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

Ahmed Alahmadi Mai Abdelhakim Jian Ren Tongtong Li
Department of Electrical & Computer Engineering
Michigan State University, East Lansing, MI 48824, USA
Email: {alahmadi, abdelhak, renjian, tongli}@egr.msu.edu

***Abstract*—This paper considers primary user emulation attacks (PUEA) in cognitive radio networks operating in the white spaces of the digital TV (DTV) band. We propose a reliable AES-encrypted DTV scheme, in which an AES-encrypted reference signal is generated at the TV transmitter and used as the sync bytes of each DTV data frame. 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. We analyze the effectiveness of the proposed approach through both theoretical derivation and simulation examples. It is shown that with the AES-encrypted DTV scheme, the primary user can be detected with high accuracy and low false alarm rate under primary user emulation attacks. It should be emphasized that the proposed scheme requires no changes in hardware or system structure except of a plug-in AES chip. Potentially, it can be applied to today's DTV system directly to mitigate primary user emulation attacks, and achieve efficient spectrum sharing.**

***Index Terms*—Cognitive Radio Networks, 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 radio spectrum, spectrum scarcity has become a pressing problem 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 provide a promising solution to the spectrum scarcity and underutilization problems [2].

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. The spectrum sharing is made under the condition that the secondary users do not interfere with the primary system's traffic. The CRs identify the unused bands (white spaces) through *spectrum sensing*, then utilize the idle bands for data transmissions. The spectrum sensing function is continuously performed. If a secondary user detected a primary signal in the band that it operates in, it should evacuate the band and operate in another white space.

The CR system is vulnerable to malicious attacks that would disrupt its operation. A well-known malicious attack is the primary user emulation attack (PUEA) [3]. In PUEA, the malicious users mimic the primary signal over the idle frequency band(s) such that the secondary users cannot use the corresponding white space(s). This leads to low spectrum utilization and inefficient cognitive network operation.

Several methods have been proposed to detect PUEA, such as in [4], [5], which considered the PUEA problem in the television (TV) spectrum bands. In [5], the direction of arrival (DOA) and the received power level are exploited jointly to obtain the transmitter's location and hence detect the malicious devices. That is, given the locations of the primary TV stations, the secondary user can distinguish the actual primary signal from the malicious user's signal by estimating the transmitter's DOA and the power level. A major limitation with the location-dependent detection approaches based on DOA and/or power level is that a malicious user can be at a location where it has the same DOA and comparable power level as that of the actual primary transmitter.

In this paper, we propose a reliable AES-encrypted DTV scheme, in which an AES-encrypted reference signal is generated at the TV transmitter and used as the sync bytes of each DTV data frame. 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. The proposed approach can effectively mitigate PUE attacks with no change in hardware or system structure except of a plug-in AES chip, which has been commercialized and widely available. In the DTV system, the generated AES-encrypted reference signal is also used for synchronization purposes at the authorized receivers.

The proposed model mitigates primary user emulation attacks, enables robust system operation, and ensures efficient spectrum sharing. The effectiveness of the proposed approach is demonstrated through both theoretical derivation and simulation examples. It is shown that with the AES-encrypted DTV scheme, the primary user can be detected with high accuracy

This research is partially supported by National Science Foundation under awards: CNS 0746811, CNS 1217206, and CNS 1117831.

978-1-4799-1353-4/13/$31.00 ©2013 IEEE

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 our proposed AES-encrypted DTV approach. In Section IV, analytical system evaluation is provided. Security analysis of our model is discussed in Section V. Numerical simulations are presented in Section VI. Finally, the paper is concluded in Section VII.

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 DTV system, the eight-level vestigial sideband (8-VSB) modulation is used for transmitting digital signals after they are partitioned into frames [6]. 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 to synchronize the frame and to estimate the channel impulse response [6], [7]. The remaining 624 segments are used for data transmission. Each data segment contains 832 symbols, including 4 symbols used for segment synchronization and data synchronization (field sync byte). The segment and field synchronization bits are identical for all data segments. The segment duration is 77.3 μs, hence the overall time for one frame is 48.4 ms [6].

