DEFENSE AGAINST PRIMARY USER EMULATION ATTACKS IN COGNITIVE RADIO NETWORKS USING ADVANCED ENCRYPTION STANDARD

By

Ahmed Salah Alahmadi

A THESIS

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

Electrical Engineering - Master of Science

2014

ABSTRACT

DEFENSE AGAINST PRIMARY USER EMULATION ATTACKS IN COGNITIVE RADIO NETWORKS USING ADVANCED ENCRYPTION STANDARD

By

Ahmed Salah Alahmadi

This thesis 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-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. 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. 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 of 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.

This thesis is dedicated to my great parents and my beloved wife.

ACKNOWLEDGMENTS

I would like to take this opportunity to express my sincere appreciation to my advisor, Dr. Tongtong Li, for her continuous support, help, patience and encouragement throughout my master study. This thesis would not have been possible without her guidance.

I would also like to thank Dr. Jian Ren and Dr. Hassan Khalil from the Department of Electrical and Computer Engineering for serving on my thesis committee. I am deeply grateful to them for their motivation and insightful comments.

Special thanks go to my colleagues in the Broadband Access and Wireless Communication (BAWC) Laboratory. I am particularly indebted to Mai Abdelhakim for her help and invaluable comments and suggestions on the research issues.

Last but not least, I am deeply grateful to my family and friends for their tremendous support and encouragement.

TABLE OF CONTENTS

LIST OF FIGURES . . . . . **viii**

Chapter 1 INTRODUCTION **1**
1.1 Overview 1
1.2 Related Works 2
1.3 Summary of Thesis Contributions 3
1.4 Thesis Organization 4

Chapter 2 THE PROPOSED AES-ASSISTED DTV APPROACH **5**
2.1 A Brief Review of the Terrestrial Digital TV System 5
2.2 AES-Assisted DTV Transmitter 7
2.3 AES-Assisted DTV Receiver 8
2.3.1 Detection of the Primary User 9
2.3.2 Detection of the Malicious User 11
2.3.3 Further Discussions 12
2.4 Summary 14

Chapter 3 ANALYTICAL EVALUATION OF THE PROPOSED AES-ASSISTED DTV APPROACH **15**
3.1 Analytical Evaluation of Primary User Detection 15
3.2 Analytical Evaluation of Malicious User Detection 19
3.2.1 False Alarm Rate and Miss Detection Probability for Malicious User Detection 19
3.2.2 The Optimal Thresholds for Malicious User Detection 26
3.3 Simulation Results 28
3.4 Summary 32

Chapter 4 SECURITY AND FEASIBILITY OF THE PROPOSED AES-ASSISTED DTV APPROACH **33**
4.1 A Brief Overview of the AES Algorithm 33
4.2 Security of the AES-Assisted DTV 35
4.3 Feasibility 37
4.4 Summary 37

Chapter 5 CONCLUSIONS AND FUTURE WORK **39**
5.1 Conclusions 39
5.2 Future Work 40

BIBLIOGRAPHY **41**

LIST OF FIGURES

Figure 1.1 A possible scenario for the attackers to avoid PUEA detection approaches based on the location and/or the energy level of the received signal. For example, MU1 can produce the same DOA and comparable received power level as the primary user, while MU2 can produce comparable received power level as the primary user. 3

Figure 2.1 8-VSB signal frame structure. 6

Figure 2.2 Generation of the reference signal. 7

Figure 3.1 Example 1: The false alarm rate and miss detection probability for primary user detection. 29

Figure 3.2 Example 2: The optimal thresholds for malicious user detection for $\delta = 10^{-3}$. Here, $P_0 = 0.25$. 30

Figure 3.3 Example 3: The overall false alarm rate and the overall miss detection probability for malicious user detection. Here, $P_0 = 0.25$ and $\delta = 10^{-3}$. 31

Figure 4.1 AES encryption. 34

Figure 4.2 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. 36

Figure 4.3 Normalized cross-correlation between the reference signal and noisy versions of the primary user's signal. Here, $\sigma_s^2 = 1$. 36

Chapter 1

INTRODUCTION

1.1 Overview

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.

1.2 Related Works

PUEA have attracted considerable research attention in literature [8–19]. 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. In [9], a nonparametric Bayesian approach, called DECLOAK, was investigated to identify PUEA. The idea of this approach is to use some of the transmitted signal parameters as a fingerprint to identify the actual primary users, and hence the attackers.

Several other methods have been proposed to detect and defend against PUEA. In [10], a transmitter verification scheme (localization-based defense) was proposed to detect PUEA. In [11] and [12], 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 [13]. A similar strategy was used to detect PUEA in fading wireless environments in [14]. In [15], 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 the 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/or the 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/or comparable received power level as that of the actual primary transmitter, as shown in Fig. 1.1 (see the positions of MU1 and MU2).

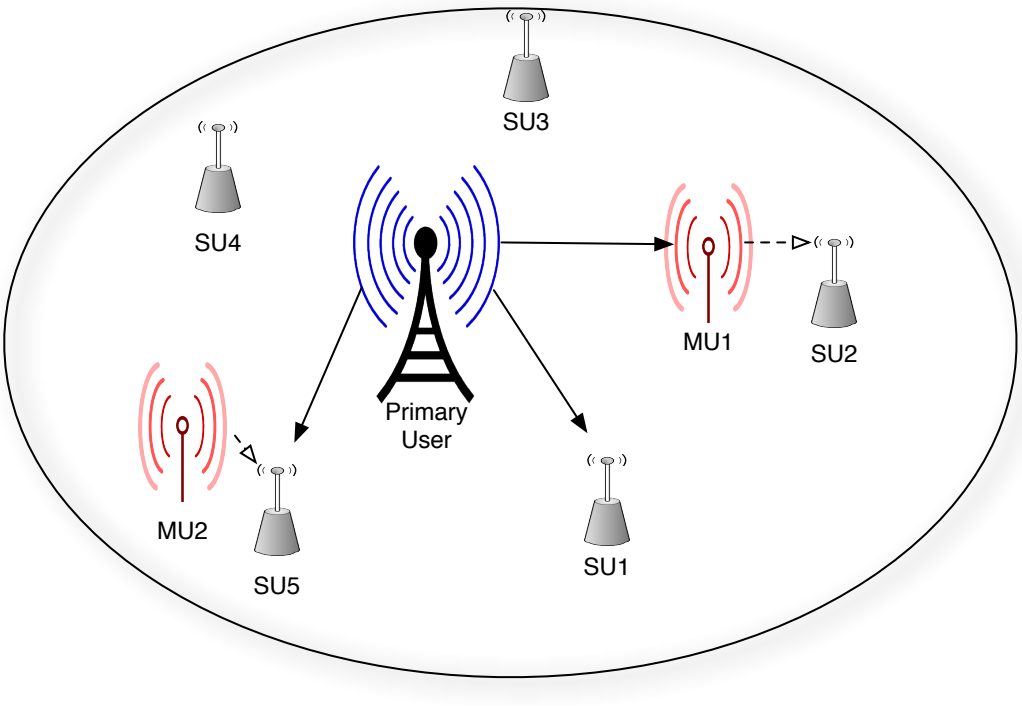


Figure 1.1: A possible scenario for the attackers to avoid PUEA detection approaches based on the location and/or the energy level of the received signal. For example, MU1 can produce the same DOA and comparable received power level as the primary user, while MU2 can produce comparable received power level as the primary user.

1.3 Summary of Thesis Contributions

In this thesis, 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 [20–22]. 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.

1.4 Thesis Organization

The rest of the thesis is structured as follows. In Chapter 2, we present the proposed AES-assisted DTV scheme. Analytical system evaluation and numerical simulations are provided in Chapter 3. Security and feasibility of the proposed scheme are discussed in Chapter 4. Finally, the thesis is concluded and future work is provided in Chapter 5.

Chapter 2

THE PROPOSED AES-ASSISTED DTV APPROACH

In this chapter, we present the proposed AES-assisted DTV scheme for robust and reliable primary and secondary system operations. We first introduce the current terrestrial digital TV system. Then, we discuss the transmitter and the receiver designs of the proposed AES-assisted DTV scheme. Furthermore, we analyze the detection problem of the proposed approach using correlation-based methods. Finally, we discuss some possible concerns with the proposed AES-assisted DTV scheme, and provide some practical solutions.

