TELKOMNIKA, Vol. 11, No. 10, October 2013, pp. 5917 ~ 5928
ISSN: 2302-4046

Audio Sensing Aid based Wireless Microphone Emulation Attacks Detection

Wang Shan-Shan*, Luo Xing-Guo, Li Bai-Nan
National Digital Switching System Engineering & Technological R&D Center
Jinshui, Zhengzhou, 450001, China, Ph./Fax: +86-03176663266
*Corresponding author, e-mail: beaklee@hotmail.com

Abstract

The wireless microphone network is an important PU network for CRN, but there is no effective technology to solve the problem of microphone evaluation attacks. Therefore, this paper propose ASA algorithm, which utilizes three devices to detect MUs, and they are loudspeaker audio sensor (LAS), environment audio sensor (EAS), and radio frequency fingerprint detector (RFFD). LASs are installed near loudspeakers, which have two main effects: One is to sense loudspeakers' output, and the other is to broadcast warning information to all SUs through the common control channel when detecting valid output. EASs are pocket voice captures provided to SU, and utilized to sense loudspeaker sound at SU's location. Utilizing EASs and energy detections in SU can detect primary user emulation attack (PUEA) fast. But to acquire the information of attacked channels, we need explore RFFDs to analyze the features of PU transmitters. The results show that the proposed algorithm can detect PUEA well.

Keywords*: Cognition Radio Networks (CRN), Spectrum Sensing, Communication Performance, Secondary User, Primary User Emulation Attack (PUEA)*

1. Introduction

Wideband multimedia communication is an important trend for wireless communication in the future. And it is restricted by two main factors, the first of which is that radio spectrum is becoming much more crowded, and the second is that the fixed allocation mechanism for spectrum use is unreasonable and has caused very low spectrum utilization in some areas [1, 2]. CR networks (CRN) take spectrum sensing and dynamical spectrum resource allocation to make secondary users (SUs) using licensed radio spectrum authorized to primary users (PUs) [3, 4]. This new technique can dramatically enhance spectrum efficiency, and has attracted more and more attentions [5, 6].

In CRN, spectrum sensing needs to reliably detect primary signals to find the idle primary bands referred to as spectrum holes. Then the SUs access to these holes. When PU begins to transport data, SU must vacate the corresponding spectrum immediately [7]. This principle can protect PUs from the SUs' interference, and also be advantage to extend the available spectrum scope for SU. However, it may be utilized by some misbehavior secondary users (MUs) to launch denial of service (DoS) attacks, i.e., PUEA [8], [11], [15].

Federal Communication Commission (FCC) has already made the radio TV bands to CRNs, which have nice transmission characters and there are two main users: TV users and wireless microphone users. The PUEA detection manners of sensing the former spectrum have been researched deeply, while the last research has few achievements for its low transmitter power and mobile ability leading to high difficulties. Wireless microphones are widely used in theaters, stadiums, studios, conference halls, classrooms, and exhibition centers; therefore it's very important to ensure the CRNs sensing wireless microphone networks securely in these places. To solve the wireless microphone emulation attacks, we propose a novel PUEA detection algorithm based on audio sensing aid (ASA).

The rest of the paper is organized as follows. Section II presents the system model and the assumptions made to formulate the problem. Performance analysis are formulated and solved in Section III. In Section IV, we provide the simulation results and discussion. Section V presents the conclusion.

Received April 24, 2013; Revised July 6, 2013; Accepted July 18, 2013

2. System Model

The wireless microphone network mainly contains pocket transmitter, signal receiver, mixer, power amplifier, loudspeaker and so on. It's shown in Figure 1 that the voice signal $x(t)$ is transformed to electrical $e(t)$, and then modulated to $s(t)$ and transmitted by transmitter, the received signal $r(t)$ is demodulated ($e'(t)$), and amplified ($x'(t)$). The wireless microphone networks can be divided into two types: frequency modulation (FM) type and amplitude modulation (AM) type. The FM type is used more widely than the AM type for its high frequency bandwidth, large dynamic range, far transmission distance and strong anti-interference capability. Different from TV station, in wireless microphone networks, there are many transmitters, namely PUs, and every transmitter uses one channel, different channel has different frequency. The receiver has a console to control the open states of all channels. When the PU amount is known, the console operator will close extra channels. And signals transmitted in the open channels will be received, demodulated, and enlarged (as Figure 2). The amount of loudspeakers is set according to actual demands, and they are usually fixed at some places. Input of loudspeakers can be single PU signal or many PUs mixed signals. Therefore, only analysis the output of loudspeakers cannot derive the working PU amount.

If MUs launch PUEA by emulate voice signals, they'll be recognized easily, so MUs usually emulate power, frequency, and other characters of the modulated signal $s(t)$, signed by $s_{MU}(t)$. Meanwhile, if MUs transmit in the open channels, signals will be broadcast by loudspeakers or result in noise, which will interfere with PUs, so no matter whether the open channels are used or not by PUs, MUs don't transmit data in them. Determining which channels are open is related to the security of MUs, they can solve the problem by two ways: to avoid all the channels which are detected PU signals in the observation period, or to transmit emulated signals in every channels and monitor the output of loudspeakers, when interference is detected, MUs stop attacking the corresponding channel at once.