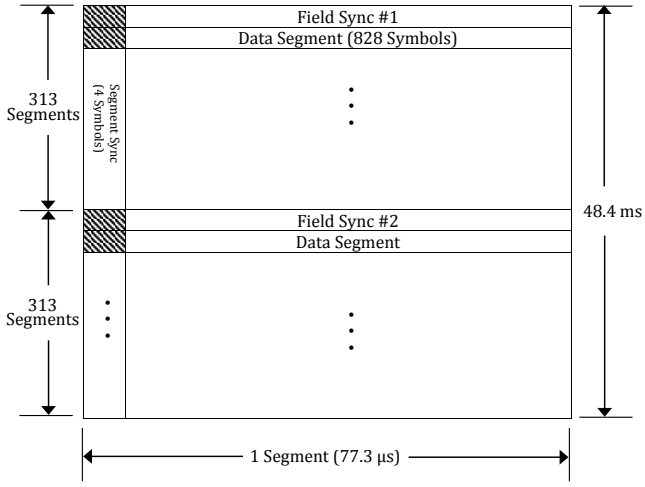

Fig. 1. 8-VSB signal frame structure.

III. The Proposed AES-Encrypted DTV Approach

In this section, we present our proposed AES-encrypted 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 624 segment sync bytes. The two sync bytes in the field sync segments remain unchanged for the channel estimation purposes. At the receiving end, the reference signal is regenerated for primary user detection. It should be emphasized that synchronization is still guaranteed in the proposed model since the reference bits are also used for synchronization purposes. In the following subsections, we discuss the AES-encrypted DTV transmitter and receiver in more details.

A. AES-encrypted 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 *Linear Feedback Shift Register* (LFSR)[1]. Maximum-length LFSR sequences can be achieved by tapping the LFSR according to primitive polynomials. The maximum sequence length that can be achieved with the primitive polynomials is $2^m - 1$, where m is the number of registers. Without loss of generality, a maximum-length sequence is assumed throughout this paper.

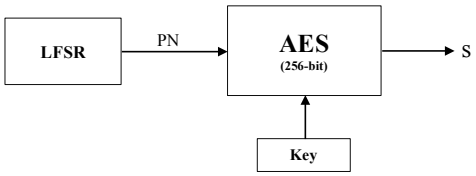

Fig. 2. Block diagram for generating the reference signal.

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 is used for the AES encryption so that the maximum possible security is achieved. Security analysis will be provided in Section V.

Denote the PN sequence by x, then the output (i.e. the reference signal) of the AES algorithm is expressed as follows:

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

where k is the key, and $E(.,.)$ denotes the AES encryption. The transmitter places the reference signal s in the 624 sync bytes of the DTV data segments.

B. AES-encrypted DTV receiver

The receiver regenerates the encrypted reference signal. We assume that the secret key is available at the receiver and the PN sequence can be regenerated. A cross-correlation detector is employed, where the receiver evaluates the cross-correlation between the received signal $r = s + n$ and the regenerated reference signal s, where n represents noise. The cross-correlator output can be represented as:

$$R_{rs} \triangleq \sum_{i=1}^{N} \frac{r_i \cdot s_i}{N}, \tag{2}$$

where N is the signal length, s_i and r_i are the ith symbols of the reference and received signals, respectively.

[1]Any other pseudo-random generators can be used as well.

To distinguish between the actual TV transmitter and an attacker emulating the primary signal, the receiver compares the cross-correlator output to a predefined threshold λ. We have two cases:

- If the cross-correlator output is greater than or equal to λ, i.e.
$$R_{rs} \geq \lambda, \tag{3}$$
then the receiver concludes that the primary user is present.
- If the cross-correlator output is less than λ, i.e.
$$R_{rs} < \lambda, \tag{4}$$
then the receiver concludes that the primary user is absent.

This detection problem can be modeled as a binary hypothesis test problem under the following two hypotheses,

H_0: the primary user is absent

H_1: the primary user is present

The performance of the detection process is evaluated through the *false alarm rate* and *miss detection probability*, as will be discussed in Section IV. The optimal threshold that minimizes the miss detection probability subject to a false alarm rate constraint is also obtained in Section IV.

