Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard

Ahmed Alahmadi, Mai Abdelhakim, Jian Ren, and Tongtong Li

***Abstract*— This paper considers primary user emulation attacks in cognitive radio networks operating in the white spaces of the digital TV (DTV) band. We propose a reliable AES-assisted DTV scheme, in which an AES-encrypted reference signal is generated at the TV transmitter and used as the sync bits of the DTV data frames. By allowing a shared secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver and used to achieve accurate identification of the authorized primary users. In addition, when combined with the analysis on the autocorrelation of the received signal, the presence of the malicious user can be detected accurately whether or not the primary user is present. We analyze the effectiveness of the proposed approach through both theoretical analysis and simulation examples. It is shown that with the AES-assisted DTV scheme, the primary user, as well as malicious user, can be detected with high accuracy under primary user emulation attacks. It should be emphasized that the proposed scheme requires no changes in hardware or system structure except for a plug-in AES chip. Potentially, it can be applied directly to today's DTV system under primary user emulation attacks for more efficient spectrum sharing.**

***Index Terms*— Network security, primary user emulation attacks (PUEA), secure spectrum sensing, dynamic spectrum access (DSA), eight-level vestigial sideband (8-VSB).**

I. Introduction

ALONG with the ever-increasing demand in high-speed wireless communications, spectrum scarcity has become a serious challenge to the emerging wireless technologies. In licensed networks, the primary users operate in their allocated licensed bands. It is observed that the licensed bands are generally underutilized and their occupation fluctuates temporally and geographically in the range of 15–85% [1]. Cognitive radio (CR) networks [2], [3] provide a promising solution to the spectrum scarcity and underutilization problems [4].

CR networks are based on dynamic spectrum access (DSA), where the unlicensed users (also known as the secondary users) are allowed to share the spectrum with the primary users under the condition that the secondary users do not interfere with the primary system's traffic [5]. Unused bands (white spaces) are identified through *spectrum sensing* [3], then utilized by the CRs for data transmissions. The spectrum sensing function is continuously performed. 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 [6].

The CR system is vulnerable to malicious attacks that could disrupt its operation. A well-known malicious attack is the primary user emulation attack (PUEA) [7]. In PUEA, malicious users mimic the primary signal over the idle frequency band(s) such that the authorized secondary users cannot use the corresponding white space(s). This leads to low spectrum utilization and inefficient cognitive network operation.

PUEA have attracted considerable research attention in literature [8]–[18]. In [8], an analytical model for the probability of successful PUEA based on the energy detection was proposed, where the received signal power is modeled as a log-normally distributed random variable. In this approach, a lower bound on the probability of a successful PUEA is obtained using Markov inequality. Several other methods have been proposed to detect and defend against PUEA. In [9], a transmitter verification scheme (localization-based defense) was proposed to detect PUEA. In [10] and [11], the authors proposed a received signal strength (RSS)-based defense 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 [12]. A similar strategy was used to detect PUEA in fading wireless environments in [13]. In [14], a cooperative secondary user model was proposed for primary user detection in the presence of PUEA. In this approach, the decision whether the primary user is present or absent is based on the energy detection method.

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.

Manuscript received October 9, 2013; revised January 19, 2014; accepted February 28, 2014. Date of publication March 11, 2014; date of current version April 2, 2014. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. T. Charles Clancy.

The authors are with the Department of Electrical and Computer Engineering, Michigan State University, East Lansing, MI 48824 USA (e-mail: alahmadi@egr.msu.edu; abdelhak@egr.msu.edu; renjian@egr.msu.edu; tongli@egr.msu.edu).

Digital Object Identifier 10.1109/TIFS.2014.2310355

1556-6013 © 2014 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Recently, PUEA detection based on cryptographic techniques have also been proposed, see [15]–[17], for example. In [15], a public key cryptography mechanism is used between primary users and secondary users, such that the secondary users can identify the primary users accurately based on their public keys. A possible concern with this scheme is that public key based approaches generally have high computational complexity. In [16], a two-stage primary user authentication method was proposed: (i) first, generate the authentication tag for the primary user using a one-way hash chain; (ii) embed the tag in the primary user's signal through constellation shift. This tag embedding scheme resembles that of digital watermarking. It introduces some distortions to the primary user signals, and is sensitive to noise.

In this paper, we propose a reliable AES-assisted DTV scheme, where an AES-encrypted reference signal is generated at the TV transmitter and used as the sync bits of the DTV data frames. By allowing a shared secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver and used to achieve accurate identification of authorized primary users. Moreover, when combined with the analysis on the auto-correlation of the received signal, the presence of the malicious user can be detected accurately no matter the primary user is present or not. The proposed approach can effectively combat PUEA with no change in hardware or system structure except of a plug-in AES chip, which has been commercialized and widely available [**?**], [19], [20]. It should be noted that the AES-encrypted reference signal is also used for synchronization purposes at the authorized receivers, in the same way as the conventional synchronization sequence.

The proposed scheme combats primary user emulation attacks, and enables more robust system operation and efficient spectrum sharing. The effectiveness of the proposed approach is demonstrated through both theoretical analysis and simulation examples. It is shown that with the AES-assisted DTV scheme, the primary user, as well as malicious user, can be detected with high accuracy and low false alarm rate under primary user emulation attacks.

The rest of the paper is organized as follows. In Section II, we provide a brief overview of the current terrestrial DTV system. Section III presents the proposed AES-assisted DTV approach. Analytical system evaluation is provided in Sections IV and V. Security and feasibility of the proposed scheme is discussed in Section VI. Numerical simulations are presented in Section VII. Finally, the paper is concluded in Section VIII.

II. A Brief Review of the Terrestrial Digital TV system

In this section, we provide a brief overview of the existing DTV system in the US.

In the DTV system, eight-level vestigial sideband (8-VSB) modulation is used for transmitting digital signals after they are partitioned into frames [21]. The frame structure of the 8-VSB signal is illustrated in Fig. 1. Each frame has two data fields, and each data field has 313 data segments. The first data segment of each data field is used for frame synchronization

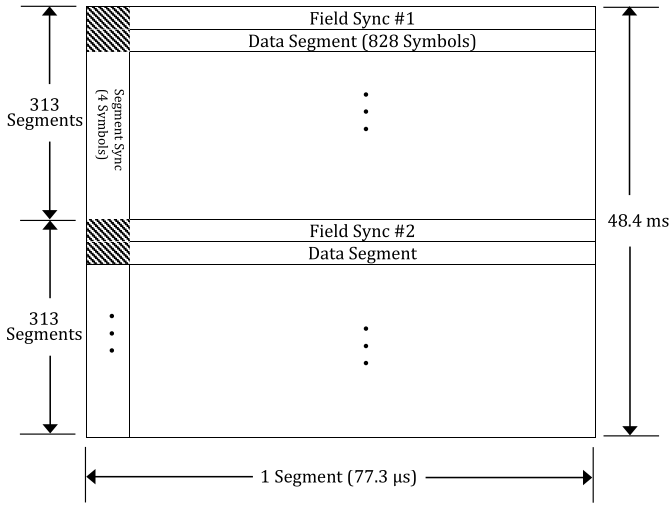


Fig. 1. 8-VSB signal frame structure.

and channel estimation at the receiver [21], [22]. The remaining 624 segments are used for data transmission. Each data segment contains 832 symbols, including 4 symbols used for segment synchronization. The segment synchronization bits are identical for all data segments. Each segment lasts 77.3 μs, hence the overall time duration for one frame, which has 626 segments, is $626 * 77.3\ \mu s = 48.4\ ms$ [21].