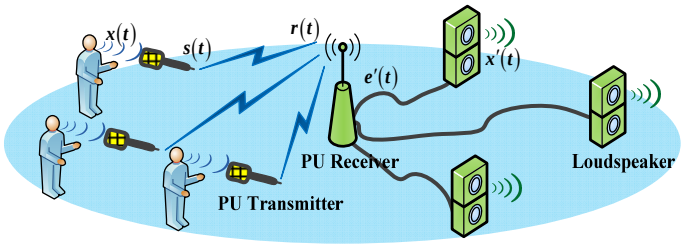

Figure 1. Working Principle of Wireless Microphone

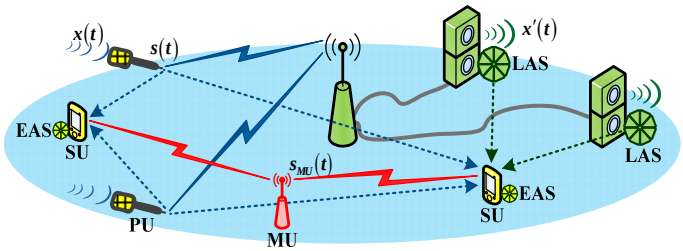

Figure 2. Wireless Microphone Emulation Attacks Detection

3. Algorithm Principle Analysis

In our research, energy detection is selected to sensing available spectrum, which can detect the energy of $x(t)$, $s(t)$, $x'(t)$ and $s_{MU}(t)$, but cannot distinguish these signals' identities. Therefore, some more detection schemes should be used to identify PUEA. We

design three devices to detect MUs, and they are loudspeaker audio sensor (LAS), environment audio sensor (EAS), and radio frequency fingerprint detector (RFFD), which are shown by Figure 2.

3.1. LAS

For most of the loudspeakers locations are fixed, it is feasible to install LAS near them to make long-term detection. This device has two main effects: One is to sense loudspeakers' output, and the other is to broadcast warning information to all SUs through the common control channel when detecting valid output (as Figure 3). In fact, wired microphone can be used as LAS when it has signal processing module and signal transmitting module. The former is to capture the loudspeaker's output voice signal. And the latter is to transmit warning messages, which can be realized by using a resistance and a diode.

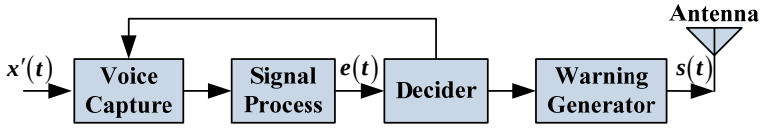

Figure 3. LAS Realization Principle

According to the demands of CRN, LASs can be configured to every loudspeaker or selected loudspeakers which are homogeneously distributed. Multiple LASs can ensure that: (1)the accuracy of voice sensing: specially when LAS has failure or cannot sensing normally caused by the loudspeakers nearby break down, other LASs also can broadcast right warning message; (2)the resistance to shadow effect: several homogeneous distributed LASs are able to ensure all the SUs can receive warning messages even at the with varied topographies or many barriers; (3)the reliability of system: each LAS can be a backup mean for other LASs.

The warning broadcast of multiple LASs has two manners: (1)individual mode: once a LAS sensing the output of loudspeaker, it will broadcast warning message immediately, which causes that there may be more than one warning message; (2)collaborative mode: all the LASs can release warning information in polling way, or one will not warn for some period, when it has received others' warning, which can reduce the crowd degree of the common control channel.

3.2. EAS

This device is a pocket voice capture provided to SU, and can be made by miniature microphone and signal processing module. The miniature microphone is utilized to sensing loudspeaker voice at SU's location. The signal processing module is utilized to analysis voice amplitude information, and compare it with signal energy information of objective channel gathered by energy detector, from which it can be clear whether the channel is attacked by MUs or not. This is because the following research:

The modulated signal $s(t)$ of wireless microphone is [11]

$$s(t)=A_s \cos 2\pi\left[f_s t+k_f \int_{-\infty}^{t} e(\tau)d\tau \right] \quad (1)$$

where A_s is the uniform amplitude of carrier wave, f_s is the frequency of carrier wave, k_f is the frequency offset constant (or namely, the frequency sensitivity of the modulator). The voice wave can be expressed as

$$e(t)=A_e(t)\cos\left[2\pi f_e(t)t\right] \quad (2)$$

in which, $A_e(t)$ is voice wave amplitude, and represents sound volume; $f_e(t)$ is voice wave frequency, and represents pitch. Thus

$$s(t)=A_s \cos\left\{2\pi f_s t+\left[A_e(t)k_f / f_e(t)\right]\sin 2\pi f_e t\right\} \quad (3)$$