2.1 A Brief Review of the Terrestrial Digital TV System

Digital Television (DTV) is an innovative technology for enhancing the quality and performance of the analog television broadcasting. Several great benefits can be gained by the adoption of the DTV systems such as better picture and sound quality, less transmission power, and spectrum efficiency, where up to six channels can broadcast simultaneously over the same frequency band that is used by one analog channel [23]. Many countries have switched from the analog TV broadcasting to the digital TV by adopting one of the

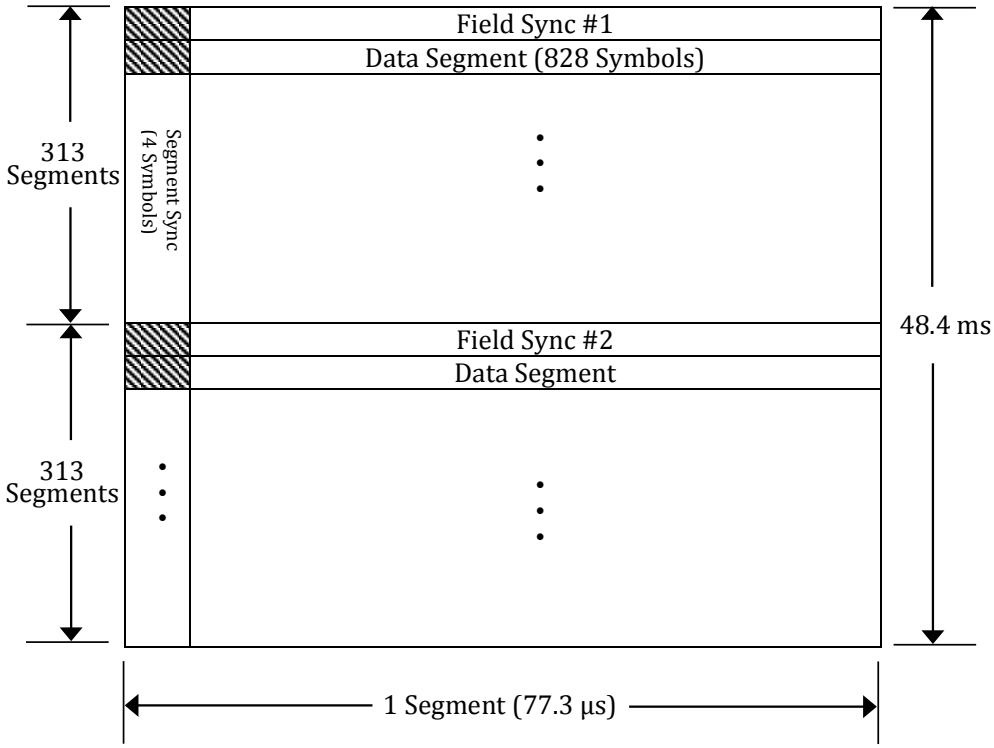


Figure 2.1: 8-VSB signal frame structure.

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 the United States, the Federal Communications Commission (FCC) has adopted the ATSC standard as the official DTV terrestrial broadcasts. In 1996, the U.S. government allowed the TV companies to broadcast digital signals along with the analog broadcasting. By 2009, the FCC has announced that digital TV broadcasting is mandatory in the U.S.

In the ATSC standard, eight-level vestigial sideband (8-VSB) modulation is used for transmitting digital signals after they are partitioned into frames [24]. The frame structure of the 8-VSB signal is illustrated in Fig. 2.1. 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 and channel estimation at the receiver [24], [25]. 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 $626 * 77.3\ \mu s = 48.4\ ms$ [24].

2.2 AES-Assisted DTV Transmitter

The DTV transmitter obtains the reference signal through two steps: first, generating a pseudo-random binary sequence (PRBS), then encrypting the sequence with the AES algorithm. More specifically, a pseudo-random binary sequence is first generated using a *Linear Feedback Shift Register* (LFSR)[1] 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 thesis.

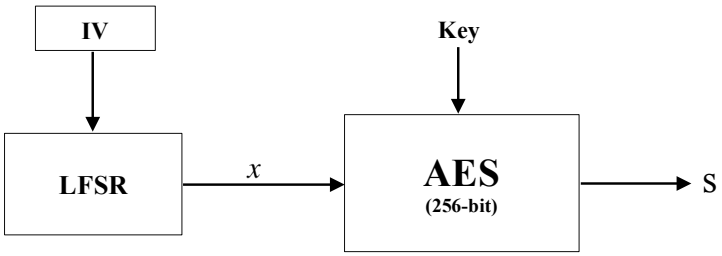


Figure 2.2: Generation of the reference signal.

Once the maximum-length sequence is generated, it is used as an input to the AES encryption algorithm, as illustrated in Fig. 2.2. We propose that a 256-bit secret key be used for the AES encryption so that the maximum possible security is achieved. Security

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

analysis will be provided in Chapter 4.

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

$$\mathbf{s} = E\left(k, x\right), \tag{2.1}$$

where k is the encryption/decryption 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 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. To prevent impersonation attack, the key should be time varying [26].

2.3 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:

$$\mathbf{R_{xy}} =< \mathbf{x}, \mathbf{y} >= \mathbf{E}\{\mathbf{x}\mathbf{y}^*\} \tag{2.2}$$

Under PUEA, the received signal can be modeled as:

$$\mathbf{r} = \alpha\mathbf{s} + \beta\mathbf{m} + \mathbf{n}, \tag{2.3}$$

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.

2.3.1 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.,

$$\begin{aligned} \mathbf{R}_{rs} &= <\mathbf{r}, \mathbf{s}> = \alpha <\mathbf{s}, \mathbf{s}> + \beta <\mathbf{m}, \mathbf{s}> + <\mathbf{n}, \mathbf{s}> \\ &= \alpha\sigma_s^2, \end{aligned} \tag{2.4}$$

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 (2.4), 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:

$$\hat{\mathbf{R}}_{rs} \triangleq \sum_{i=1}^{N} \frac{\mathbf{r}_i \cdot \mathbf{s}_i^*}{N}, \tag{2.5}$$

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:

1. If the cross-correlation is greater than or equal to λ, that is:

$$\hat{\mathbf{R}}_{rs} \geq \lambda, \tag{2.6}$$

   then the receiver concludes that the primary user is present, i.e., $\alpha = 1$.

2. If the cross-correlation is less than λ, that is:

$$\hat{\mathbf{R}}_{rs} < \lambda, \tag{2.7}$$

   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 (2.4), 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.

2.3.2 Detection of the Malicious User

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

$$\begin{aligned}\mathbf{R}_{rr} &= <\mathbf{r}, \mathbf{r}> = \alpha^2 <\mathbf{s}, \mathbf{s}> + \beta^2 <\mathbf{m}, \mathbf{m}> + <\mathbf{n}, \mathbf{n}> \\ &= \alpha^2\sigma_s^2 + \beta^2\sigma_m^2 + \sigma_n^2,\end{aligned} \tag{2.8}$$

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 (2.8). We have the following cases:

$$\mathbf{R}_{rr} = \begin{cases} \sigma_s^2 + \sigma_m^2 + \sigma_n^2, & \alpha = 1,\ \beta = 1 \\ \sigma_s^2 + \sigma_n^2, & \alpha = 1,\ \beta = 0 \\ \sigma_m^2 + \sigma_n^2, & \alpha = 0,\ \beta = 1 \\ \sigma_n^2, & \alpha = 0,\ \beta = 0 \end{cases} \tag{2.9}$$

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

$$\hat{\mathbf{R}}_{rr} \triangleq \sum_{i=1}^{N} \frac{\mathbf{r}_i \cdot \mathbf{r}_i^*}{N}. \tag{2.10}$$

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:

$$\begin{cases} \hat{H}_{00} : \hat{\mathbf{R}}_{rr} < \lambda_0, & \text{given that } \hat{\alpha} = 0, \ (\hat{\beta} = 0) \\ \hat{H}_{01} : \hat{\mathbf{R}}_{rr} \geq \lambda_0, & \text{given that } \hat{\alpha} = 0, \ (\hat{\beta} = 1) \\ \hat{H}_{10} : \hat{\mathbf{R}}_{rr} < \lambda_1, & \text{given that } \hat{\alpha} = 1, \ (\hat{\beta} = 0) \\ \hat{H}_{11} : \hat{\mathbf{R}}_{rr} \geq \lambda_1, & \text{given that } \hat{\alpha} = 1, \ (\hat{\beta} = 1) \end{cases} \tag{2.11}$$

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 Chapter 3.