C. Feasibility

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

The AES algorithm is one of the block ciphers that can be implemented in different operational modes to generate stream data. In [8], Singhal et al. performed an experiment to measure the AES algorithm performance. They encrypted several file sizes from 100KB to 50MB using a laptop with 2.99 GHz processor. Based on their experiment, when the AES operates in the cipher feedback (CFB) mode [9], 554bytes can be encrypted using 256-bit AES algorithm in 77.3 μs. Therefore, 2.99GHz CPU can generate the encrypted AES reference signal within the frame duration. Note that the TV stations generally have much faster processing units, hence it is not a problem to generate the required secure sync bytes within one frame duration.

IV. Analytical system evaluation

A. False alarm rate and miss detection probability

In this subsection, we analyze the system performance through the miss detection probability and the false alarm rate. The miss detection probability (P_m) is the conditional probability that the primary is assumed absent, when it is present, i.e.,

$$P_m = Pr(H_0|H_1). \tag{5}$$

The false alarm rate (P_f) is the conditional probability that the primary user is assumed present, when it is not, i.e.,

$$P_f = Pr(H_1|H_0). \tag{6}$$

As can be seen from (2), the cross-correlator output is the summation of N random variables. Since N is very large, then from the central limit theorem, the cross-correlator output can be modeled as a Gaussian random variable. That is, under H_1, $R_{rs} \sim \mathcal{N}(\mu_1, \sigma_1^2)$, where μ_1 and σ_1^2 are the mean and the variance of the cross-correlator output, respectively, under H_1.

The miss detection probability P_m can be obtained as:

$$\begin{aligned} P_m &= P_r\{R_{rs} < \lambda | H_1\} \\ &= \int_{-\infty}^{\lambda} \frac{1}{\sigma_1\sqrt{2\pi}} e^{-\frac{(X-\mu_1)^2}{2\sigma_1^2}} dX \\ &= 1 - \int_{\lambda}^{\infty} \frac{1}{\sigma_1\sqrt{2\pi}} e^{-\frac{(X-\mu_1)^2}{2\sigma_1^2}} dX \\ &= 1 - Q(\tfrac{\lambda-\mu_1}{\sigma_1}). \end{aligned} \tag{7}$$

Note that under H_1, the received signal is represented as $r_i = s_i + n_i$, where s_i is the ith primary symbol, and $n_i \sim \mathcal{N}(0, \sigma_n^2)$. We assume that the primary signal has zero mean and power P_s, i.e., $\mathbb{E}\{s_i^2\} = P_s \ \forall i$. We further assume that both $\{s_i\}$ and $\{n_i\}$ are i.i.d. sequences, and $\{s_i\}$ and $\{n_i\}$ are independent.

Under these assumptions, the mean μ_1 can be obtained as follows:

$$\begin{aligned} \mu_1 &= \mathbb{E}\left\{\frac{\sum_{i=1}^{N}(s_i+n_i)s_i}{N}\right\} \\ &= \mathbb{E}\left\{\frac{\sum_{i=1}^{N} s_i^2}{N}\right\} \\ &= P_s. \end{aligned} \tag{8}$$

The variance σ_1^2 is obtained as:

$$\begin{aligned} \sigma_1^2 &= \mathbb{E}\{R_{rs}^2\} - \mu_1^2 \\ &= \mathbb{E}\left\{\frac{\sum_{i=1}^{N}(s_i+n_i)s_i}{N}\frac{\sum_{j=1}^{N}(s_j+n_j)s_j}{N}\right\} - P_s^2 \\ &= \frac{1}{N^2}\mathbb{E}\left\{\sum_{i=1}^{N}\sum_{j=1}^{N}\left[s_i^2 s_j^2 + n_i n_j s_i s_j\right]\right\} - P_s^2 \\ &= \frac{1}{N^2}\left[\sum_{i=1}^{N}\left(\mathbb{E}\{s_i^4\} + \mathbb{E}\{n_i^2\}\mathbb{E}\{s_i^2\}\right)\right. \\ &\quad \left. + \sum_{i=1}^{N}\sum_{\substack{j=1 \\ j\neq i}}^{N}\left(\mathbb{E}\{s_i^2\}\mathbb{E}\{s_j^2\} + \mathbb{E}\{n_i n_j\}\mathbb{E}\{s_i s_j\}\right)\right] - P_s^2 \\ &= \frac{1}{N}\left[\mathbb{E}\{\tilde{s}^4\} + P_s(\sigma_n^2 - P_s)\right], \end{aligned} \tag{9}$$