Let angular frequency $\omega_s = 2\pi f_s$, $\omega_e(t)=2\pi f_e(t)$, and frequency modulation index $m_f(t)=A_e(t)k_f / f_e(t)$, then

$$s(t) = A_s \cos\left\{\omega_s t + m_f(t)\sin\left[\omega_e(t)t\right]\right\} \quad (4)$$

and Equ. (4) can expressed as

$$s(t)=A_s \operatorname{Re}\left\{e^{j\omega_s t}\cdot e^{jm_f(t)\sin\left[\omega_e(t)t\right]}\right\} \quad (5)$$

where $\operatorname{Re}(\cdot)$ represent get the real part. The Fourier series expansion of $s(t)$ is

$$s(t) = A_s \operatorname{Re}\left\{\sum_{n=-\infty}^{\infty} J_n\left[m_f(t)\right]e^{j\left[\omega_s + n\omega_e(t)t\right]t}\right\} \quad (6)$$

in which $J_n\left[m_f(t)\right]$ is the n-th first type Bessel function of $m_f(t)$ [12]: with the rise of $m_f(t)$, the values of $J_0\left[m_f(t)\right], J_1\left[m_f(t)\right],\ldots$ are more and more similar. So when $m_f(t)$ rises, signal power will transfer to harmonic components, which results in the power of fundamental component to reduce. Therefore, the power of harmonic component, P_{f_s}, is similarly inverse to $m_f(t)$:

$$P_{f_s} \propto 1/m_f(t)= f_e(t)/\left[A_e(t)k_f\right] \propto f_e(t)/A_e(t) \quad (7)$$

as $f_e(t)\in[200,5000]$ Hz, in which the maximum value is 25 times more than the minimum one, and man voice varies among $[20,80]$ dB, in which the maximum value is 1000 times more than the minimum one. That is to say, $A_e(t)$ has a decisive effect in Equ. (7), thus, this equation is similar to

$$P_{f_s} \propto 1/A_e(t) \quad (8)$$

However, MU cannot predict the variousness of $A_e(t)$ when it transmits by emulating $s(t)$. Therefore, the power change is not in inverse proportion to the volume change of fundamental component in emulating signals, which can be exploited to distinguish between MUs and PUs. In the detect procedure, we can record the energy changing data of channel i in band $[f_s-\Delta f, f_s+\Delta f]$ in Δt time, ΔE_d, by SU energy detection module, and obtain the change value of $A_e(t)$ in Δt time, ΔA_e, by EAS module. If

$$\Delta E_d \propto 1/\Delta A_e \quad (9)$$

then it can conclude that the signal is from PU, else from MU.

3.2. RFFD

The radio frequency features such as amplitude, frequency, bandwidth and so on, are significant features inherent for radio signals. In radio systems, the signals contains rich features from the radio devices such as antenna, power amplifier, digital-analog and analog-digital converter are infinitely various, and so on. Because of the diversity of the model types, components performance, production procedure, installation manners, configuration parameters, working environment, and using experience, all the devices are different from

others, so the features contained in the signals can be utilized to disguise transmitters, which is called radio frequency fingerprint (RFF). The RFFD technology has already been researched deeply [13, 14].

In the detection procedure, we shall design different sensing scheme for different detecting object, so that which object to choose is very important. It can be seen that $s(t)$ includes the radio frequency features of many devices. Because of the low power value, and narrow bandwidth of this signal, many features are not distinctive. But the narrow band high frequency power amplifier is a main device affecting the transmitting signals, and generates some new frequency components [15]. The narrow band high frequency power amplifier can be considering as a memoryless non-linear device [16], which is suitable to be depicted by Taylor series [17]. Therefore, we choose narrow band high frequency power amplifiers as the feature extraction object. The detailed analysis is given as follows.

If the input of the narrow band high frequency power amplifier is $v(t)$, then the Taylor series expression of the output signal $s(t)$ is

$$s(t)=\sum_{n=0}^{N} a_n v^n(t), N\to\infty \tag{10}$$

where $n=0$ represents the direct current component, $n=1$ represents fundamental component, and $n\geq 2$ represents the n-th harmonic component; N is the maximum number of the harmonic component, and when $N\to\infty$, the left of Equ. (10) is equal to the right; if n is odd number, $a_n v^n(t)$ generates the odd harmonic components and intermodulation products for $s(t)$, while if n is even number, $a_n v^n(t)$ generates the even harmonic components and direct current component for $s(t)$. The intermodulation components are inside the pass band, while harmonic and direct current components are outside, which can be filtered by filters [18]. Therefore, the items that n is even in the Taylor series can be omitted, and remain the items that n is odd. Thus, Equ. (10) is derived by

$$s(t)=\sum_{n=0}^{\lfloor (N-1)/2\rfloor} a_{2n+1} v^{2n+1}(t) \tag{11}$$

in which $\lfloor\cdot\rfloor$ represents the operation of rounded down.

According to Equ. (4), $v(t)$ can be illustrated by

$$v(t)=A_v\cos\left[\omega_s t+\theta(t)\right] \tag{12}$$

in which, A_v is uniform amplitude of the FM signal $v(t)$; $\theta(t)$ is phase modulation function of $v(t)$, and it can be derived by