2.3.3 Further Discussions

The nature of the CR networks operation, which is based on the coexistence of primary users and secondary users, makes it vulnerable to hostile attacks such as PUEA. Several approaches have been proposed to detect PUEA, which can be categorized into two classes: (i) energy level and DOA based approaches [10–15], and (ii) user authentication approaches [16, 17]. In Chapter 2, we revisited some energy level based approaches, and discussed their major limitations. That is, they would fail when a malicious user is at a location where

it produces the same DOA and/or comparable received power level as that of the actual primary transmitter, as shown in Fig. 1.1.

The primary user and secondary user detection approaches proposed in this thesis can effectively overcome this drawback.

Some other user authentication based techniques have also been proposed such as in [16, 17]. In [16], 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 [17], a two-stage primary user authentication method was proposed: (i) generate the authentication tag for the primary user using a one-way hash chain, and (ii) embed the tag in the primary user's signal through constellation shift. Since the authentication tag is superimposed over the primary user transmitted symbols, it introduces some distortions to the primary user signals, and is sensitive to noise. Comparing with the existing user authentication based approaches, our approach is more efficient and has higher detection accuracy.

Although user authentication approaches are generally more reliable under various attack scenarios and generally have no assumptions on the primary user's transmission power or location, they can only be applied to detect the presence of the primary user and the malicious user but not the white spaces in the spectrum.

A more effective and practical solution for this problem would be to combine the proposed approach with the energy level detection approaches. In this case, both the primary user and malicious user, as well as the white spaces, can be accurately identified.

To completely resolve this problem, the primary user needs to use multi-carrier system such as the Orthogonal Frequency Division Multiplexing (OFDM), where each sub-carrier

operates in a particular sub-band in the allocated frequency spectrum. With this, it is possible to detect the primary user and malicious user in each sub-band using the proposed scheme, which we will consider in the future work.

2.4 Summary

In this chapter, we presented the proposed AES-assisted DTV scheme for reliable and efficient CR network operation. First, we revisited the existing terrestrial digital TV System. Then, we discussed the transmitter design, where the primary user generates a pseudo-random AES-encrypted reference signal that is used as the segment sync bits of the DTV data frames. Next, we considered the proposed AES-assisted DTV receiver. At the receiver, the reference signal is regenerated using the secret key for the detection of the primary user and malicious user. Note that the secret key can be obtained from a trusted third party, which serves as an authentication center between the primary users and secondary users. It should also be noted that synchronization is still guaranteed in the proposed scheme since the reference bits are also used for synchronization purposes. We further analyzed the detection problem of the proposed approach using correlation-based methods. Finally, we discussed the major limitation with the proposed AES-assisted DTV scheme, and provided some practical solutions that will be considered in the future work.

Chapter 3

ANALYTICAL EVALUATION OF THE PROPOSED AES-ASSISTED DTV APPROACH

In this chapter, we analyze the detection performance of the the proposed AES-assisted DTV approach through both theoretical analysis and simulation examples. First, we evaluate the system performance for primary user detection. Then, we analyze the effectiveness of the proposed AES-assisted DTV scheme in detecting malicious nodes. Finally, we provide some simulation examples.

3.1 Analytical Evaluation of 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.,

$$P_f = Pr(H_1|H_0). \tag{3.1}$$

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

$$P_m = Pr(H_0|H_1). \tag{3.2}$$

As can be seen from (2.5), $\hat{\mathbf{R}}_{rs}$ 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:

$$\begin{aligned}
\mu_0 &= \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N}(\beta\mathbf{m}_i + \mathbf{n}_i)\mathbf{s}_i^*\right\} \\
&= \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N}(\beta\mathbf{m}_i\mathbf{s}_i^* + \mathbf{n}_i\mathbf{s}_i^*)\right\} \\
&= \frac{1}{N}\left[\sum_{i=1}^{N}(\beta\mathbb{E}\{\mathbf{m}_i\}\mathbb{E}\{\mathbf{s}_i^*\} + \mathbb{E}\{\mathbf{n}_i\}\mathbb{E}\{\mathbf{s}_i^*\})\right] \\
&= 0.
\end{aligned} \tag{3.3}$$

The variance σ_0^2 can be obtained as:

$$\begin{aligned}
\sigma_0^2 &= \mathbb{E}\left\{|\hat{\mathbf{R}}_{rs}|^2\right\} - |\mu_0|^2 \\
&= \frac{1}{N^2}\mathbb{E}\left\{\sum_{i=1}^{N}(\beta\mathbf{m}_i + \mathbf{n}_i)\mathbf{s}_i^* \sum_{j=1}^{N}(\beta\mathbf{m}_j + \mathbf{n}_j)^*\mathbf{s}_j\right\} \\
&= \frac{1}{N^2}\mathbb{E}\left\{\sum_{i=1}^{N}\sum_{j=1}^{N}(\beta^2\mathbf{m}_i\mathbf{m}_j^*\mathbf{s}_j\mathbf{s}_i^* + \mathbf{n}_i\mathbf{n}_j^*\mathbf{s}_j\mathbf{s}_i^*)\right\} \\
&= \frac{1}{N^2}\left[\sum_{i=1}^{N}(\beta^2\mathbb{E}\{|\mathbf{m}_i|^2\}\mathbb{E}\{|\mathbf{s}_i|^2\} + \mathbb{E}\{|\mathbf{n}_i|^2\}\mathbb{E}\{|\mathbf{s}_i|^2\})\right] \\
&= \frac{1}{N}\Big[\beta^2\sigma_s^2\sigma_m^2 + \sigma_s^2\sigma_n^2)\Big]. \qquad (3.4)
\end{aligned}$$

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:

$$\begin{aligned}
\mu_1 &= \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N}(\mathbf{s}_i + \beta\mathbf{m}_i + \mathbf{n}_i)\mathbf{s}_i^*\right\} \\
&= \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N}(\mathbf{s}_i\mathbf{s}_i^* + \beta\mathbf{m}_i\mathbf{s}_i^* + \mathbf{n}_i\mathbf{s}_i^*)\right\} \\
&= \frac{1}{N}\left[\sum_{i=1}^{N}(\mathbb{E}\{|\mathbf{s}_i|^2\} + \beta\mathbb{E}\{\mathbf{m}_i\}\mathbb{E}\{\mathbf{s}_i^*\} + \mathbb{E}\{\mathbf{n}_i\}\mathbb{E}\{\mathbf{s}_i^*\})\right] \\
&= \sigma_s^2, \qquad (3.5)
\end{aligned}$$

and σ_1^2 can be obtained as:

$$\begin{aligned}
\sigma_1^2 &= \mathbb{E}\left\{|\hat{\mathbf{R}}_{rs}|^2\right\} - |\mu_1|^2 \\
&= \frac{1}{N^2}\mathbb{E}\left\{\sum_{i=1}^{N}(\mathbf{s}_i + \beta\mathbf{m}_i + \mathbf{n}_i)\mathbf{s}_i^* \sum_{j=1}^{N}(\mathbf{s}_j + \beta\mathbf{m}_j + \mathbf{n}_j)^*\mathbf{s}_j\right\} - (\sigma_s^2)^2 \\
&= \frac{1}{N^2}\mathbb{E}\left\{\sum_{i=1}^{N}\sum_{j=1}^{N}(\mathbf{s}_i\mathbf{s}_i^*\mathbf{s}_j\mathbf{s}_j^* + \beta^2\mathbf{m}_i\mathbf{m}_j^*\mathbf{s}_j\mathbf{s}_i^* + \mathbf{n}_i\mathbf{n}_j^*\mathbf{s}_j\mathbf{s}_i^*)\right\} - (\sigma_s^2)^2 \\
&= \frac{1}{N^2}\left[\sum_{i=1}^{N}(\mathbb{E}\{|\mathbf{s}_i|^4\} + \beta^2\mathbb{E}\{|\mathbf{m}_i|^2\}\mathbb{E}\{|\mathbf{s}_i|^2\} + \mathbb{E}\{|\mathbf{n}_i|^2\}\mathbb{E}\{|\mathbf{s}_i|^2\})\right. \\
&\quad \left. + \sum_{i=1}^{N}\sum_{\substack{j=1 \\ j\neq i}}^{N}\mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{s}_j|^2\}\right] - (\sigma_s^2)^2 \\
&= \frac{1}{N^2}\left[N(\mathbb{E}\{|\tilde{\mathbf{s}}|^4\} + \beta^2\sigma_m^2\sigma_s^2 + \sigma_n^2\sigma_s^2) + N(N-1)(\sigma_s^2)^2\right] - (\sigma_s^2)^2 \\
&= \frac{1}{N}\left[\mathbb{E}\{|\tilde{\mathbf{s}}|^4\} + \beta^2\sigma_m^2\sigma_s^2 + \sigma_n^2\sigma_s^2 - (\sigma_s^2)^2\right], \qquad (3.6)
\end{aligned}$$

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

Following (3.1), the false alarm rate P_f can be obtained as:

$$\begin{aligned}
P_f &= P_r\{\hat{\mathbf{R}}_{rs} \geq \lambda | H_0\} \\
&= \frac{1}{\sqrt{2\pi}\sigma_0}\int_{\lambda}^{\infty} e^{-\frac{(x-\mu_0)^2}{2\sigma_0^2}}\, dx \\
&= Q(\tfrac{\lambda-\mu_0}{\sigma_0}). \qquad (3.7)
\end{aligned}$$

Similarly, following (3.2), the miss detection probability P_m can be obtained as:

$$\begin{aligned} P_m &= P_r\{\hat{\mathbf{R}}_{rs} < \lambda | H_1\} \\ &= \frac{1}{\sqrt{2\pi}\sigma_1} \int_{-\infty}^{\lambda} e^{-\frac{(x-\mu_1)^2}{2\sigma_1^2}} dx \\ &= 1 - Q(\frac{\lambda-\mu_1}{\sigma_1}). \end{aligned} \tag{3.8}$$

Remark 1 *As will be shown later in this chapter, 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 $\boldsymbol{R}_{rs} = \alpha\sigma_s^2$ (see (2.4)), which is independent of both σ_m^2 and σ_n^2.*

3.2 Analytical Evaluation of Malicious User Detection

In Section 3.1, we discussed the detection performance of the primary user. In this section, we evaluate the false alarm rate and miss detection probability for malicious user detection. Further, we obtain the optimal thresholds that minimize the miss detection probability subject to a constraint on the false alarm rate for malicious user detection.

3.2.1 False Alarm Rate and Miss Detection Probability for Malicious User Detection

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

$$\tilde{P}_{f,0} = Pr(\hat{H}_{01} | \hat{H}_{00}), \tag{3.9}$$

$$\tilde{P}_{f,1} = Pr(\hat{H}_{11}|\hat{H}_{10}). \tag{3.10}$$

The overall false alarm rate is given by:

$$\tilde{P}_f = \hat{P}_0\tilde{P}_{f,0} + (1 - \hat{P}_0)\tilde{P}_{f,1}, \tag{3.11}$$

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

$$\hat{P}_0 = (1 - P_f)P(\alpha = 0) + P_m P(\alpha = 1). \tag{3.12}$$

As will be shown in Chapter 4, 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 later in this chapter. 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:

$$\tilde{P}_f = P_0\tilde{P}_{f,0} + (1 - P_0)\tilde{P}_{f,1}. \tag{3.13}$$

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.,

$$\tilde{P}_{m,0} = Pr(H_{00}|H_{01}). \tag{3.14}$$

$$\tilde{P}_{m,1} = Pr(H_{10}|H_{11}). \tag{3.15}$$

The overall malicious node miss detection probability is defined as:

$$\tilde{P}_m = P_0 \tilde{P}_{m,0} + (1 - P_0)\tilde{P}_{m,1}. \tag{3.16}$$

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:

$$\begin{cases} \hat{\mathbf{R}}_{rr} \sim \mathcal{N}(\mu_{00}, \sigma_{00}^2), & H_{00} \\ \hat{\mathbf{R}}_{rr} \sim \mathcal{N}(\mu_{01}, \sigma_{01}^2), & H_{01} \\ \hat{\mathbf{R}}_{rr} \sim \mathcal{N}(\mu_{10}, \sigma_{10}^2), & H_{10} \\ \hat{\mathbf{R}}_{rr} \sim \mathcal{N}(\mu_{11}, \sigma_{11}^2), & H_{11} \end{cases} \tag{3.17}$$

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:

$$\begin{aligned} \mu_{00} &= \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N} \mathbf{n}_i \mathbf{n}_i^*\right\} \\ &= \frac{1}{N}\sum_{i=1}^{N} \mathbb{E}\{|\mathbf{n}_i|^2\} \\ &= \sigma_n^2, \end{aligned} \tag{3.18}$$

and σ_{00}^2 can be obtained as:

$$\begin{aligned}
\sigma_{00}^2 &= \mathbb{E}\left\{|\hat{\mathbf{R}}_{rr}|^2\right\} - |\mu_{00}|^2 \\
&= \frac{1}{N^2}\mathbb{E}\left\{\sum_{i=1}^{N}\sum_{j=1}^{N}\mathbf{n}_i\mathbf{n}_i^*\mathbf{n}_j^*\mathbf{n}_j\right\} - (\sigma_n^2)^2 \\
&= \frac{1}{N^2}\left[\sum_{i=1}^{N}\mathbb{E}\{|\mathbf{n}_i|^4\} + \sum_{i=1}^{N}\sum_{\substack{j=1\\ j\neq i}}^{N}\mathbb{E}\{|\mathbf{n}_i|^2\}\mathbb{E}\{|\mathbf{n}_j|^2\}\right] - (\sigma_n^2)^2 \\
&= \frac{1}{N^2}\left[N\mathbb{E}\{|\tilde{\mathbf{n}}|^4\} + N(N-1)(\sigma_n^2)^2\right] - (\sigma_n^2)^2 \\
&= \frac{1}{N}\left[\mathbb{E}\{|\tilde{\mathbf{n}}|^4\} - (\sigma_n^2)^2\right], \qquad (3.19)
\end{aligned}$$

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:

$$\begin{aligned}
\mu_{01} &= \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N}(\mathbf{m}_i + \mathbf{n}_i)(\mathbf{m}_i + \mathbf{n}_i)^*\right\} \\
&= \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N}(\mathbf{m}_i\mathbf{m}_i^* + \mathbf{n}_i\mathbf{n}_i^*)\right\} \\
&= \frac{1}{N}\left[\sum_{i=1}^{N}(\mathbb{E}\{|\mathbf{m}_i|^2\} + \mathbb{E}\{|\mathbf{n}_i|^2\})\right] \\
&= \sigma_m^2 + \sigma_n^2. \qquad (3.20)
\end{aligned}$$