III. The Proposed AES-Assisted DTV Approach

In this section, we present the proposed AES-assisted DTV system for robust and reliable primary and secondary system operations. In the proposed system, the primary user generates a pseudo-random AES-encrypted reference signal that is used as the segment sync bits. The sync bits in the field sync segments remain unchanged for the channel estimation purposes. At the receiving end, the reference signal is regenerated for the detection of the primary user and malicious user. It should be emphasized that synchronization is still guaranteed in the proposed scheme since the reference bits are also used for synchronization purposes.

A. AES-Assisted DTV Transmitter

The DTV transmitter obtains the reference signal through two steps: first, generating a pseudo-random (PN) sequence, then encrypting the sequence with the AES algorithm. More specifically, a pseudo-random (PN) sequence is first generated using a *Linear Feedback Shift Register* (LFSR) with a secure initialization vector (IV). Maximum-length LFSR sequences can be achieved by tapping the LFSRs according to primitive polynomials. The maximum sequence length that can be achieved with a primitive polynomial of degree m is $2^m - 1$. Without loss of generality, a maximum-length sequence is assumed throughout this paper.

Once the maximum-length sequence is generated, it is used as an input to the AES encryption algorithm, as illustrated in Fig. 2. We propose that a 256-bit secret key be used for the AES encryption so that the maximum possible security is achieved. Security analysis will be provided in Section VI.

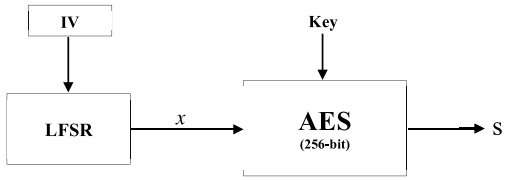


Fig. 2. Generation of the reference signal.

Denote the PN sequence by x, then the output of the AES algorithm is used as the reference signal, which can be expressed as:

$$\mathbf{s} = E\left(k, x\right), \tag{1}$$

here k is the key, and $E(\cdot,\cdot)$ denotes the AES encryption operation. The transmitter then places the reference signal $\mathbf{s}$ in the sync bits of the DTV data segments.

The secret key can be generated and distributed to the DTV transmitter and receiver from a trusted 3rd party in addition to the DTV and the CR user. The 3rd party serves as the authentication center for both the primary user and the CR user, and can carry out key distribution. To prevent impersonation attack, the key should be time varying [23].

B. AES-Assisted DTV Receiver

The receiver regenerates the encrypted reference signal, with the secret key and IV that are shared between the transmitter and the receiver. A correlation detector is employed, where for primary user detection, the receiver evaluates the cross-correlation between the received signal $\mathbf{r}$ and the regenerated reference signal $\mathbf{s}$; for malicious user detection, the receiver further evaluates the auto-correlation of the received signal $\mathbf{r}$. The cross-correlation of two random variables $\mathbf{x}$ and $\mathbf{y}$ is defined as:

$$\mathbf{R_{xy}} = < \mathbf{x}, \mathbf{y} > = \mathbf{E}\{\mathbf{x}\mathbf{y}^*\} \tag{2}$$

Under PUEA, the received signal can be modeled as:

$$\mathbf{r} = \alpha\mathbf{s} + \beta\mathbf{m} + \mathbf{n}, \tag{3}$$

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

$$\begin{aligned}\mathbf{R}_{rs} &= < \mathbf{r}, \mathbf{s} > = \alpha < \mathbf{s}, \mathbf{s} > + \beta < \mathbf{m}, \mathbf{s} > + < \mathbf{n}, \mathbf{s} > \\ &= \alpha\sigma_s^2,\end{aligned} \tag{4}$$

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 in (4), 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. The estimated cross-correlation $\hat{\mathbf{R}}_{rs}$ is given by:

$$\hat{\mathbf{R}}_{rs} \triangleq \sum_{i=1}^{N} \frac{\mathbf{r}_i \cdot \mathbf{s}_i^*}{N}, \tag{5}$$

where N is the reference signal's length, $\mathbf{s}_i$ 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 λ. We have two cases:

- If the cross-correlation is greater than or equal to λ, that is:
$$\hat{\mathbf{R}}_{rs} \geq \lambda, \tag{6}$$
then the receiver concludes that the primary user is present, i.e., $\alpha = 1$.
- If the cross-correlation is less than λ, that is:
$$\hat{\mathbf{R}}_{rs} < \lambda, \tag{7}$$
then the receiver concludes that the primary user is absent, i.e., $\alpha = 0$.

This detection problem can be modeled as a binary hypothesis test problem with the following two hypotheses:

H_0: the primary user is absent ($\hat{\mathbf{R}}_{rs} < \lambda$)

H_1: the primary user is present ($\hat{\mathbf{R}}_{rs} \geq \lambda$)

As can be seen from (4), 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 $\lambda = \sigma_s^2/2$ as the threshold for primary user detection.

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

$$\begin{aligned}\mathbf{R}_{rr} &= < \mathbf{r}, \mathbf{r} > = \alpha^2 < \mathbf{s}, \mathbf{s} > + \beta^2 < \mathbf{m}, \mathbf{m} > + < \mathbf{n}, \mathbf{n} > \\ &= \alpha^2\sigma_s^2 + \beta^2\sigma_m^2 + \sigma_n^2,\end{aligned} \tag{8}$$

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 (8). We have the following cases:

$$\mathbf{R}_{rr} = \begin{cases} \sigma_s^2 + \sigma_m^2 + \sigma_n^2, & \alpha = 1,\ \beta = 1 \\ \sigma_s^2 + \sigma_n^2, & \alpha = 1,\ \beta = 0 \\ \sigma_m^2 + \sigma_n^2, & \alpha = 0,\ \beta = 1 \\ \sigma_n^2, & \alpha = 0,\ \beta = 0 \end{cases} \tag{9}$$

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

$$\hat{\mathbf{R}}_{rr} \triangleq \sum_{i=1}^{N} \frac{\mathbf{r}_i \cdot \mathbf{r}_i^*}{N}. \tag{10}$$