$$\theta(t)=m_f(t)\sin\left[\omega_e(t)t\right] \tag{13}$$

Take Equ. (12) into Equ. (11), then

$$\begin{aligned}
s(t)&=\sum_{n=0}^{\lfloor (N-1)/2\rfloor} a_{2n+1} A_v^{2n+1}\cos^{2n+1}\left[\omega_s t+\theta(t)\right]\\
&=\sum_{n=0}^{\lfloor (N-1)/2\rfloor} 2^{-2n} a_{2n+1} A_v^{2n+1}\sum_{i=0}^{n} C_{2n+1}^{i}\cos\left\{(2n-2i+1)\left[\omega_s t+\theta(t)\right]\right\}\\
&=\sum_{n=0}^{\lfloor (N-1)/2\rfloor} 2^{-2n} a_{2n+1} A_v^{2n+1}\sum_{i=0}^{n} C_{2n+1}^{n-i}\cos\left\{(2i+1)\left[\omega_s t+\theta(t)\right]\right\}\\
&=\sum_{n=0}^{\lfloor (N-1)/2\rfloor}\sum_{i=0}^{n} 2^{-2n} a_{2n+1} A_v^{2n+1} C_{2n+1}^{n-i}\cos\left\{(2i+1)\left[\omega_s t+\theta(t)\right]\right\}\\
&=\sum_{i=0}^{\lfloor (N-1)/2\rfloor}\sum_{n=i}^{\lfloor (N-1)/2\rfloor}\left(a_{2n+1} C_{2n+1}^{n-i}\right) 2^{-2n} A_v^{2n+1}\cos\left\{(2i+1)\left[\omega_s t+\theta(t)\right]\right\}
\end{aligned} \tag{14}$$

where, $i=0$ represents fundamental component, and $i\geq 1$ represents $(2i+1)$-th harmonic component.

Because of the short coverage of wireless microphone network, it's reasonable to consider the radio link between SU and PU is ideal, and linear. Therefore, $r_{SU}(t)$ can be derived by

$$r_{SU}(t)=\sum_{i=0}^{\lfloor (N-1)/2\rfloor}\sum_{n=i}^{\lfloor (N-1)/2\rfloor}\left(a_{2n+1}C_{2n+1}^{n-i}\right)\xi_{2i+1}2^{-2n}A_v^{2n+1}\cos\left\{(2i+1)\left[\omega_s t+\theta(t)\right]\right\}+n(t) \quad (15)$$

where, ξ_{2i+1} represents the link gain between fundamental and harmonic component; and $n(t)$ is channel noise. Let

$$\gamma(i,n)=a_{2n+1}C_{2n+1}^{n-i},i=0,1,2,\ldots, \quad (16)$$

$$\theta'(i,n,t)=2^{-2n}A_v^{2n+1}\cos\left\{(2i+1)\left[\omega_s t+\theta(t)\right]\right\},i=0,1,2,... \quad (17)$$

thus

$$r_{SU}(t)=\sum_{i=0}^{\lfloor (N-1)/2\rfloor}\sum_{n=i}^{\lfloor (N-1)/2\rfloor}\theta'(i,n,t)\gamma(i,n)\xi_{2i+1}+n(t) \quad (18)$$

It can be seen that: (1) $\theta'(i,n,t)$ includes all the information about signal resource in the $(2i+1)$-th harmonic component, namely characteristic parameter of signal resource; (2) $\gamma(i,n)$ includes all the information about the narrow band high frequency power amplifier in PU transmitter, namely characteristic parameter of PU transmitter; (3) ξ_{2i+1} represents radio link information, namely link characteristic parameter.

Let's make intermediate frequency sampling to fundamental and harmonic component of $r_{SU}(t)$ synchronously, then the k-th sample point of the $(2i+1)$-th harmonic component, $r_{SU}(i,k)$, is

$$r_{SU}(i,k)=\sum_{n=i}^{\lfloor (N-1)/2\rfloor}\theta'(i,n,k)\gamma(i,n)\xi_{2i+1}+n(i,k),i=0,1,2,...;k=1,2,...,K \quad (19)$$

where $n(i,k)$ is the k-th sample point of noise in the $(2i+1)$-th harmonic component, ω_{mid} is intermediate frequency angular frequency, K is the total amount of sample points. Thus the received sample sequence can be represented by

$$\begin{bmatrix} r_{SU}(i,1)\\ r_{SU}(i,2)\\ \vdots\\ r_{SU}(i,K)\end{bmatrix}=\begin{bmatrix} \theta'(i,i,1) & \theta'(i,i+1,1) & \cdots & \theta'(i,\lfloor (N-1)/2\rfloor,1)\\ \theta'(i,i,2) & \theta'(i,i+1,2) & \cdots & \theta'(i,\lfloor (N-1)/2\rfloor,2)\\ \vdots & \vdots & \ddots & \vdots\\ \theta'(i,i,K) & \theta'(i,i+1,K) & \cdots & \theta'(i,\lfloor (N-1)/2\rfloor,K)\end{bmatrix}\cdot\begin{bmatrix}\gamma(i,i)\\ \gamma(i,i+1)\\ \vdots\\ \gamma(i,\lfloor (N-1)/2\rfloor)\end{bmatrix}\cdot\xi_{2i+1}+\begin{bmatrix} n(i,1)\\ n(i,2)\\ \vdots\\ n(i,K)\end{bmatrix} \quad (20)$$