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

$$\begin{aligned}
\sigma_{01}^2 &= \mathbb{E}\left\{|\hat{\mathbf{R}}_{rr}|^2\right\} - |\mu_{01}|^2 \\
&= \frac{1}{N^2}\mathbb{E}\left\{\sum_{i=1}^{N}(\mathbf{m}_i+\mathbf{n}_i)(\mathbf{m}_i+\mathbf{n}_i)^*\sum_{j=1}^{N}(\mathbf{m}_j+\mathbf{n}_j)^*(\mathbf{m}_j+\mathbf{n}_j)\right\} - (\sigma_m^2+\sigma_n^2)^2 \\
&= \frac{1}{N^2}\Bigg[\sum_{i=1}^{N}(\mathbb{E}\{|\mathbf{m}_i|^4\}+\mathbb{E}\{|\mathbf{n}_i|^4\}+4\mathbb{E}\{|\mathbf{m}_i|^2\}\mathbb{E}\{|\mathbf{n}_i|^2\}+\mathbb{E}\{2\mathrm{Re}\{(\mathbf{m}_i)^2(\mathbf{n}_i^*)^2\}\}) \\
&\quad + \sum_{i=1}^{N}\sum_{\substack{j=1\\ j\neq i}}^{N}\mathbb{E}\{|\mathbf{m}_i|^2\}\mathbb{E}\{|\mathbf{m}_j|^2\}+\mathbb{E}\{|\mathbf{n}_i|^2\}\mathbb{E}\{|\mathbf{n}_j|^2\}+2\mathbb{E}\{|\mathbf{m}_i|^2\}\mathbb{E}\{|\mathbf{n}_i|^2\}\Bigg] - (\sigma_m^2+\sigma_n^2)^2 \\
&= \frac{1}{N}\Big[\mathbb{E}\{|\tilde{\mathbf{m}}|^4\}+\mathbb{E}\{|\tilde{\mathbf{n}}|^4\}+\mathbb{E}\{2\mathrm{Re}\{(\tilde{\mathbf{m}})^2(\tilde{\mathbf{n}}^*)^2\}\}+2\sigma_m^2\sigma_n^2-(\sigma_m^2)^2-(\sigma_n^2)^2\Big], \qquad (3.21)
\end{aligned}$$

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:

$$\begin{aligned}
\mu_{10} &= \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N}(\mathbf{s}_i+\mathbf{n}_i)(\mathbf{s}_i+\mathbf{n}_i)^*\right\} \\
&= \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N}(\mathbf{s}_i\mathbf{s}_i^*+\mathbf{n}_i\mathbf{n}_i^*)\right\} \\
&= \frac{1}{N}\left[\sum_{i=1}^{N}(\mathbb{E}\{|\mathbf{s}_i|^2\}+\mathbb{E}\{|\mathbf{n}_i|^2\})\right] \\
&= \sigma_s^2+\sigma_n^2, \qquad (3.22)
\end{aligned}$$

and σ_{10}^2 can be obtained as:

$$\begin{aligned}
\sigma_{10}^2 &= \mathbb{E}\left\{|\hat{\mathbf{R}}_{rr}|^2\right\} - |\mu_{10}|^2 \\
&= \frac{1}{N^2}\mathbb{E}\left\{\sum_{i=1}^{N}(\mathbf{s}_i+\mathbf{n}_i)(\mathbf{s}_i+\mathbf{n}_i)^*\sum_{j=1}^{N}(\mathbf{s}_j+\mathbf{n}_j)^*(\mathbf{s}_j+\mathbf{n}_j)\right\} - (\sigma_s^2+\sigma_n^2)^2 \\
&= \frac{1}{N^2}\Bigg[\sum_{i=1}^{N}(\mathbb{E}\{|\mathbf{s}_i|^4\}+\mathbb{E}\{|\mathbf{n}_i|^4\}+4\mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{n}_i|^2\}+\mathbb{E}\{2\mathrm{Re}\{(\mathbf{s}_i)^2(\mathbf{n}_i^*)^2\}\}) \\
&\quad + \sum_{i=1}^{N}\sum_{\substack{j=1\\ j\neq i}}^{N}\mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{s}_j|^2\}+\mathbb{E}\{|\mathbf{n}_i|^2\}\mathbb{E}\{|\mathbf{n}_j|^2\}+2\mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{n}_i|^2\}\Bigg] - (\sigma_s^2+\sigma_n^2)^2 \\
&= \frac{1}{N}\Big[\mathbb{E}\{|\tilde{\mathbf{s}}|^4\}+\mathbb{E}\{|\tilde{\mathbf{n}}|^4\}+\mathbb{E}\{2\mathrm{Re}\{(\tilde{\mathbf{s}})^2(\tilde{\mathbf{n}}^*)^2\}\}+2\sigma_s^2\sigma_n^2-(\sigma_s^2)^2-(\sigma_n^2)^2\Big]. \qquad (3.23)
\end{aligned}$$

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:

$$\begin{aligned}
\mu_{11} &= \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N}(\mathbf{s}_i+\mathbf{m}_i+\mathbf{n}_i)(\mathbf{s}_i+\mathbf{m}_i+\mathbf{n}_i)^*\right\} \\
&= \frac{1}{N}\mathbb{E}\left\{\sum_{i=1}^{N}(\mathbf{s}_i\mathbf{s}_i^*+\mathbf{m}_i\mathbf{m}_i^*+\mathbf{n}_i\mathbf{n}_i^*)\right\} \\
&= \frac{1}{N}\left[\sum_{i=1}^{N}(\mathbb{E}\{|\mathbf{s}_i|^2\}+\mathbb{E}\{|\mathbf{m}_i|^2\}+\mathbb{E}\{|\mathbf{n}_i|^2\})\right] \\
&= \sigma_s^2+\sigma_m^2+\sigma_n^2. \qquad (3.24)
\end{aligned}$$

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

$$\begin{aligned}
\sigma_{11}^2 &= \mathbb{E}\left\{|\hat{\mathbf{R}}_{rr}|^2\right\} - |\mu_{11}|^2 \\
&= \frac{1}{N^2}\Bigg[\sum_{i=1}^{N}(\mathbb{E}\{|\mathbf{s}_i|^4\} + \mathbb{E}\{|\mathbf{m}_i|^4\} + \mathbb{E}\{|\mathbf{n}_i|^4\} + 4\mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{m}_i|^2\} + 4\mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{n}_i|^2\} \\
&\quad + 4\mathbb{E}\{|\mathbf{m}_i|^2\}\mathbb{E}\{|\mathbf{n}_i|^2\} + \mathbb{E}\{2\mathrm{Re}\{(\mathbf{s}_i)^2(\mathbf{m}_i^*)^2\}\} + \mathbb{E}\{2\mathrm{Re}\{(\mathbf{s}_i)^2(\mathbf{n}_i^*)^2\}\} \\
&\quad + \mathbb{E}\{2\mathrm{Re}\{(\mathbf{m}_i)^2(\mathbf{n}_i^*)^2\}\}) + \sum_{i=1}^{N}\sum_{\substack{j=1 \\ j\neq i}}^{N}\mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{s}_j|^2\} + \mathbb{E}\{|\mathbf{m}_i|^2\}\mathbb{E}\{|\mathbf{m}_j|^2\} \\
&\quad + \mathbb{E}\{|\mathbf{n}_i|^2\}\mathbb{E}\{|\mathbf{n}_j|^2\} + \mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{m}_j|^2\} + \mathbb{E}\{|\mathbf{s}_j|^2\}\mathbb{E}\{|\mathbf{m}_i|^2\} + \mathbb{E}\{|\mathbf{s}_i|^2\}\mathbb{E}\{|\mathbf{n}_j|^2\} \\
&\quad + \mathbb{E}\{|\mathbf{s}_j|^2\}\mathbb{E}\{|\mathbf{n}_i|^2\} + \mathbb{E}\{|\mathbf{m}_i|^2\}\mathbb{E}\{|\mathbf{n}_j|^2\} + \mathbb{E}\{|\mathbf{m}_j|^2\}\mathbb{E}\{|\mathbf{n}_i|^2\}\Bigg] - |\mu_{11}|^2 \\
&= \frac{1}{N}\Bigg[\mathbb{E}\{|\tilde{\mathbf{s}}|^4\} + \mathbb{E}\{|\tilde{\mathbf{m}}|^4\} + \mathbb{E}\{|\tilde{\mathbf{n}}|^4\} + \mathbb{E}\{2\mathrm{Re}\{(\tilde{\mathbf{s}})^2(\tilde{\mathbf{m}}^*)^2\}\} + \mathbb{E}\{2\mathrm{Re}\{(\tilde{\mathbf{s}})^2(\tilde{\mathbf{n}}^*)^2\}\} \\
&\quad + \mathbb{E}\{2\mathrm{Re}\{(\tilde{\mathbf{m}})^2(\tilde{\mathbf{n}}^*)^2\}\} + 2\sigma_s^2\sigma_m^2 + 2\sigma_s^2\sigma_n^2 + 2\sigma_m^2\sigma_n^2 - (\sigma_s^2)^2 - (\sigma_m^2)^2 - (\sigma_n^2)^2\Bigg]. \quad (3.25)
\end{aligned}$$