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 $\alpha = 0$

H_{01} : the malicious user is present given that $\alpha = 0$

H_{10} : the malicious user is absent given that $\alpha = 1$

H_{11} : the malicious user is present given that $\alpha = 1$

In practical scenarios, however, we only have an estimated value of α, denoted as $\hat{\alpha}$. We estimate β after we obtain $\hat{\alpha}$. To do this, the receiver compares the auto-correlation of the received signal to two predefined thresholds λ_0 and λ_1 based on the previously detected $\hat{\alpha}$. More specifically, the receiver compares the auto-correlation of the received signal to λ_0 when $\hat{\alpha} = 0$, and to λ_1 when $\hat{\alpha} = 1$. That is:

$$\begin{cases} \hat{H}_{00} : \hat{\mathbf{R}}_{rr} < \lambda_0, & \text{given that } \hat{\alpha} = 0, \ (\hat{\beta} = 0) \\ \hat{H}_{01} : \hat{\mathbf{R}}_{rr} \geq \lambda_0, & \text{given that } \hat{\alpha} = 0, \ (\hat{\beta} = 1) \\ \hat{H}_{10} : \hat{\mathbf{R}}_{rr} < \lambda_1, & \text{given that } \hat{\alpha} = 1, \ (\hat{\beta} = 0) \\ \hat{H}_{11} : \hat{\mathbf{R}}_{rr} \geq \lambda_1, & \text{given that } \hat{\alpha} = 1, \ (\hat{\beta} = 1) \end{cases} \tag{11}$$

The performance of the detection process for the primary user and malicious user is evaluated through the *false alarm rates* and the *miss detection probabilities*, as will be discussed in Sections IV and V.

Discussions: We would like to point that due to the characteristic of the DTV signal in the US, which is a 8-VSB signal of 6 MHz [21], the PUEA detection approaches based on cryptographic techniques (including the approach proposed here as well as those in [15] and [16]) can detect the existence of primary user and malicious user accurately, and can successfully overcome the shortcoming of power level and DOA based detection techniques. However, the detection of white spaces still relies on spectrum sensing. To detect the existence of primary user and malicious user in each sub-band, then the DTV signal needs to be a multi-carrier signal which transmitted through multiple sub-bands as well, as in the European DTV standard [24].

IV. Analytical Evaluation for Primary User Detection

In this section, we analyze the system performance for primary user detection, under H_0 and H_1, through the evaluation of the false alarm rate and the miss detection probability.

We assume that the detection of the primary user has a false alarm rate P_f and a miss detection probability P_m, respectively. The false alarm rate P_f is the conditional probability that the primary user is considered to be present, when it is actually absent, i.e.,

$$P_f = Pr(H_1|H_0). \tag{12}$$

The miss detection probability P_m is the conditional probability that the primary is considered to be absent, when it is present, i.e.,

$$P_m = Pr(H_0|H_1). \tag{13}$$

As can be seen from (5), $\hat{\mathbf{R}}_{rs}$ is the averaged summation of N random variables. Since N is large, then based on the central limit theorem, $\hat{\mathbf{R}}_{rs}$ can be modeled as a Gaussian random variable. More specifically, under H_0, $\hat{\mathbf{R}}_{rs} \sim \mathcal{N}(\mu_0, \sigma_0^2)$, and under H_1, $\hat{\mathbf{R}}_{rs} \sim \mathcal{N}(\mu_1, \sigma_1^2)$, where μ_0, σ_0, and μ_1, σ_1 can be derived as follows.

Under H_0, the received signal is represented as $\mathbf{r}_i = \beta\mathbf{m}_i + \mathbf{n}_i$, where $\mathbf{m}_i$ is the ith malicious symbol, and $\mathbf{n}_i \sim \mathcal{N}(0, \sigma_n^2)$. Then, the mean μ_0 can be obtained as:

$$\begin{aligned} \mu_0 &= \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N}(\beta\mathbf{m}_i + \mathbf{n}_i)\mathbf{s}_i^*\right\} \\ &= 0. \end{aligned} \tag{14}$$

The variance σ_0^2 can be obtained as:

$$\begin{aligned} \sigma_0^2 &= \mathbb{E}\left\{|\hat{\mathbf{R}}_{rs}|^2\right\} - |\mu_0|^2 \\ &= \frac{1}{N}\Big[\beta^2\sigma_s^2\sigma_m^2 + \sigma_s^2\sigma_n^2)\Big]. \end{aligned} \tag{15}$$

Similarly, under H_1, the received signal is represented as $\mathbf{r}_i = \mathbf{s}_i + \beta\mathbf{m}_i + \mathbf{n}_i$, and the mean μ_1 can be obtained as follows:

$$\begin{aligned} \mu_1 &= \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N}(\mathbf{s}_i + \beta\mathbf{m}_i + \mathbf{n}_i)\mathbf{s}_i^*\right\} \\ &= \sigma_s^2, \end{aligned} \tag{16}$$

and σ_1^2 can be obtained as:

$$\begin{aligned} \sigma_1^2 &= \mathbb{E}\left\{|\hat{\mathbf{R}}_{rs}|^2\right\} - |\mu_1|^2 \\ &= \frac{1}{N}\Big[\mathbb{E}\{|\tilde{\mathbf{s}}|^4\} + \beta^2\sigma_s^2\sigma_m^2 + \sigma_s^2\sigma_n^2 - (\sigma_s^2)^2\Big], \end{aligned} \tag{17}$$

where we assume that $\mathbb{E}\{|\mathbf{s}_i|^4\} = \mathbb{E}\{|\tilde{\mathbf{s}}|^4\}\ \forall i$.

Following (12), the false alarm rate P_f can be obtained as:

$$\begin{aligned} P_f &= P_r\{\hat{\mathbf{R}}_{rs} \geq \lambda|H_0\} \\ &= \tfrac{1}{\sqrt{2\pi}\sigma_0}\int_{\lambda}^{\infty} e^{-\frac{(x-\mu_0)^2}{2\sigma_0^2}}\,dx \\ &= Q(\tfrac{\lambda-\mu_0}{\sigma_0}). \end{aligned} \tag{18}$$

Similarly, following (13), the miss detection probability P_m can be obtained as:

$$\begin{aligned} P_m &= P_r\{\hat{\mathbf{R}}_{rs} < \lambda|H_1\} \\ &= \tfrac{1}{\sqrt{2\pi}\sigma_1}\int_{-\infty}^{\lambda} e^{-\frac{(x-\mu_1)^2}{2\sigma_1^2}}\,dx \\ &= 1 - Q(\tfrac{\lambda-\mu_1}{\sigma_1}). \end{aligned} \tag{19}$$

Remark 1: As will be shown in Section VII, when $\lambda = \sigma_s^2/2$, both P_f and P_m are essentially zero, and independent of the SNR values. The underlying argument is that the detection of the primary user is based on $\mathbf{R}_{rs} = \alpha\sigma_s^2$ (see (4)), which is independent of both σ_m^2 and σ_n^2.

V. Analytical Evaluation for Malicious User Detection

A. False Alarm Rate and Miss Detection Probability for Malicious User Detection

In this subsection, we evaluate the false alarm rate and miss detection probability for the detection of malicious user.