Let

$$\begin{cases}\mathbf{r}_{SU}(i)=\left[r_{SU}(i,1) \quad r_{SU}(i,2) \quad \cdots \quad r_{SU}(i,K)\right]^{\mathrm{T}} \\ \boldsymbol{\gamma}(i)=\left[\gamma(i,i) \quad \gamma(i,i+1) \quad \cdots \quad \gamma\left(i,\lfloor(N-1)/2\rfloor\right)\right]^{\mathrm{T}}\end{cases} \tag{21}$$

$$\boldsymbol{\theta}'(i)=\begin{bmatrix}\theta'(i,i,1) & \theta'(i,i+1,1) & \cdots & \theta'\left(i,\lfloor(N-1)/2\rfloor,1\right) \\ \theta'(i,i,2) & \theta'(i,i+1,2) & \cdots & \theta'\left(i,\lfloor(N-1)/2\rfloor,2\right) \\ \vdots & \vdots & \vdots & \vdots \\ \theta'(i,i,K) & \theta'(i,i+1,K) & \cdots & \theta'\left(i,\lfloor(N-1)/2\rfloor,K\right)\end{bmatrix} \tag{22}$$

$$\mathbf{n}(i)=\left[n(i,1) \quad n(i,2) \quad \cdots \quad n(i,K)\right]^{\mathrm{T}} \tag{23}$$

then

$$\mathbf{r}_{SU}(i)=\boldsymbol{\theta}'(i)\boldsymbol{\gamma}(i)\xi_{2i+1}+\mathbf{n}(i) \tag{24}$$

According to the least square method, we can obtain that

$$\boldsymbol{\gamma}(i)=\left\{\left[\boldsymbol{\theta}'(i)\right]^{H}\boldsymbol{\theta}'(i)\right\}^{-1}\boldsymbol{\theta}'(i)\mathbf{r}_{SU}(i)\xi_{2i+1}^{-1} \tag{25}$$

In Equ. (25), $\mathbf{r}_{SU}(i)$ is observation sampling value, and it's already known, $\boldsymbol{\gamma}(i)$, $\boldsymbol{\theta}'(i)$, $\mathbf{n}(i)$, ξ_{2i+1} is not known. If the rank of the part on the right of equal sign is more than four, we can estimate the value of $\boldsymbol{\gamma}(i)$. For simply the calculating complexity, make the following simplification: because in the signal processing of the narrow band high frequency power amplifier, the amplification of fundamental component is much more than that of harmonic component, so

$$\gamma(0,0)\square\ \gamma(i,q), i=0,1,2,...; q=1,2,...,\text{and } q>i \tag{26}$$

thus

$$r_{SU}(0,k)\approx\theta'(0,0,k)\gamma(0,0)\xi_1+n(0,k)=A_v\cos\left[\omega_s k+\theta(k)\right]a_1\xi_1+n(0,k) \tag{27}$$

So we can estimate the values of A_v and $\theta(k)$ from $r_{SU}(0,k)$ in the condition of ignoring noise affects:

$$\hat{A}_v=\left|r_{SU}(0,k)\right|\cdot\rho^{-1},\quad \hat{\theta}(k)=\varphi\left[r_{SU}(0,k)\right] \tag{28}$$

where $|\cdot|$ is the operation of calculating the module; $\varphi[\cdot]$ is the operation of calculating the angel of arrival signal; ρ is the coefficient, its value is unknown. And the estimate value of $\rho\boldsymbol{\theta}'(i)$, $\hat{\boldsymbol{\theta}}'_{\rho}(i)$, can be derived from putting Equ. (28) into Equ. (17) and (22) by

$$\hat{\boldsymbol{\theta}}'_{\rho}(i)=\hat{\rho}\cdot\hat{\boldsymbol{\theta}}'(i) \tag{29}$$

The estimate value of $\boldsymbol{\gamma}(i)$, $\hat{\boldsymbol{\gamma}}(i)$, can be obtained by putting Equ. (29) into Equ. (25):

$$\hat{\boldsymbol{\gamma}}(i)=\left\{\left[\hat{\boldsymbol{\theta}}'_{\rho}(i)\right]^{H}\hat{\boldsymbol{\theta}}'_{\rho}(i)\right\}^{-1}\hat{\boldsymbol{\theta}}'_{\rho}(i)\mathbf{r}_{SU}(i)\hat{\rho}\cdot\hat{\xi}_{2i+1}^{-1} \tag{30}$$

in which $\hat{\rho}$ and $\hat{\xi}_{2i+1}$ are the estimate values of ρ and ξ_{2i+1}, respectively, which are both unknown. And let

$$\hat{\boldsymbol{\gamma}}_{\rho,\xi}(i)=\hat{\boldsymbol{\gamma}}(i)\hat{\rho}^{-1}\hat{\xi}_{2i+1}=\left\{\left[\hat{\boldsymbol{\theta}}'_{\rho}(i)\right]^{H}\hat{\boldsymbol{\theta}}'_{\rho}(i)\right\}^{-1}\hat{\boldsymbol{\theta}}'_{\rho}(i)\mathbf{r}_{SU}(i) \tag{31}$$

$\hat{\boldsymbol{\gamma}}_{\rho,\xi}(i)$ contains the features of transmitter ρ, and ξ_{2i+1}, so we need do more work to extract the features of transmitter. $\hat{\gamma}_{\rho,\xi}(i,n)$ in $\hat{\boldsymbol{\gamma}}_{\rho,\xi}(i)$ can be obtained from Equ. (16), (21) and (31) by

$$\hat{\gamma}_{\rho,\xi}(i,n)=\hat{a}_{2n+1}C_{2n+1}^{n-i}\hat{\rho}^{-1}\hat{\xi}_{2i+1} \tag{32}$$

where, $\hat{a}_{2n+1}$ is the estimate value of a_{2n+1}. Take the logarithm of the two sides of Equ. (32) to obtain

$$\ln\hat{a}_{2n+1}=\ln\hat{\gamma}_{\rho,\xi}(i,n)-\ln C_{2n+1}^{n-i}+\ln\hat{\rho}-\ln\hat{\xi}_{2i+1} \tag{33}$$

Considering that the channels are ideal, therefore it can be obtained by ignore the differences among harmonic components that

$$\ln\hat{a}_{2n+1}\approx\ln\hat{\gamma}_{\rho,\xi}(i,n)-\ln C_{2n+1}^{n-i}+\ln\hat{\rho} \tag{34}$$

We can derive that the left part of equal sign only contains feature of the transmitter; and if the harmonic component in the right part of equal sign is collected, then $\ln C_{2n+1}^{n-i}$ is a constant; $\ln\hat{\rho}$ can be eliminated by two equation which have different value of n.
Therefore, the RFF of transmitter, $RFF(i,n)$, can be defined as

$$RFF(i,n)=\ln\hat{\gamma}_{\rho,\xi}(i,n)-\ln\hat{\gamma}_{\rho,\xi}(0,1)-\ln C_{2n+1}^{n-i} \tag{35}$$

i.e., the RFF of transmitter can be determined by comparing the $\hat{\boldsymbol{\gamma}}_{\rho,\xi}(i)$, values of a certain harmonic component and the fundamental component.

4. Algorithm Flow Analysis

The ASA algorithm procedure can be divided into two stages, as illustrated in Figure 4:

Fast Detecting Stage: LASs and SUs are working simultaneously at different places, and each procedure is:

- LAS workflow:

Step 1: LASs make sensing by polling mode, and if they detect voice output of loudspeakers, then execute step2, else execute step3;

Step 2: LASs transmit warning message $b=1$ to all the SUs in CRN through the common control channel;

Step 3: LASs don't send any message, and sense continuously.

- SU workflow:

Step 1: detect the energy of channel $i,(i=1,2,...)$, E_i, then compare it with energy threshold E_{ith}; listen to the warning information in common control channel at the moment, and if the warning amplitude exceed the threshold b_{th}, then conclude that $b=1$, else $b=0$. There may be four cases: *Case1:* if $E_i < E_{ith}$ and $b=0$, then execute step2; *Case2:* if $E_i < E_{ith}$ and $b=1$,

then execute step2; *Case3:* if $E_i \geq E_{ith}$ and $b=0$, then execute step3; *Case4:* if $E_i \geq E_{ith}$ and $b=1$, then execute step4;

Step 2: conclude that channel i is not attacked, and it's idle;

Step 3: conclude that channel i is attacked by MU;

Step 4: conclude that it is not clear that the signal transmitting in channel i is from PU or MU, and shift to the fine detecting stage.

Fine Detecting Stage: the decision of EAS will start RFFS to work, and each procedure is depicted as follows:

- EAS:

Step 1: detect amplitude information of SU's local voice signal, V_e, by EAS, execute step 2;

Step 2: record the energy changing data of channel i in band $[f_s-\Delta f, f_s+\Delta f]$, ΔE_d, by SU energy detection module, execute step3;

Step 3: compare ΔE_d with $1/\Delta V_e$, if they has similar inverse relation, then execute step 4, else execute step5;

Step 4: conclude that channel i is not attacked, and it's used by PU, execute step6~step10, and when the RFF of signal source transmitter is gotten, execute step 11;

Step 5: conclude that CRN is attacked by MU, but to know which channel is attacked, it's need to execute step6~step 10, and when the RFF of signal source transmitter is gotten, execute step 12;

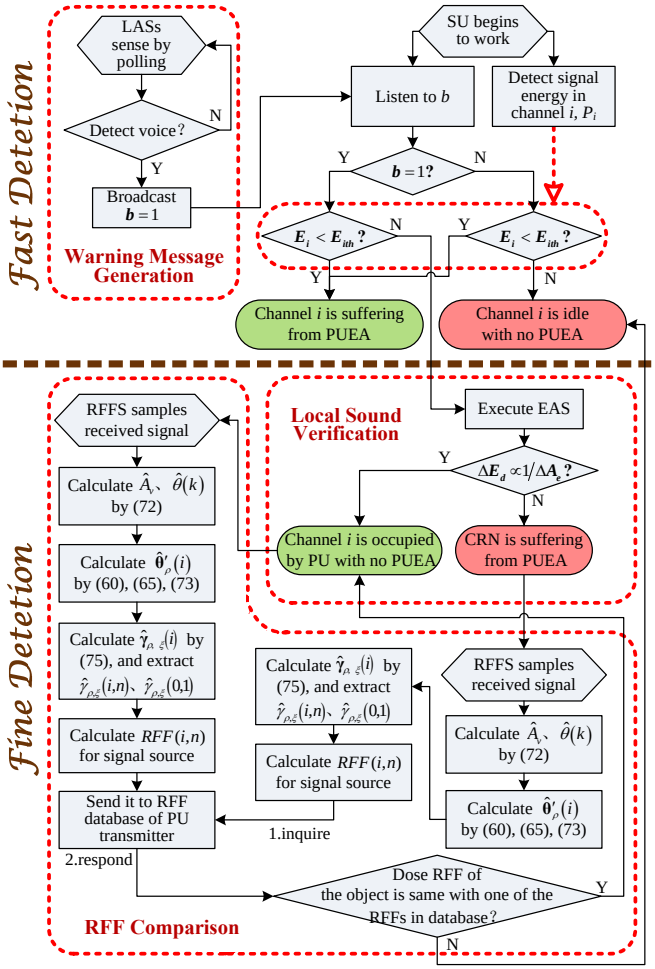

Figure 4. ASA Algorithm Procedure

➢ RFFS:

