Sub-band Detection of Primary User Emulation Attacks in OFDM-based Cognitive Radio Networks

Ahmed Alahmadi, Tianlong Song, Tongtong Li
Department of Electrical & Computer Engineering
Michigan State University, East Lansing, MI 48824, USA
Email: {alahmadi, songtia6}@msu.edu, tongli@egr.msu.edu

***Abstract*—This paper considers the primary user emulation attack (PUEA) problem in OFDM-based cognitive radio networks, and proposes a robust and efficient AES-based digital TV (DTV) scheme. In the proposed scheme, the existing reference sequence used to generate the pilot subcarriers in the DTV frames is encrypted using the Advanced Encryption Standard (AES) algorithm for accurate sub-band detection of the authorized primary user, as well as malicious user. For primary user detection, we investigate the cross-correlation between the received sequence and the AES-encrypted reference sequence over a specific frequency sub-band. The malicious user detection can be performed by investigating the auto-correlation of the received sequence. We analyze the effectiveness of the proposed approach through both theoretical derivation and simulation examples. It is shown that, with the AES-based DTV scheme, both the primary user and malicious user can be detected accurately under primary user emulation attacks.**

***Index Terms*—Cognitive Radio Networks, The Second Generation of Terrestrial Digital Video Broadcasting System (DVB-T2), Orthogonal Frequency Division Multiplexing (OFDM).**

I. Introduction

Cognitive radio (CR) networks have received considerable research attention recently because of their ability to alleviate the spectrum scarcity problem due to the rapid growth in the wireless communication devices. The basic idea of the CR networks is to allow the unlicensed users (secondary users) to share the frequency spectrum with the licensed users (primary users) under the condition that they must not cause harmful interference to the primary users. The spectrum sharing is performed through spectrum sensing, where the CRs sense the spectrum to identify the unused bands (white spaces) for data transmission. If a primary signal is detected in the band that a CR operates in, then the CR must evacuate that band and operate in another white space. A serious security threat to the CR networks is referred to as primary user emulation attack (PUEA), where the malicious users emulate the primary signal over the idle frequency band(s) such that the secondary users cannot use the corresponding white space(s).

Several approaches have been proposed to detect and defend against PUEA [1]–[4]. In [1], a localization-based transmitter verification scheme was proposed to detect PUEA. In [2] and [3], the authors proposed a received signal strength (RSS)-based technique to defend against PUEA, where the attackers can be identified by comparing the received signal power of the primary user and the suspect attacker. A Wald's sequential probability ratio test (WSPRT) was presented to detect PUEA based on the received signal power in [4]. In these existing approaches, the detection of PUEA is mainly based on the power level and/or direction of arrival (DOA) of the received signal. The basic idea is that: given the locations of the primary TV stations, the secondary user can distinguish the actual primary signal from the malicious user's signal by comparing the power level and DOA of the received signal with that of the authorized primary user's signal. The major limitation with such approaches is that: they would fail when a malicious user is at a location where it produces the same DOA and comparable received power level as that of the actual primary transmitter.

As one of the most efficient communication schemes, Orthogonal Frequency Division Multiplexing (OFDM) has found widespread applications in CR networks, of which a very successful one is the Digital Video Broadcasting-Terrestrial (DVB-T) standard applied in digital TV systems. Unlike single-carrier transmission where the signal is processed in the entire spectrum and hence allows full band detection only, the orthogonality between different subcarriers in OFDM provides potential flexibility in performing *sub-band detection* for OFDM-based CR networks.

In this paper, we consider the PUEA problem in the OFDM-based CR networks, and propose a robust AES-based DTV scheme. In the proposed scheme, the existing reference sequence used to generate the pilot subcarriers in the DTV frames is encrypted through an AES chip, which has been commercialized and widely available [5], [6]. To detect a primary user, we investigate the cross-correlation between the received sequence and the AES-encrypted reference sequence for a specific sub-band and time window. The decision can be made by comparing the cross-correlation to a predefined threshold. To guarantee the detection accuracy, the total length of the sequence calculated in the cross-correlation should be reasonably large, which leads to a trade-off between the frequency resolution and time sensitivity. More specifically, as each sub-band carries a fixed number of pilot symbols, if we aim to detect a primary user in a small time window, we have to broaden the sub-band to collect enough symbols for cross-correlation calculation, and thus the frequency resolution would be degraded. Similarly, if we are interested in a smaller sub-band, we would have to wait for a longer time period. The detection of a malicious user can be performed by investigating the auto-correlation of the received sequence based

on the derived information from the primary user detection. It should be emphasized that, in the proposed scheme, the AES-encrypted pilot subcarriers are still used for synchronization purposes at the authorized receivers as the conventional pilot subcarriers.