Define $\tilde{P}_{f,0}$ and $\tilde{P}_{f,1}$ as the false alarm rate when $\hat{\alpha}=0$ or $\hat{\alpha}=1$, respectively,

$$\tilde{P}_{f,0} = Pr(\hat{H}_{01}|\hat{H}_{00}), \tag{20}$$
$$\tilde{P}_{f,1} = Pr(\hat{H}_{11}|\hat{H}_{10}). \tag{21}$$

The overall false alarm rate is given by:

$$\tilde{P}_f = \hat{P}_0\tilde{P}_{f,0} + (1-\hat{P}_0)\tilde{P}_{f,1}, \tag{22}$$

where $\hat{P}_0$ is the probability that $\hat{\alpha}=0$, i.e.,

$$\hat{P}_0 = (1-P_f)P(\alpha=0) + P_m P(\alpha=1). \tag{23}$$

As will be shown in Section VI, with the avalanche effect of the AES algorithm, the cross-correlation between the reference signal and the received signal is always around σ_s^2 or 0, depending on whether the primary user is present or absent, respectively. That is, P_f and P_m are negligible, as will be demonstrated in Section VII. Therefore, in the following, we assume that $\hat{\alpha}=\alpha$, and we do not distinguish between $\hat{H}_{\hat{\alpha}\beta}$ and $H_{\alpha\beta}$; it follows that $\hat{P}_0 = P_0 = P(\alpha=0)$. Hence, the overall false alarm rate is given by:

$$\tilde{P}_f = P_0\tilde{P}_{f,0} + (1-P_0)\tilde{P}_{f,1}. \tag{24}$$

Similarly, the miss detection probabilities can be defined as $\tilde{P}_{m,0}$ and $\tilde{P}_{m,1}$, when the primary user is absent and present, respectively, i.e.,

$$\tilde{P}_{m,0} = Pr(H_{00}|H_{01}). \tag{25}$$
$$\tilde{P}_{m,1} = Pr(H_{10}|H_{11}). \tag{26}$$

The overall malicious node miss detection probability is defined as:

$$\tilde{P}_m = P_0\tilde{P}_{m,0} + (1-P_0)\tilde{P}_{m,1}. \tag{27}$$

Since $\hat{\mathbf{R}}_{rr}$ is the averaged summation of a large number of random variables, then based on the central limit theorem, $\hat{\mathbf{R}}_{rr}$ can be modeled as a Gaussian random variable. Hence, we have:

$$\begin{cases} \hat{\mathbf{R}}_{rr} \sim \mathcal{N}(\mu_{00}, \sigma_{00}^2), & H_{00} \\ \hat{\mathbf{R}}_{rr} \sim \mathcal{N}(\mu_{01}, \sigma_{01}^2), & H_{01} \\ \hat{\mathbf{R}}_{rr} \sim \mathcal{N}(\mu_{10}, \sigma_{10}^2), & H_{10} \\ \hat{\mathbf{R}}_{rr} \sim \mathcal{N}(\mu_{11}, \sigma_{11}^2), & H_{11} \end{cases} \tag{28}$$

where μ_{00}, σ_{00}, μ_{01}, σ_{01}, μ_{10}, σ_{10}, and μ_{11}, σ_{11} can be derived as follows.

Under H_{00}, both the primary user and malicious user are absent, resulting in $\mathbf{r}_i = \mathbf{n}_i$. It follows that:

$$\mu_{00} = \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N}\mathbf{n}_i\mathbf{n}_i^*\right\} = \sigma_n^2, \tag{29}$$

and σ_{00}^2 can be obtained as:

$$\sigma_{00}^2 = \mathbb{E}\left\{|\hat{\mathbf{R}}_{rr}|^2\right\} - |\mu_{00}|^2 = \frac{1}{N}\left[\mathbb{E}\{|\tilde{\mathbf{n}}|^4\} - (\sigma_n^2)^2\right], \tag{30}$$

where we assume that $\mathbb{E}\{|\mathbf{n}_i|^4\} = \mathbb{E}\{|\tilde{\mathbf{n}}|^4\}\ \forall i$. Similarly, under H_{01}, the received signal is represented as $\mathbf{r}_i = \mathbf{m}_i + \mathbf{n}_i$, and the mean μ_{01} can be obtained as follows:

$$\mu_{01} = \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N}(\mathbf{m}_i+\mathbf{n}_i)(\mathbf{m}_i+\mathbf{n}_i)^*\right\} = \sigma_m^2 + \sigma_n^2. \tag{31}$$

The variance σ_{01}^2 can be obtained as:

$$\sigma_{01}^2 = \mathbb{E}\left\{|\hat{\mathbf{R}}_{rr}|^2\right\} - |\mu_{01}|^2 = \frac{1}{N}\Big[\mathbb{E}\{|\tilde{\mathbf{m}}|^4\} + \mathbb{E}\{|\tilde{\mathbf{n}}|^4\} + \mathbb{E}\{2\mathrm{Re}\{(\tilde{\mathbf{m}})^2(\tilde{\mathbf{n}}^*)^2\}\} + 2\sigma_m^2\sigma_n^2 - (\sigma_m^2)^2 - (\sigma_n^2)^2\Big], \tag{32}$$

where we assume that $\mathbb{E}\{|\mathbf{m}_i|^4\} = \mathbb{E}\{|\tilde{\mathbf{m}}|^4\}$ and $\mathbb{E}\{2\mathrm{Re}\{(\mathbf{m}_i)^2(\mathbf{n}_i^*)^2\}\} = \mathbb{E}\{2\mathrm{Re}\{(\tilde{\mathbf{m}})^2(\tilde{\mathbf{n}}^*)^2\}\}$, $\forall i$.

Under H_{10}, the received signal is expressed as $\mathbf{r}_i = \mathbf{s}_i + \mathbf{n}_i$, and the mean μ_{10} can be obtained as follows:

$$\mu_{10} = \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N}(\mathbf{s}_i+\mathbf{n}_i)(\mathbf{s}_i+\mathbf{n}_i)^*\right\} = \sigma_s^2 + \sigma_n^2, \tag{33}$$

and σ_{10}^2 can be obtained as:

$$\sigma_{10}^2 = \mathbb{E}\left\{|\hat{\mathbf{R}}_{rr}|^2\right\} - |\mu_{10}|^2 = \frac{1}{N}\Big[\mathbb{E}\{|\tilde{\mathbf{s}}|^4\} + \mathbb{E}\{|\tilde{\mathbf{n}}|^4\} + \mathbb{E}\{2\mathrm{Re}\{(\tilde{\mathbf{s}})^2(\tilde{\mathbf{n}}^*)^2\}\} + 2\sigma_s^2\sigma_n^2 - (\sigma_s^2)^2 - (\sigma_n^2)^2\Big]. \tag{34}$$

Similarly, under H_{11}, the received signal is represented as $\mathbf{r}_i = \mathbf{s}_i + \mathbf{m}_i + \mathbf{n}_i$, and the mean μ_{11} can be obtained as follows:

$$\mu_{11} = \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N}(\mathbf{s}_i+\mathbf{m}_i+\mathbf{n}_i)(\mathbf{s}_i+\mathbf{m}_i+\mathbf{n}_i)^*\right\} = \sigma_s^2 + \sigma_m^2 + \sigma_n^2. \tag{35}$$