Following the discussions above, we have:

$$\begin{aligned}
\tilde{P}_{f,0} &= P_r\{\hat{\mathbf{R}}_{rr} \geq \lambda_0 | H_{00}\} \\
&= Q(\tfrac{\lambda_0 - \mu_{00}}{\sigma_{00}}), \quad (3.26)
\end{aligned}$$

and

$$\begin{aligned}
\tilde{P}_{f,1} &= P_r\{\hat{\mathbf{R}}_{rr} \geq \lambda_1 | H_{10}\} \\
&= Q(\tfrac{\lambda_1 - \mu_{10}}{\sigma_{10}}). \quad (3.27)
\end{aligned}$$

Similarly, we have:

$$\begin{aligned}\tilde{P}_{m,0} &= P_r\{\hat{\mathbf{R}}_{rr} < \lambda_0 | H_{01}\} \\ &= 1 - Q(\tfrac{\lambda_0 - \mu_{01}}{\sigma_{01}}),\end{aligned} \tag{3.28}$$

and

$$\begin{aligned}\tilde{P}_{m,1} &= P_r\{\hat{\mathbf{R}}_{rr} < \lambda_1 | H_{11}\} \\ &= 1 - Q(\tfrac{\lambda_1 - \mu_{11}}{\sigma_{11}}).\end{aligned} \tag{3.29}$$

The overall false alarm rate $\tilde{P}_f$ and miss detection probability $\tilde{P}_m$ can be calculated following (3.13), (3.16). That is:

$$\tilde{P}_f = P_0 Q(\tfrac{\lambda_0 - \mu_{00}}{\sigma_{00}}) + (1 - P_0) Q(\tfrac{\lambda_1 - \mu_{10}}{\sigma_{10}}), \tag{3.30}$$

and

$$\tilde{P}_m = 1 - P_0 Q(\tfrac{\lambda_0 - \mu_{01}}{\sigma_{01}}) + (P_0 - 1) Q(\tfrac{\lambda_1 - \mu_{11}}{\sigma_{11}}). \tag{3.31}$$

3.2.2 The Optimal Thresholds for Malicious User Detection

In this section, 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:

$$\begin{aligned}&min\ \tilde{P}_m \\ &subject\ to\ \tilde{P}_{f,0} \leq \delta, \quad \text{and} \quad \tilde{P}_{f,1} \leq \delta.\end{aligned} \tag{3.32}$$

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

$$\begin{aligned} &min\ \tilde{P}_{m,0} \\ &subject\ to\ \tilde{P}_{f,0} \leq \delta, \end{aligned} \tag{3.33}$$

and

$$\begin{aligned} &min\ \tilde{P}_{m,1} \\ &subject\ to\ \tilde{P}_{f,1} \leq \delta. \end{aligned} \tag{3.34}$$

Thus, we request:

$$\tilde{P}_{f,0} = Q(\tfrac{\lambda_0 - \mu_{00}}{\sigma_{00}}) \leq \delta, \tag{3.35}$$

and

$$\tilde{P}_{f,1} = Q(\tfrac{\lambda_1 - \mu_{10}}{\sigma_{10}}) \leq \delta, \tag{3.36}$$

which implies that:

$$\lambda_0 \geq \sigma_{00} Q^{-1}(\delta) + \mu_{00}, \tag{3.37}$$

and

$$\lambda_1 \geq \sigma_{10} Q^{-1}(\delta) + \mu_{10}. \tag{3.38}$$

Note that in order to minimize the overall miss detection probability $\tilde{P}_m$, λ_0 in (3.37), and λ_1 in (3.38) should be as small as possible. Hence, we set the thresholds to:

$$\lambda_{0,opt} = \sigma_{00} Q^{-1}(\delta) + \mu_{00}, \tag{3.39}$$

and

$$\lambda_{1,opt} = \sigma_{10} Q^{-1}(\delta) + \mu_{10}. \tag{3.40}$$

By substituting $\lambda_{0,opt}$ and $\lambda_{1,opt}$ in (3.31), we obtain the overall miss detection probability as:

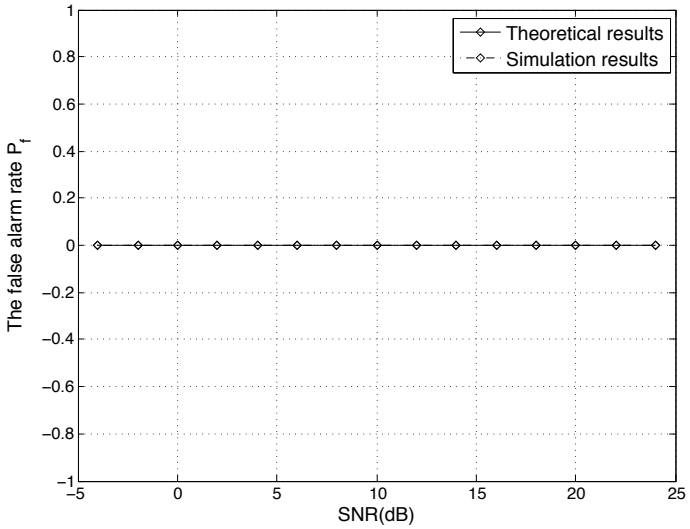
$$\begin{aligned} \tilde{P}_m = 1 - P_0 Q(&\tfrac{\sigma_{00} Q^{-1}(\delta) + \mu_{00} - \mu_{01}}{\sigma_{01}}) \\ &+ (P_0 - 1) Q(\tfrac{\sigma_{10} Q^{-1}(\delta) + \mu_{10} - \mu_{11}}{\sigma_{11}}). \end{aligned} \tag{3.41}$$

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

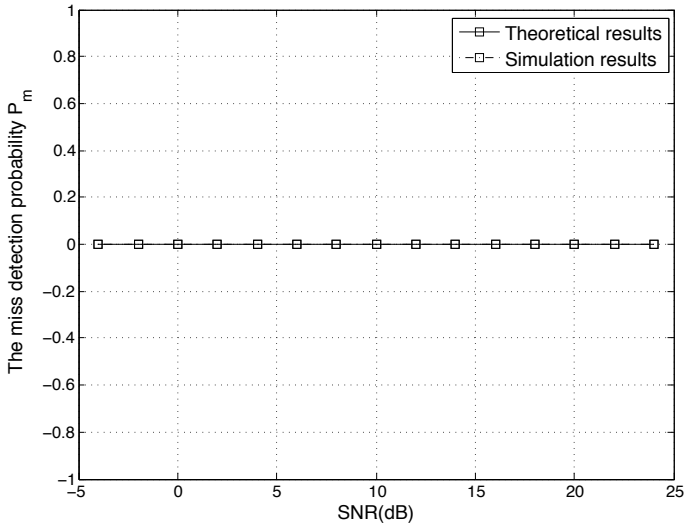
3.3 Simulation Results

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

$\delta = 10^{-3}$.



(a) The false alarm rate P_f, the two curves are identical.



(b) The miss detection probability P_m, the two curves are identical.

Figure 3.1: Example 1: The false alarm rate and miss detection probability for primary user detection.

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. 3.1(a). It is noted that the theoretical false alarm rate P_f in (3.7) depends on β,

since σ_0^2 is a function of β. However, based on (3.4) and the avalanche effect of the AES algorithm, this dependency becomes negligible when N is large. This can be seen from Fig. 3.1(a) as the theoretical calculations match perfectly with the numerical simulations.

The probability of miss detection is shown in Fig. 3.1(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. 3.2 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 (3.39) and (3.40).

