A Reversed Stackelberg Approach", International Conference on Multimedia Communications (Mediacom), 2010,202-205.

[21] R. Chen, J.-M. Park, and Kaigui Bian, "Robust distributed spectrum sensing in cognitive radio networks", in Proc. IEEE INFOCOM, 2008.

[22] P. K. Varshney, "Distributed Detection and Data Fusion", Springer-Verlag New York, 1997.

[23] H. Kim, and K. G. Shin, "In-band spectrum sensing in cognitive radio networks: energy detection or feature detection?", In MobiCom ’08, New York, NY, USA, 2008. ACM.

[24] C. Cordeiro, K. Challapali, and M. Ghosh, "Cognitive phy and mac layers for dynamic spectrum access and sharing of tv bands", In TAPAS ’06: Proceedings of the first international workshop on Technology and policy for accessing spectrum, New York, NY, USA, 2006. ACM.

[25] B. Wild, and K. Ramchandran, "Detecting primary receivers for cognitive radio applications", in Proceedings of the IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005, pp. 124–130.

[26] A. Pandharipande, J.-M. Kim, D. Mazzarese, and B. Ji, "IEEE P802.22 Wireless RANs: Technology Proposal Package for IEEE 802.22", Nov. 2005, available at: http://www.ieee802.org/22/.

[27] E. Visotsky, S. Kuffner, and R. Peterson, "On collaborative detection of TV transmissions in support of dynamic spectrum sharing", Proc. IEEE DySPAN, Nov. 2005, pp. 338–345.

[28] SafeXcel-1841 Product Brief, SafeNet Inc., Belcamp, MD, 2005. Available:http://www.safenetinccom/Library/3/SafeXcel-1841_ProductBrief.pdf.

Fatty Mustafa Salem Received her B.Sc. degree in communications and computers engineering from Helwan University, Cairo, Egypt, in 2007. Received her M.S. degree in network security from Helwan University, in 2010. She is currently working toward the 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 received his B.Sc. in communications and computers engineering from Helwan University, Cairo; Egypt. Received his M.S. and PhD in Cryptography and Network security systems from Helwan University in 2001 and 2005 respectively. Currently, working as a lecturer, post doctor researcher and also joining several network security projects in Egypt. His main interest is Cryptography and network security. More specifically, working on the design of efficient and secure cryptographic algorithms, in particular, secure distributed multiparty computations. Other things that interest him are number theory and the investigation of mathematics for designing secure and efficient cryptographic schemes.

Ibrahim Ismail Ibrahim Received his B.Sc. degree in communications and Electronics engineering from Helwan University, Cairo, Egypt, in 1976. Received his M.S. in communications from Cairo University, Cairo, Egypt in 1983 and PhD in communications from Queen University, Belfast, UK in 1987. He is a Professor in Helwan University. His research interests include wireless networks.