The variance σ_{11}^2 can be obtained as:

$$\sigma_{11}^2 = \mathbb{E}\left\{|\hat{\mathbf{R}}_{rr}|^2\right\} - |\mu_{11}|^2 = \frac{1}{N}\Big[\mathbb{E}\{|\tilde{\mathbf{s}}|^4\} + \mathbb{E}\{|\tilde{\mathbf{m}}|^4\} + \mathbb{E}\{|\tilde{\mathbf{n}}|^4\} + \mathbb{E}\{2\mathrm{Re}\{(\tilde{\mathbf{s}})^2(\tilde{\mathbf{m}}^*)^2\}\} + \mathbb{E}\{2\mathrm{Re}\{(\tilde{\mathbf{s}})^2(\tilde{\mathbf{n}}^*)^2\}\} + \mathbb{E}\{2\mathrm{Re}\{(\tilde{\mathbf{m}})^2(\tilde{\mathbf{n}}^*)^2\}\} + 2\sigma_s^2\sigma_m^2 + 2\sigma_s^2\sigma_n^2 + 2\sigma_m^2\sigma_n^2 - (\sigma_s^2)^2 - (\sigma_m^2)^2 - (\sigma_n^2)^2\Big]. \tag{36}$$

Following the discussions above, we have:

$$\tilde{P}_{f,0} = P_r\{\hat{\mathbf{R}}_{rr} \geq \lambda_0|H_{00}\} = Q(\tfrac{\lambda_0-\mu_{00}}{\sigma_{00}}), \tag{37}$$

and

$$\tilde{P}_{f,1} = P_r\{\hat{\mathbf{R}}_{rr} \geq \lambda_1|H_{10}\} = Q(\tfrac{\lambda_1-\mu_{10}}{\sigma_{10}}). \tag{38}$$

Similarly, we have:

$$\tilde{P}_{m,0} = P_r\{\hat{\mathbf{R}}_{rr} < \lambda_0 | H_{01}\} = 1 - Q(\tfrac{\lambda_0 - \mu_{01}}{\sigma_{01}}), \quad (39)$$

and

$$\tilde{P}_{m,1} = P_r\{\hat{\mathbf{R}}_{rr} < \lambda_1 | H_{11}\} = 1 - Q(\tfrac{\lambda_1 - \mu_{11}}{\sigma_{11}}). \quad (40)$$

The overall false alarm rate $\tilde{P}_f$ and miss detection probability $\tilde{P}_m$ can be calculated following (24), (27). That is:

$$\tilde{P}_f = P_0 Q(\tfrac{\lambda_0 - \mu_{00}}{\sigma_{00}}) + (1 - P_0) Q(\tfrac{\lambda_1 - \mu_{10}}{\sigma_{10}}), \quad (41)$$

and

$$\tilde{P}_m = 1 - P_0 Q(\tfrac{\lambda_0 - \mu_{01}}{\sigma_{01}}) + (P_0 - 1) Q(\tfrac{\lambda_1 - \mu_{11}}{\sigma_{11}}). \quad (42)$$

In the next subsection, we discuss the optimal thresholds $\lambda_{0,opt}$ and $\lambda_{1,opt}$ that minimize the overall miss detection probability $\tilde{P}_m$ subject to a constraint on the false alarm rate.

B. The Optimal Thresholds for Malicious User Detection

In this subsection, we seek to obtain the optimal thresholds $\lambda_{0,opt}$ and $\lambda_{1,opt}$ that minimize the overall miss detection probability of the malicious node detection problem, while maintaining the false alarm rates below a certain threshold δ. This problem can be formulated as follows:

$$\begin{aligned} &min\ \tilde{P}_m \\ &subject\ to\ \tilde{P}_{f,0} \le \delta, \quad \text{and} \quad \tilde{P}_{f,1} \le \delta. \end{aligned} \quad (43)$$

It is noted that the problem formulation above is equivalent to:

$$\begin{aligned} &min\ \tilde{P}_{m,0} \\ &subject\ to\ \tilde{P}_{f,0} \le \delta, \end{aligned} \quad (44)$$

and

$$\begin{aligned} &min\ \tilde{P}_{m,1} \\ &subject\ to\ \tilde{P}_{f,1} \le \delta. \end{aligned} \quad (45)$$

Thus, we request:

$$\tilde{P}_{f,0} = Q(\tfrac{\lambda_0 - \mu_{00}}{\sigma_{00}}) \le \delta, \quad (46)$$

and

$$\tilde{P}_{f,1} = Q(\tfrac{\lambda_1 - \mu_{10}}{\sigma_{10}}) \le \delta, \quad (47)$$

which implies that:

$$\lambda_0 \ge \sigma_{00} Q^{-1}(\delta) + \mu_{00}, \quad (48)$$

and

$$\lambda_1 \ge \sigma_{10} Q^{-1}(\delta) + \mu_{10}. \quad (49)$$

Note that in order to minimize the overall miss detection probability $\tilde{P}_m$, λ_0 in (48), and λ_1 in (49) should be as small as possible. Hence, we set the thresholds to:

$$\lambda_{0,opt} = \sigma_{00} Q^{-1}(\delta) + \mu_{00}, \quad (50)$$

and

$$\lambda_{1,opt} = \sigma_{10} Q^{-1}(\delta) + \mu_{10}. \quad (51)$$

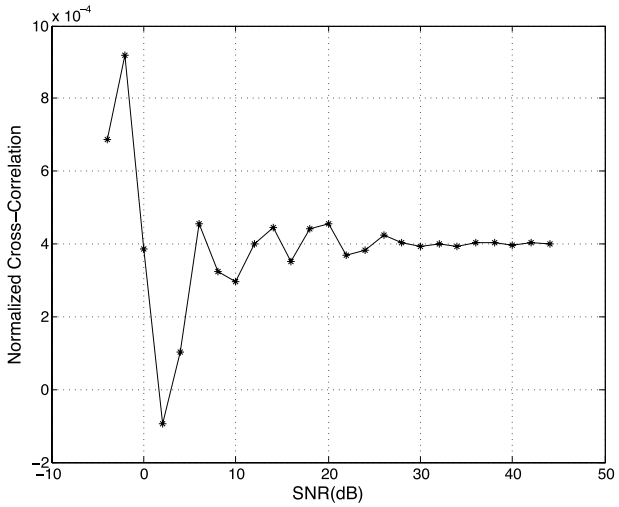


Fig. 3. Normalized cross-correlation between the reference signal and noisy versions of malicious user's signal. Note that the cross-correlation values are in the order of 10^{-4}, which is close to 0.