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

Similarly, under H_0, $R_{rs} \sim \mathcal{N}(\mu_2, \sigma_2^2)$, where μ_2 and σ_2^2 are the mean and the variance of the cross-correlator output under H_0, respectively. The false alarm rate P_f can be defined

as:

$$\begin{aligned} P_f &= P_r\{R_{rs} > \lambda | H_0\} \\ &= \int_{\lambda}^{\infty} \frac{1}{\sigma_2\sqrt{2\pi}} e^{-\frac{(X-\mu_2)^2}{2\sigma_2^2}} dX \\ &= Q(\tfrac{\lambda-\mu_2}{\sigma_2}). \end{aligned} \tag{10}$$

The received signal under H_0 is represented as $r_i = n_i$; since with AES encryption even if the malicious user is present, it is regarded as noise. In this case, let $n_i \sim \mathcal{N}(0, \sigma_{n,0}^2)$, where $\sigma_{n,0}^2$ is the noise variance under H_0.

Therefore, the mean μ_2 is obtained as:

$$\begin{aligned} \mu_2 &= \mathbb{E}\{\frac{\sum_{i=1}^{N} n_i s_i}{N}\} \\ &= 0, \end{aligned} \tag{11}$$

and σ_2^2 is obtained as:

$$\begin{aligned} \sigma_2^2 &= \mathbb{E}\{R_{rs}^2\} - \mu_2^2 \\ &= \frac{1}{N^2}\mathbb{E}\left\{\sum_{i=1}^{N}\sum_{j=1}^{N}[n_i s_i n_j s_j]\right\} \\ &= \frac{1}{N^2}\sum_{i=1}^{N}\mathbb{E}\{n_i^2 s_i^2\} \\ &= \frac{\sigma_{n,0}^2 P_s}{N}. \end{aligned} \tag{12}$$

In the next subsection, we obtain the optimal threshold that minimizes the miss detection probability under a constraint on the false alarm rate.

B. Evaluation of the optimal threshold

The objective is to minimize the miss detection probability P_m under a false alarm constraint $P_f \leq \beta$. That is, our problem can be formulated as follows:

$$\begin{aligned} &\text{Minimize} \quad P_m \\ &\text{Subject to} \quad P_f \leq \beta. \end{aligned} \tag{13}$$

In order to have $P_f \leq \beta$, using equation (10) we get:

$$P_f = Q(\tfrac{\lambda-\mu_2}{\sigma_2}) \leq \beta, \tag{14}$$

It follows that

$$\lambda \geq \sigma_2 Q^{-1}(\beta) + \mu_2, \tag{15}$$

where $Q^{-1}(\cdot)$ is the inverse Q-function[1].

It can be seen from (7) that in order to minimize the miss detection probability, λ should be as low as possible. Therefore, we choose the lowest λ that satisfies the false alarm constraint. Thus, the optimal λ that minimizes P_m and satisfies the false alarm constraint is

$$\lambda_{Opt} = \sigma_2 Q^{-1}(\beta) + \mu_2. \tag{16}$$

[1]The Q-function is defined as: $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^{\infty} e^{-\frac{u^2}{2}} du$.

Substituting by λ_{Opt} in (7), we get the miss detection probability of the proposed approach. More specifically, we get

$$\begin{aligned} P_m &= 1 - Q\left(\tfrac{\sigma_2 Q^{-1}(\beta) + \mu_2 - \mu_1}{\sigma_1}\right) \\ &= 1 - Q\left(\alpha Q^{-1}(\beta) + \gamma\right), \end{aligned} \tag{17}$$

where, $\alpha = \frac{\sigma_2}{\sigma_1}$ and $\gamma = \frac{\mu_2 - \mu_1}{\sigma_1}$. Therefore, we have the following result:

Proposition 1: *To minimize the miss detection probability subject to the false alarm rate constraint $P_f \leq \beta$, we need to set the threshold of the cross-correlator of the AES-encrypted DTV receiver to $\lambda_{Opt} = \sigma_2 Q^{-1}(\beta) + \mu_2$, where μ_2 and σ_2 are the mean and standard deviation of the cross-correlator output when the primary user is absent, i.e. under H_0.*

V. Security Analysis of the Proposed AES-Encrypted DTV Approach

A. A brief overview of AES

AES is a robust symmetric-key cipher, in which a *single key* is used for both encryption and decryption. The key is shared between the transmitter and the receiver and is kept private. Fig. 3 shows the general structure of the AES encryption algorithm. It mainly consists of four stages that are applied to the input data, which is arranged in 4×4 array of bytes. The four stages are repeated, and the number of repetition depends on the key length. The four stages of AES are:

1) SubBytes Stage
   In this stage, each byte in the 4×4 array is simply mapped to another byte based on a lookup table called the S-box. The security reason for creating the S-box is to thwart all the known cryptanalytic attacks [9].
2) ShiftRows Stage
   Here, each row in the 4×4 data array, except the first row, is shifted to the left by a number of bytes. In particular, the second row is shifted to the left by 1 byte, while the third and fourth are shifted by 2 bytes and 3 bytes, respectively. The ShiftRows stage provides diffusion in the cipher so that the output of the AES algorithm (i.e. the ciphertext) carries no statistical relationship to the input (i.e. the plaintext) [9].
3) MixColumns
   In this stage, each byte in a column is replaced by a com-

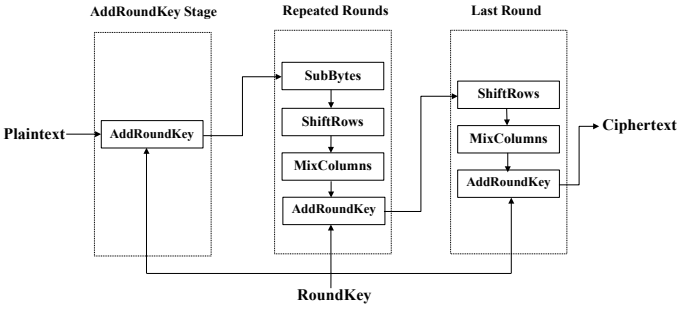

Fig. 3. AES encryption.

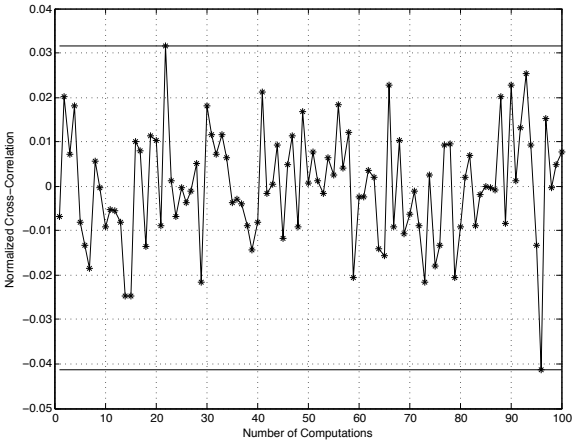

Fig. 4. Normalized cross-correlation between several computations for malicious users and the reference signal.

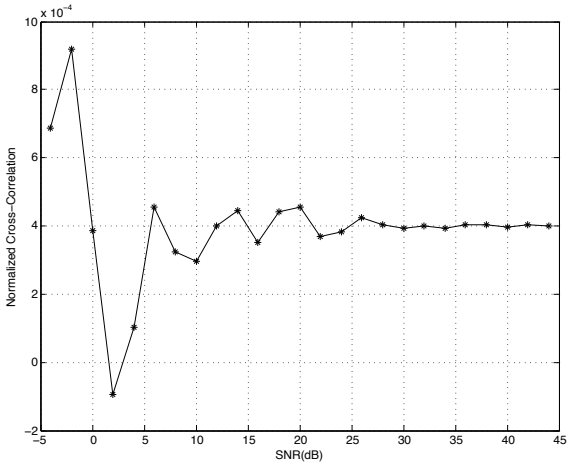

Fig. 5. Normalized cross-correlation between the reference signal and noisy versions of a malicious user. Note that the cross-correlation values are in the order of $10^{-4} \approx 0$.

bination of the fours bytes within the same column. The MixColumns operation also provides diffusion property [9].

4) AddRoundKey
In this stage, each byte in the array is added to the RoundKey array using bit-wise XOR function. The AddRoundKey stage is used to impact every bit within the array [9].

It has been proved that AES is secure under all known attacks [9]. More specifically, it is computationally infeasible to break AES.

B. Security of the AES-encrypted DTV

The AES algorithm has a very important security feature, besides the above, known as the *avalanche effect*. The avalanche effect means that a small change in the plaintext or the key yields to a large change in the ciphertext.

Because of the avalanche effect of the AES algorithm, if two random plaintexts are applied to AES algorithm, the resulting ciphertexts will have approximately 50% correlation [9]. Actually, even if one bit is changed in the plaintext, the correlation in the ciphertext will be approximately 50%.

To illustrate the security of the AES-encrypted DTV based on the avalanche effect, we obtain the cross-correlation between different malicious signals and the reference signal. From Fig. 4, we see that the cross-correlation values are scattered within a small range around μ_2 in (11), which corresponds to approximately 50% correlation between the malicious and the reference signals. It is shown that even with different SNR values the cross-correlator output is still around μ_2, as illustrated in Fig. 5. On the other hand, the cross-correlation between the primary user and its noisy versions is shown to be very high (i.e. around μ_1 in (8)) under all SNR values, as depicted in Fig. 6. In the DTV system, the minimum SNR is 28.3 dB [6].

Based on the security of AES and our analysis above, we can see that it is impossible for the malicious users to obtain the AES-encrypted sync bits. Therefore, it is computationally infeasible for the malicious users to mimic the authorized primary users in real-time.

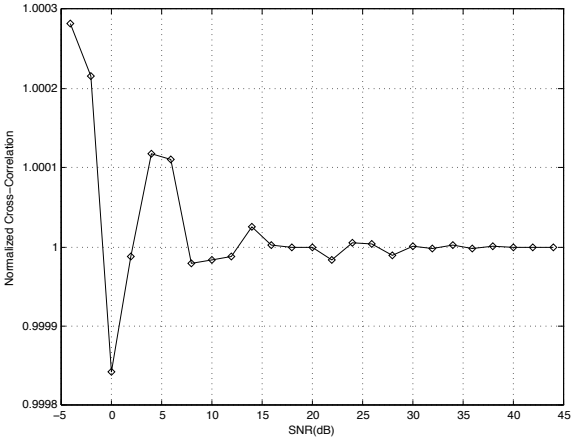

Fig. 6. Normalized cross-correlation between the reference signal and its noisy versions. Here, $P_s = 1$.

VI. Simulations

In this section, we demonstrate the effectiveness of our proposed approach through simulation examples. First, we illustrate the impact of varying the false alarm constraint β on the optimal threshold λ_{Opt} values. Then, we evaluate the false alarm rate and miss detection probability of the proposed approach.

The optimal threshold: We evaluate the optimal threshold λ_{Opt} that minimizes the miss detection probability under predefined false alarm constraint $P_f \leq \beta$. Fig. 7 shows the optimal λ_{Opt} versus SNR for different β settings (10^{-1},10^{-2},10^{-3}, and 10^{-4}). We observe that the λ_{Opt} curves decrease as the SNR increases. We further notice that larger β values results in smaller λ_{Opt} values.

The false alarm rate and miss detection probability: Using λ_{Opt}, we obtain the false alarm rate and miss detection

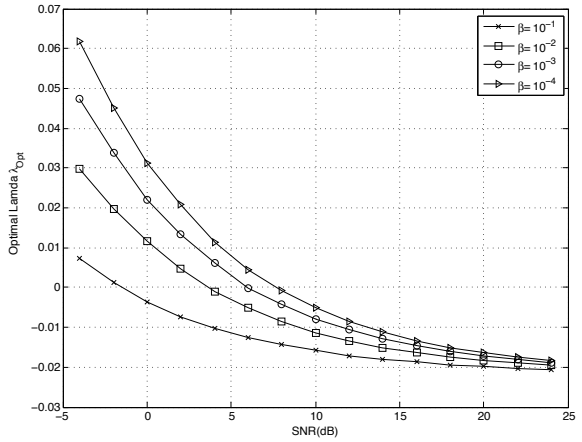

Fig. 7. Optimal threshold λ_{Opt} under different false alarm constraints.

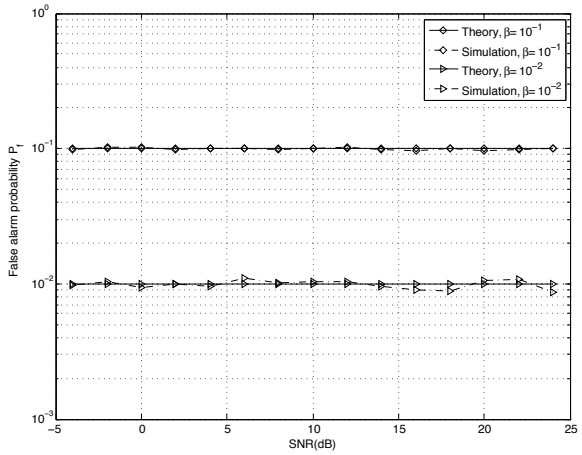

Fig. 8. The probability of false alarm P_f.

probability numerically and compare them with the theoretical results. We use the false alarm constraint $\beta = 10^{-1}$ and $\beta = 10^{-2}$. Fig. 8 shows the false alarm rate calculated both theoretically and by simulation. It can be seen that the theoretical calculations and the numerical simulations are almost identical, and the predefined false alarm constraint β is satisfied. This shows that with the proposed AES-encrypted DTV approach, primary user emulation attacks can be effectively mitigated.

The probability of miss detection is illustrated in Fig. 9. It is clear that the proposed AES-encrypted DTV approach achieves $zero$ miss detection probability even under very low SNR values. As shown in the same figure, the theoretical analysis and simulation results are identical.

From the above discussions, it is concluded that the proposed model can achieve very low false alarm rates and miss detection probabilities. That is, with the proposed AES-encrypted DTV model, primary user emulation attacks can be effectively mitigated, and the primary signal can be detected with very high accuracy. The theoretical calculations presented in Section IV are consistent with the numerical simulations.

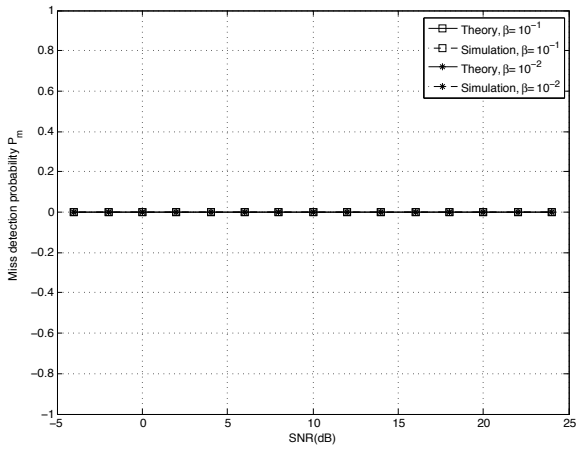

Fig. 9. The probability of miss detection P_m, all curves are identical.

VII. Conclusions

In this paper, a reliable AES-encrypted DTV scheme is proposed for robust primary and secondary system operations under primary user emulation attacks. In the proposed model, an AES-encrypted reference signal is generated at the TV transmitter and used as the sync bytes of each DTV data frame. 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. The proposed approach can effectively mitigate PUEA with no change in hardware or system structure except of a plug-in AES chip, which has been commercialized and widely available. Through both theoretical derivation and simulation examples, it is shown that with the AES-encrypted DTV scheme, the primary user can be detected with high accuracy and low false alarm rate under primary user emulation attacks.

References

[1] Federal Communications Commission, "Spectrum policy task force report," Tech. Rep., Nov. 2002.

[2] M. Thanu, "Detection of primary user emulation attacks in cognitive radio networks," in *International Conference on Collaboration Technologies and Systems (CTS)*, May 2012, pp. 605–608.

[3] R. Chen and J.-M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, Sept. 2006, pp. 110–119.

[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] 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.

[6] Advanced Televsion Systems Committee, "A/53: ATSC digital television standard, part 2," Tech. Rep., Dec. 2011.

[7] V.-H. Pham, J.-Y. Chouinard, A. Semmar, X. Wang, and Y. Wu, "Enhanced ATSC DTV channel estimation," in *Canadian Conference on Electrical and Computer Engineering*, May 2009, pp. 772–776.

[8] N. Singhal and J. Raina, "Comparative analysis of AES and RC4 algorithms for better utilization," in *International Journal of Computer Trends and Technology*, Aug. 2011.

[9] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. Prentice Hall, Jan. 2010.