The rest of the paper is organized as follows. Section II gives an overview of the existing European terrestrial DTV system. Section III presents the proposed AES-based DTV scheme. Section IV discusses the detection performance of the proposed approach. Section V provides some numerical simulations, and Section VI concludes the paper.

II. A Brief Overview of the Existing DTV Systems

Digital Television is an advanced technology for enhancing the quality and performance of the analog television broadcasting. DTV systems have several advantages over the analog systems such as: better picture and sound quality, less transmission power, and higher spectral efficiency, where up to six channels can broadcast simultaneously over the same frequency band that is used by one analog channel [7]. Many countries have switched from analog TV broadcasting to digital TV by adopting one of the four widely used DTV broadcasting standards: Advanced Television System Committee (ATSC), Digital Video Broadcasting-Terrestrial (DVB-T), Terrestrial Integrated Services Digital Broadcasting (ISDB-T), and Digital Terrestrial Multimedia Broadcasting (DTMB).

In this paper, we consider the European standard DVB-T for two main reasons: (i) it has been proved to be a very successful digital terrestrial television standard, and has been adopted by more than half of the countries in the world [8], and (ii) it is based on the OFDM system, which can be exploited for effective detection of the authorized primary user, as well as malicious user, in each individual sub-band of the allocated frequency spectrum.

For better spectral efficiency and system flexibility, the DVB Project released the second generation of the terrestrial digital television standard (known as DVB-T2) to replace the older DVB-T standard in September, 2009. The frame structure of the DVB-T2 standard is shown in Figure 1 [9]. It consists of super frames, which are partitioned into T2-frames and supplementary future extension frames (FEF). The T2-frames are further divided into OFDM symbols. The duration of the super frame T_{SF} is obtained as [9]:

$$T_{SF} = N_{T2} \times T_F + N_{FEF} \times T_{FEF}, \qquad (1)$$

where N_{T2}, N_{FEF} are the numbers of T2-frames and FEFs in a super frame, respectively, and T_F, T_{FEF} are the time duration of each T2-frame and FEF, respectively. The maximum value for T_F is $250ms$, while the maximum values for T_{SF} are $1275s$ and $63.75s$ depending whether FEFs are used or not, respectively.

As shown in Figure 1, each T2-frame consists of three kinds of OFDM symbols: P1 preamble symbol used for characterizing the basic transmission parameters, P2 preamble symbol(s) used for carrying signaling information, and data symbols for payload [9]. Furthermore, each symbol has different pilot subcarriers (scattered pilots, continual pilots, edge pilots, P2 pilots), which are used for frame synchronization, frequency synchronization, and channel estimation [9]. In this paper, we propose to use the P2 pilots for primary user and malicious user sub-band detection for two reasons. First, they are the only pilots whose frequency locations are independent of the FFT size (1K, 2K, 4K, 8K, 16K, 32K) and the operational modes (SISO, MIMO) except in 32K SISO mode. Second, they have the largest number among all the pilot subcarriers. This enables us to achieve effective sub-band detection of the authorized primary user and malicious user.

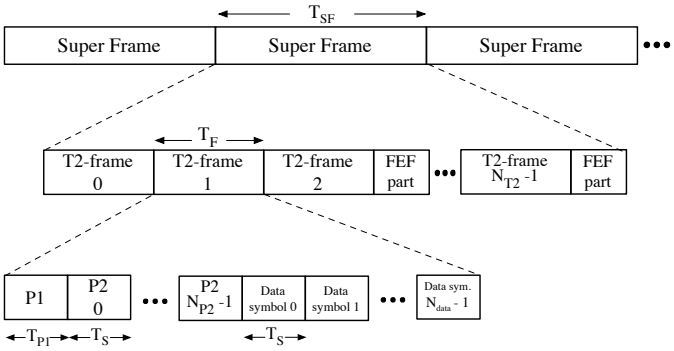

Fig. 1. The DVB-T2 frame structure.