By substituting $\lambda_{0,opt}$ and $\lambda_{1,opt}$ in (42), we obtain the overall miss detection probability as:

$$\tilde{P}_m = 1 - P_0 Q(\tfrac{\sigma_{00} Q^{-1}(\delta) + \mu_{00} - \mu_{01}}{\sigma_{01}}) + (P_0 - 1) Q(\tfrac{\sigma_{10} Q^{-1}(\delta) + \mu_{10} - \mu_{11}}{\sigma_{11}}). \quad (52)$$

***Proposition** 1: For malicious user detection, to minimize the overall miss detection probability $\tilde{P}_m$ subject to the false alarm rate constraints $\tilde{P}_{f,0} \le \delta$ and $\tilde{P}_{f,1} \le \delta$, which also ensures that $\tilde{P}_f \le \delta$, we need to choose $\lambda_{0,opt} = \sigma_{00} Q^{-1}(\delta) + \mu_{00}$, and $\lambda_{1,opt} = \sigma_{10} Q^{-1}(\delta) + \mu_{10}$.*

VI. Security and Feasibility of the Proposed AES-Assisted DTV Approach

A. Security of the AES-Assisted DTV

As is well known, AES has been proved to be secure under all known attacks [25], in the sense that it is computationally infeasible to break AES in real time. In our case, this means that it is computationally infeasible for malicious users to regenerate the reference signal. Moreover, the AES algorithm has a very important security feature known as the *avalanche effect*, which means that a small change in the plaintext or the key yields a large change in the ciphertext [23]. Actually, even if one bit is changed in the plaintext, the ciphertext will be changed by approximately 50%. Therefore, it is impossible to recover the plaintext given the ciphertext only.

To illustrate the security of the AES-assisted DTV based on the avalanche effect, the cross-correlation between the reference signal and malicious signal under different SNR values is obtained, as shown in Fig. 3. It can be seen that the cross-correlation values are around μ_0 in (14), which implies that the malicious signal and the reference signal are uncorrelated. On the other hand, the cross-correlation between the reference signal and noisy versions of the primary signal is shown to be very high (around μ_1 in (16)), under all SNR values, as depicted in Fig. 4. It should be appreciated that in the DTV system, the minimum SNR is 28.3 dB [21].

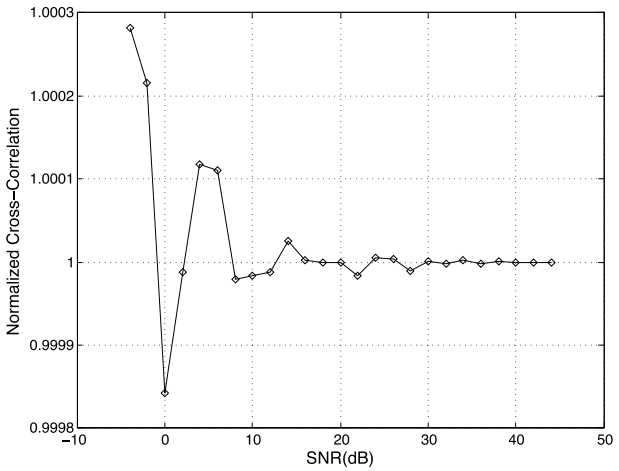


Fig. 4. Normalized cross-correlation between the reference signal and noisy versions of the primary user's signal. Here, $\sigma_s^2 = 1$.

These results show that the AES-assisted DTV scheme is secure under PUEA, as malicious users cannot regenerate the reference signal in real time.

B. Mitigation of PUEA

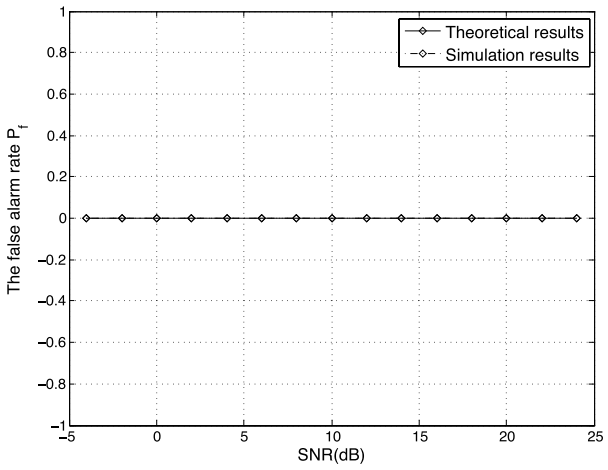
The approaches proposed in the previous sections enable the secondary users to identify the primary signal, as well as malicious nodes. Note that due to the large range of DTV channels, the malicious users would not be capable of jamming all DTV white spaces simultaneously. When a primary user emulation attack is detected, the secondary users can adopt different methodologies for effective transmission, such as:

- *Exploit techniques that are inherently jamming-resistant*, such as Code Division Multiple Access (CDMA) and Frequency Hopping (FH) techniques [26]–[29]. Both CDMA and FH were initially developed for secure military communications. CDMA is particularly efficient under narrow-band jamming [30], even if the malicious user hops from band to band. FH based systems are generally robust under wide-band jamming; when the malicious jamming pattern is time-varying, i.e., the malicious user switches between wide-band and narrow-band jamming, the transmitter then needs to be adjusted to combat the cognitive hostile attacks.
- *Avoid transmission on the white spaces jammed by malicious nodes*. For example, consider the case where the benign secondary users are OFDM-based transceivers, then they can shape their transmitted signal through proper precoding design to avoid communication over the jammed subcarriers [31].

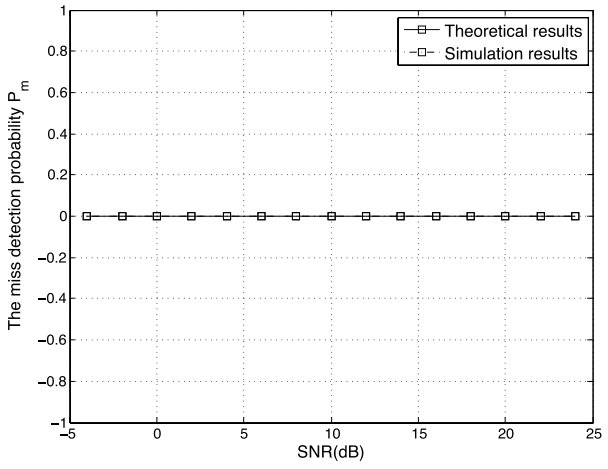
  For time-varying attacks, the precoder should be adapted accordingly for transmission. This necessitates that jamming detection needs to be performed in real-time, which can generally be achieved by evaluating the time-varying power spectrum of the jamming signal [28].

C. Feasibility

In this subsection, we show that it is practical to generate the required sync bits within the frame time duration shown in Fig. 1.



(a)



(b)

Fig. 5. Example 1: The false alarm rate and miss detection probability for primary user detection. (a) The false alarm rate P_f, the two curves are identical. (b) The miss detection probability P_m, the two curves are identical.

The AES algorithm is one of the block ciphers that can be implemented in different operational modes to generate stream data [32]. High-throughput (3.84 Gbps and higher) AES chips can be found in [19] and [20]. In [33], an experiment was performed to measure the AES algorithm performance, where several file sizes from 100KB to 50MB were encrypted using a laptop with 2.99 GHz CPU and 2 GB RAM. Based on the results of the experiment, when the AES operates in the cipher feedback (CFB) mode, 554bytes can be encrypted using 256-bit AES algorithm in 77.3 μs. Therefore, even the 2.99GHz CPU can generate the required AES reference signal within the frame time duration. Note that the TV stations generally have powerful processing units, hence it is not a problem to generate the required secure sync bits within the frame duration. With 3.84 Gbps encryption speed, for example, 39KB can be encrypted in 77.3 μs, which is more than adequate.