Step 6: start RFFS, and sample the received signal to obtain $\mathbf{r}_{SU}(i)$, then execute step 7;

Step 7: calculate $\rho\hat{A}_v$ and $\hat{\theta}(k)$ by Equ. (28), execute step 8;

Step 8: calculate $\hat{\boldsymbol{\theta}}'_{\rho}(i)$ by putting $\hat{A}_v$ and $\hat{\theta}(k)$ into Equ. (17), (22) and (29), execute step 9;

Step 9: calculate $\hat{\boldsymbol{\gamma}}_{\rho,\xi}(i)$ by putting $\hat{\boldsymbol{\theta}}'_{\rho}(i)$ and $\mathbf{r}_{SU}(i)$ into Equ. (31), and extract $\hat{\gamma}_{\rho,\xi}(i,n)$ and $\hat{\gamma}_{\rho,\xi}(0,1)$ from it, then execute step 10;

Step 10: calculate $RFF(i,n)$ by Equ. (35);

Step 11: send the result to RFF database of PU transmitter, which can be inquired by SUs;

Step 12: access to the PU RFF database, and detect whether RFF of the object is same with one of the RFFs in PU database. If yes then conclude that channel i is not attacked, and it's used by PU, else conclude that channel i is attacked by MU.

ASA algorithm has been done.

5. Simulation Results

We assume that there is one PU, one SU, and one MU in a rectangular conference hall, which has 130 meters in length, and 42 meters in width. There are a microphone transmitter and a receiver near the short side, and each corner has a loudspeaker. The output power of the transmitter is 15 mW. We utilize wired microphone as a LAS, and mini microphone as a EAS. The goal of the experiment is to detect whether PUEA exists, not to confirm which channel is attacked. First, we test the power of environmental sound and radio signal at places which have different distances from the microphone transmitter, and the results are shown by Figure 5. Sencondly, we simulate the performance of ASA algorithm varying with Δt in different conditions of Δf , and the results are shown by Figure 6.

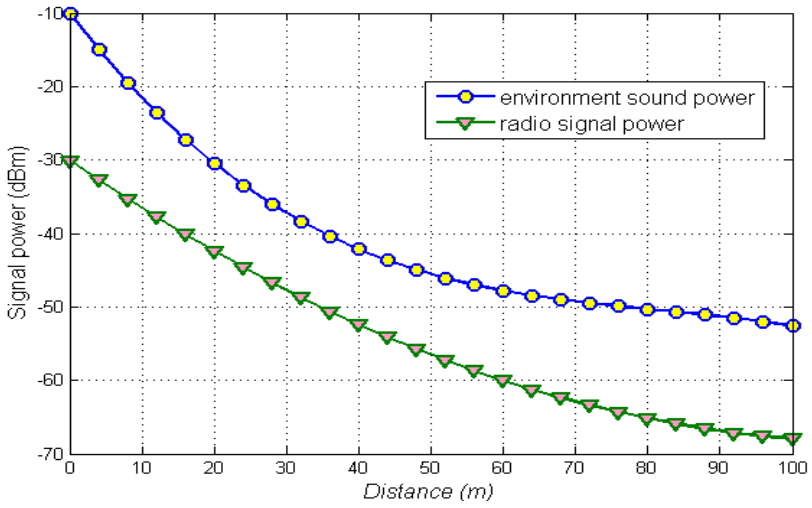

Figure 5. Power of environmental sound and radio signal at places with different distances from microphone transmitter

Figure 5 depicts that the environmental sound power declines slower than radio signal power with the increasing distance, i.e., if SU can detect the radio signal from microphone, the EAS can receives environmental sound.

Figure 6 shows that: (1) in the same bandwidth condition, the performance of ASA algorithm will become better when the detecting time increases. (2) the performance of ASA algorithm will be more better when the detecting bandwidth is narrower. However, the filter capability needs to be raised when bandwidth is narrow, which will cost more. (3) when the

detecting time is more than 20 ms, and the detecting bandwidth is 20 kHz, the PU detecting probability of ASA algorithm can reach 0.85, which illustrates the performance of ASA algorithm is good enough.

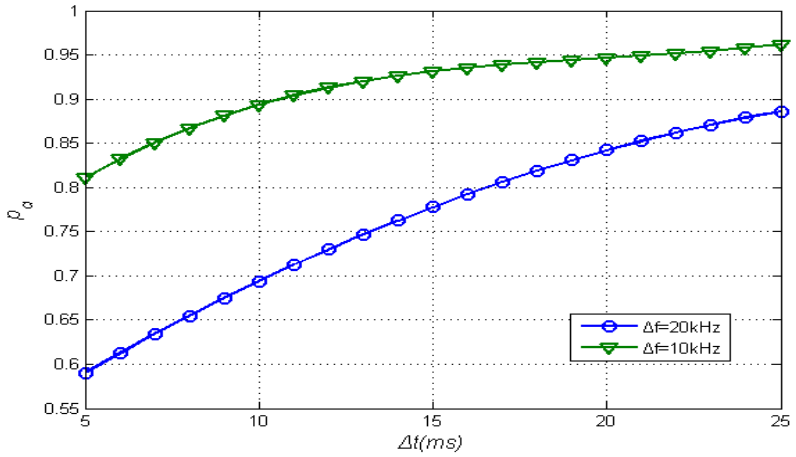

Figure 6. Performance of ASA algorithm varying with Δt in different conditions of Δf