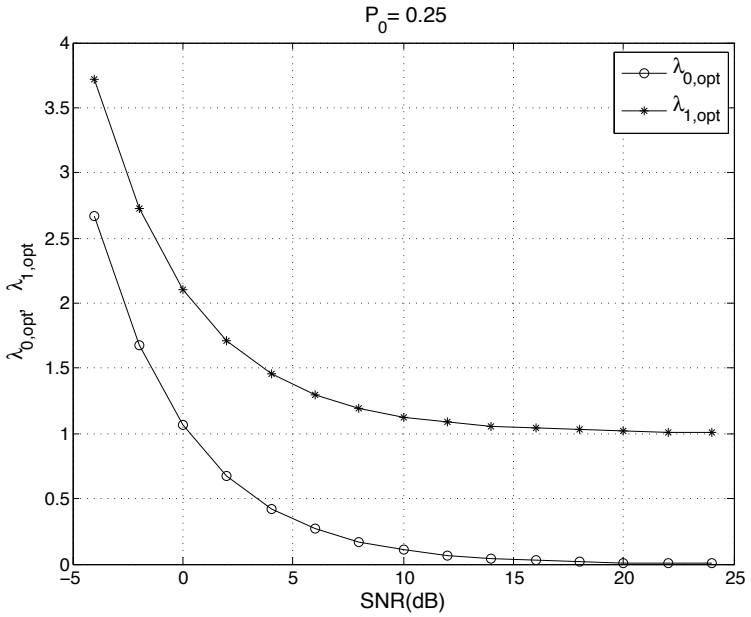
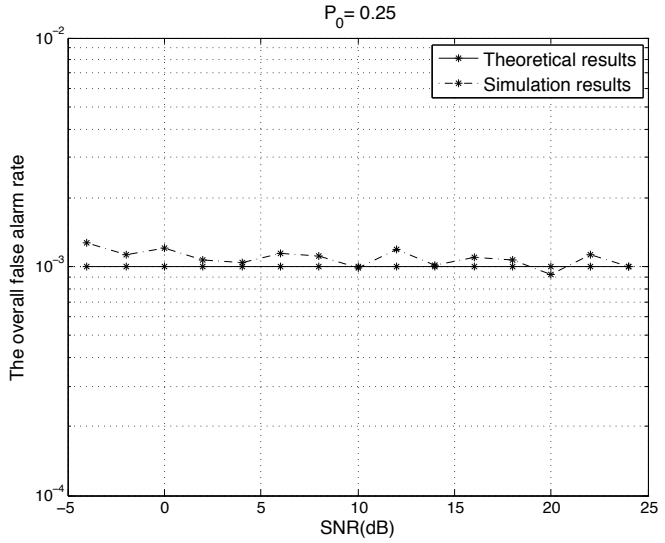
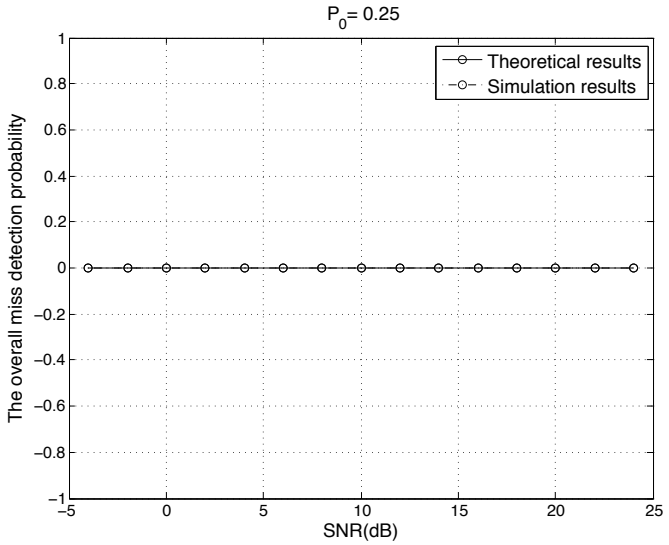


Figure 3.2: Example 2: The optimal thresholds for malicious user detection for $\delta = 10^{-3}$. Here, $P_0 = 0.25$.



(a) The overall false alarm rate $\tilde{P}_f$.



(b) The overall miss detection probability $\tilde{P}_m$, the two curves are identical.

Figure 3.3: Example 3: The overall false alarm rate and the overall miss detection probability for malicious user detection. Here, $P_0 = 0.25$ and $\delta = 10^{-3}$.

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. 3.3(a) shows the overall false alarm rate $\tilde{P}_f$ for $\delta = 10^{-3}$. 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. 3.3(b). It is shown that the proposed approach achieves *zero* overall miss detection probability under a large range of SNR values.

3.4 Summary

In this chapter, we analyzed the detection performance of the the proposed AES-assisted DTV approach through both theoretical analysis and simulation examples. First, we investigated the system performance for primary user detection by obtaining the false alarm rate and the miss detection probability. It was shown that both the false alarm rate and the miss detection probability are essentially zero, and independent of the SNR values. Then, we evaluated the false alarm rate and the miss detection probability for malicious user detection. We further derived two optimal thresholds that minimize the miss detection probability, while keeping the false alarm rate under certain value. From the simulation examples, it was shown that the miss detection probability is essentially zero, and the predefined false alarm constraint is satisfied. It can be concluded that the proposed AES-assisted DTV scheme 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 are consistent with the numerical simulations.

Chapter 4

SECURITY AND FEASIBILITY OF THE PROPOSED AES-ASSISTED DTV APPROACH

This chapter is devoted to discuss the security and feasibility of the proposed AES-assisted DTV scheme. We begin the chapter by providing a general overview of the AES algorithm. We then discuss and investigate the security and practicability of the AES-assisted DTV scheme and provide some numerical results.

4.1 A Brief Overview of the AES Algorithm

Advanced Encryption Standard (AES) is the current National Institute of Standards and Technology (NIST) data encryption standard, it has been adopted by the U.S. Department of Commerce in 2001 after going through a long evaluation period. It has been chosen because of its security (resistance against all known attacks), simplicity, availability in different key sizes, and efficiency in hardware and software implementations [27]. AES is a symmetric-key cipher, in which a *single key* is used for both encryption and decryption. The key is shared between the communication parties, and kept private. Fig. 4.1 shows the general structure

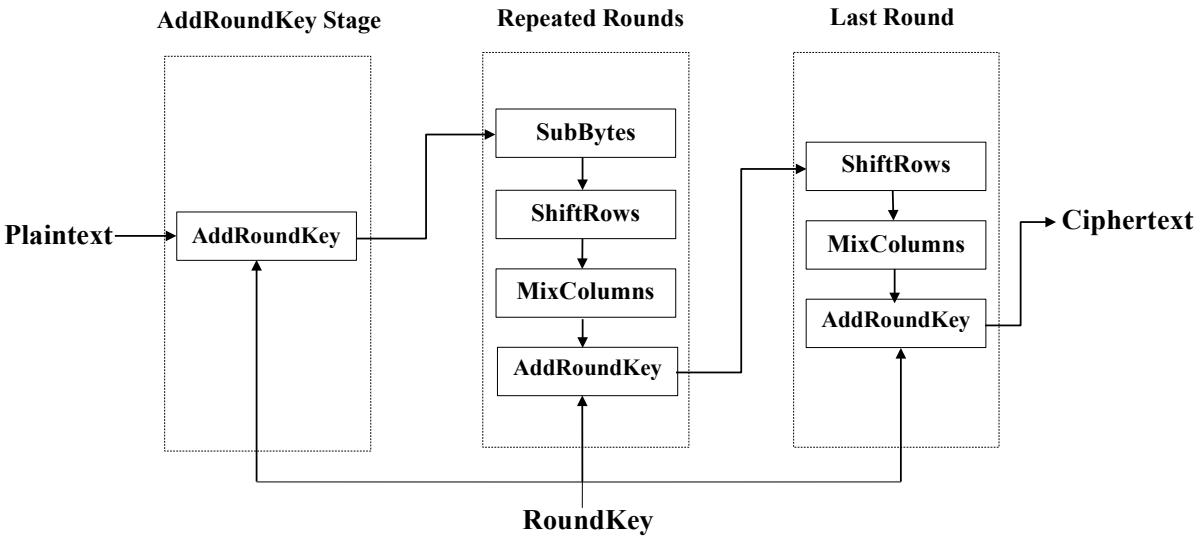


Figure 4.1: AES encryption.

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 repetitions depends on the key length (128, 192, or 256 bits). 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 [26].

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) [26].

3. MixColumns

In this stage, each byte in a column is replaced by a combination of the fours bytes within the same column. The MixColumns operation also provides diffusion property [26].

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 [26].

4.2 Security of the AES-Assisted DTV

As stated earlier, AES has been proven to be secure under all known attacks, 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 [26]. 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. 4.2. It can be seen that the cross-correlation values are around μ_0 in (3.3), 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 (3.5)), under all SNR values, as depicted in Fig. 4.3. It should be appreciated that in the DTV system, the minimum SNR

is 28.3 dB [24].

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

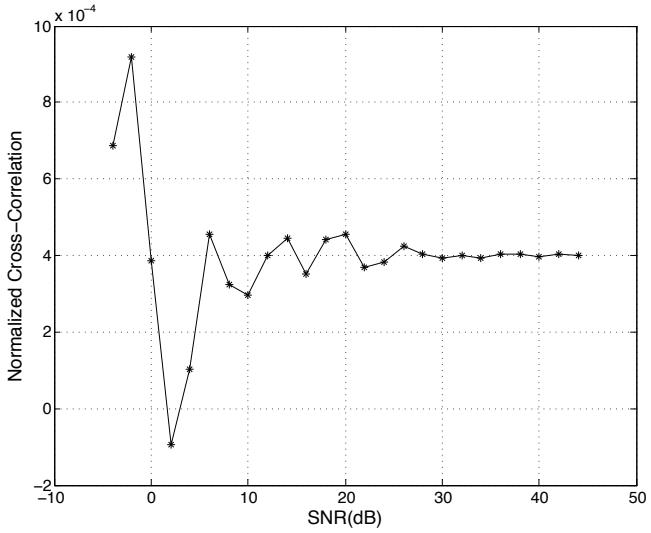


Figure 4.2: Normalized cross-correlation between the reference signal and noisy versions of malicious user's signal. Note that the cross-correlation values are in the order of 10^{-4}, which is close to 0.

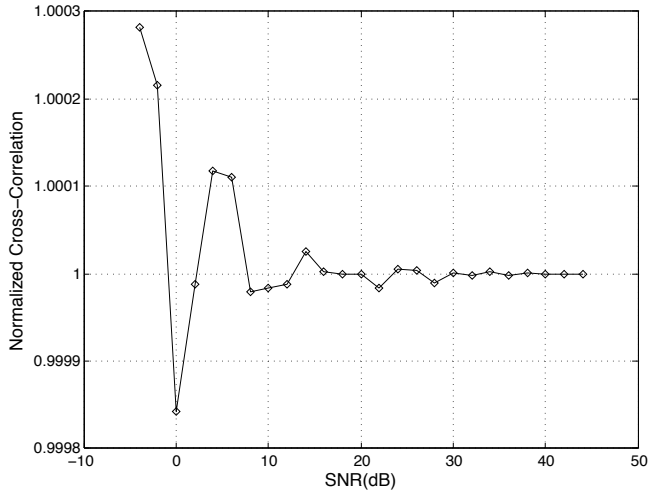


Figure 4.3: Normalized cross-correlation between the reference signal and noisy versions of the primary user's signal. Here, $\sigma_s^2 = 1$.

4.3 Feasibility

In this section, we show that it is practical to generate the required sync bits within the frame time duration shown in Fig. 2.1.

The AES algorithm is one of the block ciphers that can be implemented in different operational modes to generate stream data [28]. High-throughput (3.84 Gbps and higher) AES chips can be found in [21, 22]. In [29], 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.

4.4 Summary

In this chapter, we discussed the security and feasibility of the proposed AES-assisted DTV approach. First, we briefly described the AES algorithm, which is proven to be secure under all known cryptographic attacks. Then, we discussed the security aspects of the proposed AES-assisted DTV scheme. It was shown that the proposed AES-assisted DTV is as secure as the AES algorithm. That is, the AES-assisted DTV scheme is secure under PUEA, as malicious users cannot regenerate the reference signal in real time. Finally, we proved that our proposed AES-assisted DTV approach is practical and can be applied directly to today's

DTV systems under primary user emulation attacks for more robust spectrum sharing.

Chapter 5

CONCLUSIONS AND FUTURE WORK

5.1 Conclusions

In this thesis, 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 DTV systems for more robust spectrum sharing. It would be interesting to explore PUEA detection over each sub-band in multi-carrier DTV systems.

5.2 Future Work

The proposed scheme in this thesis enables the secondary users to accurately identify the primary signal, as well as malicious nodes. Note that due to the large range of DTV channels, the malicious users are unlikely to jam 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 [30–33]. Both CDMA and FH were initially developed for secure military communications. CDMA is particularly efficient under narrow-band jamming [34], 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 [35]. We plan to carry out more research on this by exploiting secure symbol-level coding, which can provide more design flexibility under hostile jamming, especially disguised jamming, where the attacker mimics the characteristics of the authorized primary user signal.

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] Federal Communications Commission, "Spectrum policy task force report," *ET Docket No. 02-135*, November 2002.

[2] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, 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," *Computer Networks*, vol. 50, no. 13, pp. 2127 – 2159, 2006.

[4] 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.

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

[6] Federal Communications Commission, "Unlicensed operation in the TV broadcast bands and additional spectrum for unlicensed devices below 900 MHz and in the 3 GHz band," *ET Docket No. 04-186 and 02-380*, September 2010.

[7] 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.

[8] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE on Symposium*, 2008, pp. 1–6.

[9] N. Nguyen, R. Zheng, and Z. Han, "On identifying primary user emulation attacks in cognitive radio systems using nonparametric Bayesian classification," *IEEE Transactions on Signal Processing*, vol. 60, no. 3, pp. 1432–1445, 2012.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] ——, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 13, no. 2, pp. 74–85, 2009. [Online]. Available: http://doi.acm.org/10.1145/1621076.1621084

[15] 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 Transactions on Wireless Communications*, vol. 10, no. 7, pp. 2135–2141, 2011.

[16] C. Mathur and K. P. Subbalakshmi, "Digital signatures for centralized DSA networks," in *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE*, 2007, pp. 1037–1041.

[17] K. Borle, B. Chen, and W. Du, "A physical layer authentication scheme for countering primary user emulation attack," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2013, pp. 2935–2939.

[18] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 428–445, 2013.

[19] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *2010 IEEE Symposium on Security and Privacy (SP)*, 2010, pp. 286–301.

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

[21] 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.

[22] S.-Y. Lin and C.-T. Huang, "A high-throughput low-power AES cipher for network applications," in *Design Automation Conference,*, 2007, pp. 595–600.

[23] J. Adda and M. Ottaviani, "Digital television 1: The transition to digital television *," September 2004. [Online]. Available: http://idei.fr/doc/conf/ecm/ottaviani.pdf

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

[25] 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.

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

[27] W. Burr, "Selecting the advanced encryption standard," *IEEE Security Privacy*, vol. 1, no. 2, pp. 43–52, Mar 2003.

[28] T. Good and M. Benaissa, "AES as stream cipher on a small FPGA," in *Circuits and Systems, 2006. ISCAS 2006. Proceedings. 2006 IEEE on International Symposium*, 2006, pp. 4 pp.–.

[29] 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.

[30] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping – part i: System design," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 70–79, 2013.

[31] L. Zhang and T. Li, "Anti-jamming message-driven frequency hopping – part ii: Capacity analysis under disguised jamming," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 80–88, 2013.

[32] L. Zhang, J. Ren, and T. Li, "Time-varying jamming modeling and classification," *IEEE Transactions on Signal Processing*, vol. 60, no. 7, pp. 3902–3907, 2012.

[33] L. Lightfoot, L. Zhang, J. Ren, and T. Li, "Secure collision-free frequency hopping for OFDMA-based wireless networks," *EURASIP Journal on Advances in Signal Processing*, vol. 2009, pp. 1:1–1:11, Mar. 2009. [Online]. Available: http://dx.doi.org/10.1155/2009/361063

[34] T. Li, Q. Ling, and J. Ren, "Physical layer built-in security analysis and enhancement algorithms for CDMA systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2007, no. 1, p. 083589, Jul 2007. [Online]. Available: http://jwcn.eurasipjournals.com/content/2007/1/083589

[35] M. Abdelhakim, J. Ren, and T. Li, "Reliable OFDM system design under hostile multi-tone jamming," in *2012 IEEE Global Communications Conference, GLOBECOM'12*, 2012, pp. 4290–4295.