VII. Simulations

In this section, we demonstrate the effectiveness of the AES-assisted DTV scheme through simulation examples. First,

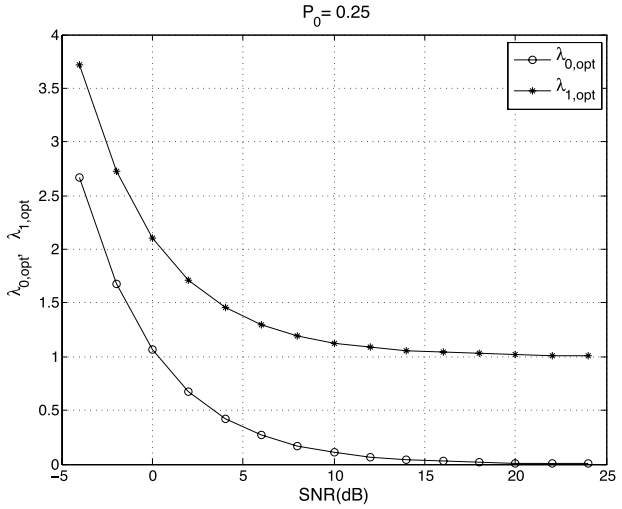


Fig. 6. Example 2: The optimal thresholds for malicious user detection for $\delta = 10^{-3}$. Here, $P_0 = 0.25$.

we illustrate the impact of the noise level on the optimal thresholds $\lambda_{0,opt}$ and $\lambda_{1,opt}$. Then, we evaluate the false alarm rates and miss detection probabilities for both primary user and malicious user detection. In the simulations, we assume that $\mathbf{s}_i$, $\mathbf{m}_i$, and $\mathbf{n}_i$ are i.i.d. sequences, and are of zero mean. We further assume that the primary user is absent with probability $P_0 = 0.25$. The primary user's signal power is assumed to be normalized to $\sigma_s^2 = 1$. For malicious user detection, we set the false alarm constraint $\delta = 10^{-3}$.

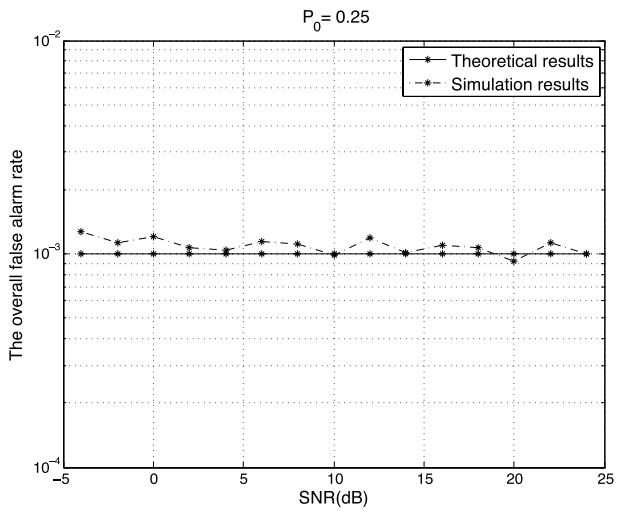
Example 1: False alarm rate and miss detection probability for primary user detection. Using $\lambda = \sigma_s^2/2$, we obtain the false alarm rate and miss detection probability numerically and compare them with the theoretical results. The false alarm rate is illustrated in Fig. 5(a). It is noted that the theoretical false alarm rate P_f in (18) depends on β, since σ_0^2 is a function of β. However, based on (15) and the avalanche effect of the AES algorithm, this dependency becomes negligible when N is large. This can be seen from Fig. 5(a) as the theoretical calculations match perfectly with the numerical simulations.

The probability of miss detection is shown in Fig. 5(b). It also can be seen that the theoretical calculations and numerical simulations are matched perfectly. It is clear that the proposed AES-assisted DTV approach achieves $zero$ false alarm rate and miss detection probability under a large range of SNR values.

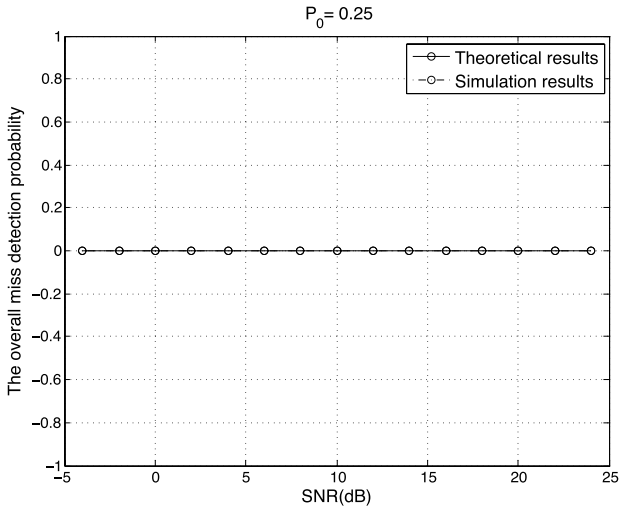
Example 2: The optimal thresholds for malicious user detection. In this example, we demonstrate the optimal thresholds that minimize the miss detection probabilities under a predefined constraint on the false alarm rates for malicious user detection.

Fig. 6 shows the two optimal thresholds $\lambda_{0,opt}$ and $\lambda_{1,opt}$ versus SNR for $\delta = 10^{-3}$. We observe that the two curves decrease as the SNR increases, which can be verified with (50) and (51).

Example 3: False alarm rate and miss detection probability for malicious user detection. In this example, we obtain the overall false alarm rate and miss detection probability numerically and compare them with the theoretical results. Fig. 7(a) shows the overall false alarm rate $\tilde{P}_f$ for



(a)



(b)

Fig. 7. Example 3: The overall false alarm rate and the overall miss detection probability for malicious user detection. Here, $P_0 = 0.25$ and $\delta = 10^{-3}$. (a) The overall false alarm rate $\tilde{P}_f$. (b) The overall miss detection probability $\tilde{P}_m$, the two curves are identical.

$\delta = 10^{-3}$. It is noted that the theoretical calculations and numerical simulations are almost equal, and the predefined false alarm constraint δ is satisfied.

The overall miss detection probability $\tilde{P}_m$ is illustrated in Fig. 7(b). It is shown that the proposed approach achieves $zero$ overall miss detection probability under a large range of SNR values.

From the discussions above, it is concluded that the proposed AES-assisted DTV can achieve very low false alarm rates and miss detection probabilities when detecting the primary user and malicious user . That is, with the proposed AES-assisted DTV scheme, primary user emulation attacks can be effectively combated. The theoretical calculations presented in Sections IV and V are consistent with the numerical simulations.