Furthermore, there are three issues need to notice:

(1) to complete the RFF of the PU transmitter need some time, so it's impossible to confirm the exact information of the channel suffering attacking. And when the RFFD contains enough RFFs, the detection becomes better and better. (2) it doesn't need that each SU has a RFFD, but only DFC or center node needs this function. (3) in fact, the amount of microphones isn't large in a meeting place, and the number and position of the microphones are usually fixed, which is convenient to utilize this RFFD scheme.

6. Conclusion

This paper propose ASA algorithm to solve the problem of microphone evaluation attacks. LASs are designed sense loudspeakers' output, and if output is detected then broadcast warning information to all SUs. EASs are designed to sense loudspeaker sound at SU's location. Fast PUEA detection can be realized by LASs, EASs and energy detections in SU. RFFDs are designed to analyze the features of PU transmitters, which can realize fine PUEA detection. The results show that the proposed algorithm can detect PUE attacks well.

Acknowledgements

This paper is sponsored by National High-tech R&D Program of China (No. 2009AA012201) and Shanghai Committee of Science and Technology of China (No. 08dz501600).

References

[1] Claudia Cormio, Kaushik R Chowdhury. *An Adaptive Multiple Rendezvous Control Channel for Cognitive Radio Wireless Ad Hoc Networks*. 8th IEEE International Conference on Pervasive Computing and Communications. Mannheim. 2010: 346-351.

[2] J Mitola, GQ Maguire. Cognitive Radio: Making Software Radios More Personal. *IEEE Personal Communication Magazine*. 1999; 6(4): 13-18.

[3] Federal Communications Commission. *Notice of Proposed Rule Making and Order: Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies.* USA FCC. Report number: 2005; 03-108.

[4] Dengyin Zhang, Kuankuan Li, Li Xiao. An Improved Cognitive Radio Spectrum Sensing Algorithm. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2013; 11(2): 583-590.

[5] S Geirhofer, L Tong, B Sadler. Dynamic Spectrum Access in the Time Domain: Modeling and Exploiting White Space. *IEEE Commun. Magazine.* 2007; 45(5): 66-72.
[6] Nicola Baldo, Alfred Asterjadhi, Lorenza Giupponi. *A Scalable Dynamic Spectrum Access Solution for Large Wireless Networks*. ISWPC 5th IEEE International Symposium on Wireless Pervasive Computing. Modena. 2010: 430-435.
[7] Tevfik Yucek, Huseyin Arslan. A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications. *IEEE Communications Surveys & Tutorials*. 2009; 11(1): 116-130.
[8] Yao Liu, Peng Ning, Huaiyu Dai. *Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures*. IEEE Symposium on Security and Privacy (SP). Oakland. 2010: 286-301.
[9] Geethapriya Thamilarasu, Sumita Mishra, Ramalingam Sridhar. Improving Reliability of Jamming Attack Detection in Ad hoc Networks. *International Journal of Communication Networks and Information Security (IJCNIS)*. 2011; 3(1): 57-66.
[10] Baldini G., Sturman T, Biswas A. Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead. *IEEE Communications Surveys & Tutorials*. 2011: 1-25.
[11] Zhang Xianda, Bao Zheng. Communication Signal Processing. Beijing: National Defense Industry Press. 2000: 100-120.
[12] PENG Geng, HUANG Zhi-tao, JIANG Wen-li, et al. Blind Estimation of Modulation Index for Angle Modulation Signals. *Chinese Journal of Electronics*. 2010; 38(4): 737-741.
[13] Ureten O, Serinken N. Wireless security through RF fingerprinting. Electrical and Computer Engineering. *Canadian Journal of Winter*. 2007; 32(1): 27-33.
[14] Md. Shamim Hossain, Md. Ibrahim Abdullah, Mohammad Alamgir Hossain. Hard Combination Data Fusion for Cooperative Spectrum Sensing in Cognitive Radio. *International Journal of Electrical and Computer Engineering.* 2012; 2(6): 811-818.
[15] Tang Zhi-Ling, Yang Xiao-Niu, Li Jian-Dong. A Novel Method Based on Order Statistics for Extracting Fingerprint of Narrow Band Emitter. *Journal of Electronics and Information Technology.* 2011; 33(5): 1224-1228.
[16] Schreurs D, Odroma M, Goacher AA, Gadringer M. RF Power Amplifier Behavioral Modeling. Cambridge: Cambridge University Press. 2009: 136-140.
[17] Lin Qiang, ZhangZuying, GuoWei. Analysis of Microwave Power Amplifier Nonlinear Distortion. *Journal of Microwaves.* 2004; 20(4): 79-82.
[18] JIN Zhe, SONG Zhi-huan, HE Jia-ming. Modeling and identification of RF power amplifiers based on simplified Vblterra series. *Journal of Circuits and Systems*. 2008; 13(5): 90-94.