III. The Proposed AES-based DTV Scheme

In this section, we present the proposed AES-based DTV approach for reliable and effective CR network operation. We first discuss the transmitter design, where the existing reference sequence used to generate the P2 subcarriers is encrypted using the AES algorithm. Then, we investigate the receiver design for accurate sub-band detection of the primary user and malicious user.

A. Transmitter Design

The locations of P2 pilots in the frequency domain are determined by:

$$k \equiv 0 \pmod 3, \qquad \mathrm{K_{min}} \le k < \mathrm{K_{max}}, \qquad (2)$$

where $\mathrm{K_{min}}$ and $\mathrm{K_{max}}$ are the minimum and maximum frequency indexes in the P2 symbol. The P2 pilots are generated based on the reference sequence $\mathbf{r}_s$, which is obtained by

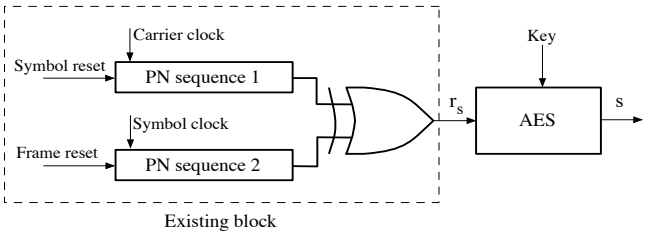

Fig. 2. Generation of the proposed reference signal **s**.

performing the XOR (exclusive-OR) function to two pseudo-random sequences, as shown in Figure 2 [9]. More details on the PN sequences generation can be found in [9].

In this paper, we propose that the existing reference sequence $\mathbf{r}_s$ is encrypted using the AES algorithm with a secret key to obtain the proposed reference signal $\mathbf{s}$, as illustrated in Figure 2, and as follows:

$$\mathbf{s} = E\left(k, \mathbf{r}_s\right), \tag{3}$$

where k is the key, and $E(\cdot,\cdot)$ denotes the AES encryption operation.

It should be noted that the encrypted pilot subcarriers are still used as the conventional subcarriers for synchronization purposes. Moreover, the secret key can be generated and distributed to the DTV transmitter and receiver from a trusted third party in addition to the DTV and the CR user. The third party serves as the authentication center for both the primary user and the CR user, and can carry out key distribution.

B. Receiver Design

The received signal, under PUEA, can be modeled as:

$$\mathbf{r} = \alpha\mathbf{s} + \beta\mathbf{m} + \mathbf{n}, \tag{4}$$

where $\mathbf{s}$ is the reference signal, $\mathbf{m}$ is the malicious signal, $\mathbf{n}$ is the noise, α and β are binary indicators for the presence of the primary user and malicious user, respectively. More specifically, $\alpha = 0$ or 1 means the primary user is absent or present, respectively; and $\beta = 0$ or 1 means the malicious user is absent or present, respectively.

1) Primary user detection: To detect the presence of the primary user, the receiver evaluates the cross-correlation between the received signal $\mathbf{r}$ and the *regenerated* reference signal $\mathbf{s}$, i.e.,

$$\mathbf{R}_{rs} =< \mathbf{r}, \mathbf{s} >= \alpha\sigma_s^2, \tag{5}$$

where σ_s^2 is the primary user's signal power, and $\mathbf{s}$, $\mathbf{m}$, $\mathbf{n}$ are assumed to be independent with each other and are of zero mean. Depending on the value of α, the receiver decides whether the primary user is present or absent.

Assuming that the signals are ergodic, then the ensemble average can be approximated by the time average. Here, we use the time average to estimate the cross-correlation, i.e.,

$$\hat{\mathbf{R}}_{rs} \triangleq \frac{1}{M}\sum_{i=1}^{M} \mathbf{r}_i \cdot \mathbf{s}_i^*, \tag{6}$$

where M is the sample size, $\mathbf{s}_i$ and $\mathbf{r}_i$ denote the ith symbol of the reference and received signal, respectively.

To detect the presence of the primary user, the receiver compares the cross-correlation between the reference signal and the received signal to a predefined threshold T. We have two cases: (i) if $\hat{\mathbf{R}}_{rs} \geq T$, then we determine that the primary user is present, and (ii) if $\hat{\mathbf{R}}_{rs} < T$, then we determine that the primary user is absent. The detection problem can be modeled as a binary hypothesis test problem as follows:

H_0: the primary user is absent $(\alpha = 0)$
H_1: the primary user is present $(\alpha = 1)$

As can be seen from (5), the cross-correlation between the reference signal and the received signal is equal to 0 or σ_s^2, in case when the primary user is absent or present, respectively. Following the *minimum distance rule*, we choose $T = \sigma_s^2/2$ as the threshold for primary user detection.

2) Malicious user detection: For malicious user detection, the receiver further evaluates the auto-correlation of the received signal $\mathbf{r}$, i.e.,

$$\mathbf{R}_{rr} =< \mathbf{r}, \mathbf{r} >= \alpha^2\sigma_s^2 + \beta^2\sigma_m^2 + \sigma_n^2, \tag{7}$$

where σ_m^2 and σ_n^2 denote the malicious user's signal power and the noise power, respectively. Based on the value of α, β can be determined accordingly through (7). We have the following cases:

$$\mathbf{R}_{rr} = \begin{cases} \sigma_s^2 + \sigma_m^2 + \sigma_n^2, & \alpha = 1,\ \beta = 1 \\ \sigma_s^2 + \sigma_n^2, & \alpha = 1,\ \beta = 0 \\ \sigma_m^2 + \sigma_n^2, & \alpha = 0,\ \beta = 1 \\ \sigma_n^2, & \alpha = 0,\ \beta = 0 \end{cases} \tag{8}$$

Assuming ergodic signals, we can use the time average to estimate the auto-correlation as follows:

$$\hat{\mathbf{R}}_{rr} \triangleq \frac{1}{M}\sum_{i=1}^{M} \mathbf{r}_i \cdot \mathbf{r}_i^*. \tag{9}$$

Threshold based detection method can be developed accordingly. Here, we can model the detection problem using four hypotheses, denoted by $H_{\alpha\beta}$, where $\alpha, \beta \in \{0, 1\}$:
H_{00}: the malicious user is absent given that $\alpha = 0$ ($\hat{\mathbf{R}}_{rr} < T_0$)
H_{01}: the malicious user is present given that $\alpha = 0$ ($\hat{\mathbf{R}}_{rr} \geq T_0$)
H_{10}: the malicious user is absent given that $\alpha = 1$ ($\hat{\mathbf{R}}_{rr} < T_1$)
H_{11}: the malicious user is present given that $\alpha = 1$ ($\hat{\mathbf{R}}_{rr} \geq T_1$)

IV. Performance Analysis

In this section, we evaluate the detection performance of the proposed AES-based DTV scheme for both the primary user and malicious user through false alarm rate and miss detection probability. We further discuss the effect of the sample size M upon the detection measures.

A. False Alarm Rate and Miss Detection Probability

Denote the false alarm rate for primary user detection by P_f, and the miss detection probability by P_m. The false alarm rate is defined as the conditional probability that the primary user is considered to be present, when it is actually absent, i.e.,

$$P_f = Pr(H_1|H_0), \tag{10}$$

whereas the miss detection probability is defined as the conditional probability that the primary is considered to be absent, when it is present, i.e.,

$$P_m = Pr(H_0|H_1). \tag{11}$$

Note that the cross-correlation $\hat{\mathbf{R}}_{rs}$, defined in (6), is the sample mean of independent random variables of size M.

According to the central limit theorem (CLT), as long as M is sufficiently large (i.e., $M \geq 30$), this sample mean approximately follows the Gaussian distribution [10]. More specifically, under H_0, $\hat{\mathbf{R}}_{rs} \sim \mathcal{N}(\mu_0, \sigma_0^2)$ with mean $\mu_0 = 0$ and variance $\sigma_0^2 = \frac{1}{M}\left[\beta^2\sigma_s^2\sigma_m^2 + \sigma_s^2\sigma_n^2)\right]$. Similarly, under H_1, $\hat{\mathbf{R}}_{rs} \sim \mathcal{N}(\mu_1, \sigma_1^2)$ with mean $\mu_1 = \sigma_s^2$ and variance $\sigma_1^2 = \frac{1}{M}\left[\mathbb{E}\{|\tilde{\mathbf{s}}|^4\}+\beta^2\sigma_s^2\sigma_m^2+\sigma_s^2\sigma_n^2-(\sigma_s^2)^2\right]$, where we assume that $\mathbb{E}\{|\mathbf{s}_i|^4\} = \mathbb{E}\{|\tilde{\mathbf{s}}|^4\}\ \forall i$. The false alarm rate P_f can be obtained as:

$$P_f = P_r\{\hat{\mathbf{R}}_{rs} \geq T|H_0\} = Q(\tfrac{T-\mu_0}{\sigma_0}), \quad (12)$$

and the miss detection probability P_m can be obtained as:

$$P_m = P_r\{\hat{\mathbf{R}}_{rs} < T|H_1\} = 1 - Q(\tfrac{T-\mu_1}{\sigma_1}). \quad (13)$$

Similarly, for malicious user detection, denote the false alarm rate by $\tilde{P}_f$ and the miss detection probability by $\tilde{P}_m$, which can be obtained as:

$$\tilde{P}_f = P_0 Q(\tfrac{T_0-\mu_{00}}{\sigma_{00}}) + (1-P_0)Q(\tfrac{T_1-\mu_{10}}{\sigma_{10}}), \quad (14)$$

$$\tilde{P}_m = 1 - P_0 Q(\tfrac{T_0-\mu_{01}}{\sigma_{01}}) + (P_0-1)Q(\tfrac{T_1-\mu_{11}}{\sigma_{11}}), \quad (15)$$

where $P_0 = P_r(\alpha = 0)$, and μ_{00}, σ_{00}, μ_{01}, σ_{01}, μ_{10}, σ_{10}, μ_{11}, σ_{11}, and the optimal values for T_0 and T_1 can be calculated similarly as in [11].

B. Detection Performance Versus Sample Size

Substituting by $\sigma_s^2/2$ for T in (12) and (13), we have:

$$P_f = Q(C_1\sqrt{M}) \quad and \quad P_m = 1 - Q(-C_2\sqrt{M}), \quad (16)$$

where $C_1 = \sigma_s^2/(2\ .\ \sqrt{\beta^2\sigma_s^2\sigma_m^2 + \sigma_s^2\sigma_n^2}\ )$ and $C_2 = \sigma_s^2/(2\ .\ \sqrt{\mathbb{E}\{|\tilde{\mathbf{s}}|^4\} + \beta^2\sigma_s^2\sigma_m^2 + \sigma_s^2\sigma_n^2 - (\sigma_s^2)^2}\ )$.

Following (16), we have the following result:

***Proposition** 1: Assuming **s**, **m**, **n** are independent with each other and are of zero mean. For a fixed SNR level, both the false alarm rate P_f and the miss detection P_m decrease as the sample size increases. More specifically,* $\lim_{M\to\infty} P_m = 0$ *and* $\lim_{M\to\infty} P_f = 0$.

Discussions: It should be noted that there is always a trade-off between the frequency resolution and time sensitivity. In our case, this implies that to obtain a sufficiently large sample size M, we can either use a wider sub-band to improve the time sensitivity, or use a larger observation time window to increase the sub-band detection accuracy in the frequency domain.

V. Simulation Results

In this section, we demonstrate the detection performance of the proposed AES-based DTV scheme through the evaluation of the false alarm rate and miss detection probability for primary user and malicious user detection. In the following, we assume that **s**, **m**, and **n** are independent and are of zero mean. Furthermore, the primary user's signal power is assumed to be normalized to $\sigma_s^2 = 1$, which follows that $T = \sigma_s^2/2 = 0.5$.

Using the sample size $M = 100$, we obtain the false alarm rates and miss detection probabilities numerically and compare them with the theoretical results. Figure 3 shows the false alarm rate for primary user detection versus SNR. For malicious user detection, we set $\tilde{P}_f \leq 10^{-3}$ that minimizes $\tilde{P}_m$. The miss detection probabilities are depicted in Figure 4. It can be seen that the proposed AES-based DTV scheme can achieve very low false alarm rates and miss detection probabilities even under very low SNR values when detecting the primary user and malicious user.

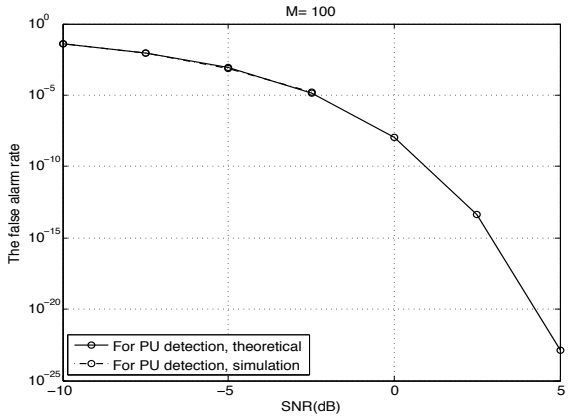

Fig. 3. The false alarm rate P_f versus SNR for primary user detection.

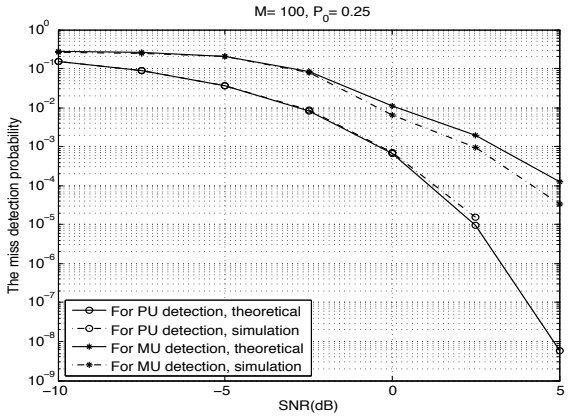

Fig. 4. The miss detection probabilities versus SNR. For malicious user detection, $\tilde{P}_m$ is minimized under the constraint that $\tilde{P}_f \leq 10^{-3}$.

VI. Conclusions

In this paper, we studied the PUEA problem in the OFDM-based CR networks, and proposed a reliable and efficient AES-based DTV scheme. In the proposed approach, the existing reference sequence in the DTV system is encrypted using the AES algorithm for accurate sub-band detection of the authorized primary user, as well as malicious user, in the allocated frequency spectrum. It was shown that, with the AES-based DTV scheme, both the primary user and the malicious user can be detected accurately under primary user emulation attacks. The proposed approach is practically feasible in the sense that it can effectively detect primary user and malicious user with no change in hardware or system structure except of a plug-in AES chip.

REFERENCES

[1] R. Chen, J.-M. Park, and J. 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, Jan. 2008.

[2] Z. Yuan, D. Niyato, H. Li, and Z. Han, "Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks," in *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, 2011, pp. 599–604.

[3] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han, "Defeating primary user emulation attacks using belief propagation in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 10, pp. 1850–1860, 2012.

[4] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *IEEE International Conference on Communications*, June 2009, pp. 1–5.

[5] AT32UC3A3256S. [Online]. Available: http://www.atmel.com/devices/at32uc3a3256s.aspx

[6] A. Hodjat, D. D. Hwang, B. Lai, K. Tiri, and I. Verbauwhede, "A 3.84 Gbits/s AES crypto coprocessor with modes of operation in a 0.18-μm CMOS technology," in *Proceedings of the 15th ACM Great Lakes symposium on VLSI*. New York, NY, USA: ACM, 2005, pp. 60–63.

[7] J. Adda and M. Ottaviani, "Digital television 1: The transition to digital television *," September 2004.

[8] A. Fernando, *3DTV : processing and transmission of 3D video signals*. Chichester, West Sussex, United Kingdom: Wiley, 2013.

[9] Digital Video Broadcasting, "Frame structure channel coding and modulation for a second generation digital terrestrial television broadcasting system (DVB-T2)," *ETSI Std. EN 302 755 V1.3.1*, April 2012.

[10] P. S. Mann, *Introductory Statistics*, 7th ed. Wiley, February 2010.

[11] A. Alahmadi, M. Abdelhakim, J. Ren, and T. Li, "Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 772–781, May 2014.