VIII. Conclusion

In this paper, a reliable AES-assisted DTV scheme was proposed for robust primary and secondary system operations

under primary user emulation attacks. In the proposed scheme, an AES-encrypted reference signal is generated at the TV transmitter and used as the sync bits of the DTV data frames. By allowing a shared secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver and be used to achieve accurate identification of authorized primary users. Moreover, when combined with the analysis on the auto-correlation of the received signal, the presence of the malicious user can be detected accurately no matter the primary user is present or not. The proposed approach is practically feasible in the sense that it can effectively combat PUEA with no change in hardware or system structure except of a plug-in AES chip. Potentially, it can be applied directly to today's HDTV systems for more robust spectrum sharing. It would be interesting to explore PUEA detection over each sub-band in multi-carrier DTV systems.

REFERENCES

[1] FCC, "Spectrum policy task force report," Federal Commun. Commission, Columbia, SC, USA, Tech. Rep. ET Docket No. 02-135, Nov. 2002.

[2] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[3] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Comput. Netw., Int. J. Comput. Telecommun. Netw.*, vol. 50, no. 13, pp. 2127–2159, Sep. 2006.

[4] M. Thanu, "Detection of primary user emulation attacks in cognitive radio networks," in *Proc. Int. Conf. CTS*, May 2012, pp. 605–608.

[5] Q. Zhao and B. Sadler, "A survey of dynamic spectrum access," *IEEE Signal Process. Mag.*, vol. 24, no. 3, pp. 79–89, May 2007.

[6] FCC, "Unlicensed operation in the TV broadcast bands and additional spectrum for unlicensed devices below 900 MHz and in the 3 GHz band," Federal Commun. Commission, Columbia, SC, USA, Tech. Rep. ET Docket No. 04-186 and 02-380, Sep. 2010.

[7] R. Chen and J.-M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *Proc. IEEE Workshop Netw. Technol. Softw. Defined Radio Netw.*, Sep. 2006, pp. 110–119.

[8] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in *Proc. 3rd IEEE Symp. New Frontiers Dyn. Spectrum Access Netw.*, Oct. 2008, pp. 1–6.

[9] R. Chen, J.-M. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[10] 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 *Proc. IEEE WCNC*, Mar. 2011, pp. 599–604.

[11] 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 J. Sel. Areas Commun.*, vol. 30, no. 10, pp. 1850–1860, Nov. 2012.

[12] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2009, pp. 1–5.

[13] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," *SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 13, no. 2, pp. 74–85, 2009.

[14] C. Chen, H. Cheng, and Y.-D. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack," *IEEE Trans. Wireless Commun.*, vol. 10, no. 7, pp. 2135–2141, Jul. 2011.

[15] C. Mathur and K. P. Subbalakshmi, "Digital signatures for centralized DSA networks," in *Proc. 4th IEEE CCNC*, Jan. 2007, pp. 1037–1041.

[16] K. Borle, B. Chen, and W. Du, "A physical layer authentication scheme for countering primary user emulation attack," in *Proc. IEEE ICASSP*, May 2013, pp. 2935–2939.

[17] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surv. Tuts.*, vol. 15, no. 1, pp. 428–445, Mar. 2013.

[18] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *Proc. IEEE Symp. SP*, May 2010, pp. 286–301.

[19] 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 *Proc. 15th ACM Great Lakes Symp. VLSI*, New York, NY, USA, 2005, pp. 60–63.

[20] S.-Y. Lin and C.-T. Huang, "A high-throughput low-power AES cipher for network applications," in *Proc. ASP-DAC*, Jan. 2007, pp. 595–600.

[21] ATSC, "ATSC digital television standard part 2: RF/Transmission system characteristics," Adv. Television Syst. Committee, Washington, DC, USA, Tech. Rep. ET Docket No. A/53, Dec. 2011.

[22] V.-H. Pham, J.-Y. Chouinard, A. Semmar, X. Wang, and Y. Wu, "Enhanced ATSC DTV channel estimation," in *Proc. Canadian Conf. Electr. Comput. Eng.*, May 2009, pp. 772–776.

[23] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, Jan. 2010.

[24] ETSI, "Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television," Eur. Telecommun. Stand. Inst., Final Rep. ETSI EN 300 744, Jan. 2009.

[25] C. Sanchez-Avila and R. Sanchez-Reillo, "The Rijndael block cipher (AES proposal): A comparison with DES," in *Proc. IEEE 35th Int. Carnahan Conf. Security Technol.*, Oct. 2001, pp. 229–234.

[26] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping—Part I: System design," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 70–79, Jan. 2013.

[27] L. Zhang and T. Li, "Anti-jamming message-driven frequency hopping—Part II: Capacity analysis under disguised jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 80–88, Jan. 2013.

[28] L. Zhang, J. Ren, and T. Li, "Time-varying jamming modeling and classification," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3902–3907, Jul. 2012.

[29] L. Lightfoot, L. Zhang, J. Ren, and T. Li, "Secure collision-free frequency hopping for OFDMA-based wireless networks," *EURASIP J. Adv. Signal Process.*, vol. 2009, pp. 1:1–1:11, Mar. 2009.

[30] T. Li, Q. Ling, and J. Ren, "Physical layer built-in security analysis and enhancement algorithms for CDMA systems," *EURASIP J. Wireless Commun. Netw.*, vol. 2007, no. 1, p. 083589, Jul. 2007.

[31] M. Abdelhakim, J. Ren, and T. Li, "Reliable OFDM system design under hostile multi-tone jamming," in *Proc. IEEE Global Commun. Conf.*, Dec. 2012, pp. 4290–4295.

[32] T. Good and M. Benaissa, "AES as stream cipher on a small FPGA," in *Proc. IEEE ISCAS*, May 2006, p. 4.

[33] N. Singhal and J. Raina, "Comparative analysis of AES and RC4 algorithms for better utilization," *Int. J. Comput. Trends Technol.*, pp. 177–181, Aug. 2011.



Ahmed Alahmadi received the B.S. degree in electrical engineering from Taibah University, Madina, Saudi Arabia, in 2010. He was with the Department of Electrical Engineering, Taibah University, as a Teaching Assistant, in 2010. He is currently pursuing the master's degree in electrical and computer engineering at Michigan State University. His research interests include wireless communications and networking, and wireless security.



Mai Abdelhakim received the B.Sc. and M.Sc. degrees in communications engineering from Cairo University in 2006 and 2009, respectively. She is currently a Graduate Research Assistant with the Electrical and Computer Engineering Department, Michigan State University, where she is currently pursuing the Ph.D. degree. Her current research focuses on reliable and efficient communications in sensor networks and high-speed wireless networks.



Jian Ren received the B.S. and M.S. degrees in mathematics from Shaanxi Normal University, and the Ph.D. degree in electrical engineering from Xidian University, China. He is an Associate Professor with the Department of Electrical and Computer Engineering, Michigan State University. His current research interests include cryptography, network security, cloud computing security, energy efficient sensor network security protocol design, privacy-preserving communications, and cognitive networks. He is a recipient of the U.S. National Science Foundation Faculty Early Career Development (CAREER) Award in 2009.



Tongtong Li received the Ph.D. degree in electrical engineering from Auburn University in 2000. She is an Associate Professor with the Department of Electrical and Computer Engineering, Michigan State University. Her research interests fall into the areas of wireless and wired communications, wireless security, information theory, and statistical signal processing. She is currently serving as an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING.