# A New Method to Detect Primary User Emulation Attacks in Cognitive Radio Networks

Kai Peng [1], Fanzi Zeng[2], Qingguang Zeng
College of information science and engineering, Hunan University
Changsha, China
[1]e-mail:pengkai873166623@163.com, [2]e-mail:zengfanzi @126.com

***Abstract*—Cognitive radio (CR) can improve the utilization of the spectrum by making use of licensed spectrum in an opportunistic manner. However, the security aspects of cognitive radio networks have garnered little attention. In this paper, we identify a threat to cognitive radio networks, which we call the primary user emulation (PUE) attack. To counter this threat, we proposed a new method to detect the PUE attacks which not only discuss in two kinds of situation which the primary user is stationary or mobile, but also use the Kalman filter algorithm to process the received mobile source's signal strength (RSS) value. And then, we apply with the BP neural network training and testing to complete the detection of PUE attacks. Simulations results show the goodness of the proposed method.**

***Keywords- Cognitive radio; PUE attacks; received signal strength (RSS); Kalman filter algorithm; BP neural network***

## I. INTRODUCTION

Cognitive radio networks (CRNs) [1-2] are regarded as a possible solution to the current underutilization of the spectrum by allowing cognitive radios (CRs) to act as secondary users of the spectrum left unused by licensed services. The specific features of CRNs entail several new threats [3], but one is now standing out from the rest: the primary user emulation (PUE) attack. In this attack an entity pretends to be a primary user or incumbent by transmitting a signal with similar characteristics to a primary signal or replaying a real one, thus preventing secondary users from using a vacant band.

Primary user emulation attacks and defenses have been studied in previous work [4], [5], [6], [7]. All of them proposed to use the location of the primary user to identify the primary user emulation attack. In [4], a transmitter verification scheme called LocDef (localization-based defense) and a non-interactive localization scheme is introduced to detect PUE attacks and pinpoint PUE attackers. In [5], the author provided a cooperative location method to defense PUE attacks, it relies on time difference of arrival (TDoA) measurements and a weighted least squares (WLS) method to estimate the emitter position from such measurements. In [6], the author also proposed a transmitter verification procedure which employs a location verification scheme to distinguish PUE attacks. Another method to identify the PUE attack by positioning the primary user is mentioned in [7], it proposed a mechanism based on physical layer network coding to detect the emulators.

The above method of detecting PUE attacks only use the positioning technology. However, due to the complex CR network environmental impacts and positioning errors, often resulting in the wrong position which will seriously impact on PUE attacks detection. Given this reason, some papers use other methods to detect PUE attacks. In [8], the author proposed a defense strategy the variance detection method which firstly designed an advanced PUE attack. In [9], the author proposed a PUE detection approach that combines energy detection, cyclostationary feature calculation, and artificial neural networks (ANNs). In [10], a scheme which based on radio-frequency (RF) fingerprints is introduced to detect the PUE attacks. However, an excessive number of stations used in this way, it is difficult to ensure the completeness of the radio fingerprint database. In [11], the author provided a primary user authentication mechanism which based on Hash matching technology. But this method requires the primary user base to change the original mode of operation, which is precisely the main user network can not tolerate. In [12], the author put forward a detecting PUE attacks technology that based on Support Vector Data Description (SVDD).

However, all of the mentioned methods to defense the PUE attacks do not consider whether the signal source is static or mobile. In this paper, we proposed a new method to detect the PUE attacks in CRNs which not only classified discussion of these two kinds of situations which the primary user is stationary or mobile, but also use the Kalman filter algorithm to process the received mobile source's signal strength (RSS) value. Finally, we use the BP neural network training to complete the detection of PUE attacks. This method not only makes the PUE attacks detection is more clear and concise, and greatly improves the detection accuracy and stability.

The rest of the paper is organized as follows. In Section II, we introduced the method of static source of PUE attacks detection. In Section III, we described the method of mobile source of PUE attacks detection. In Section IV, we provide the simulation results and discussion. Finally, Section V concludes this paper.

## II. PUE ATTACK DETECTION METHOD WHEN PRIMARY USER IS STATIONARY

With the large scale fading model, the signal strength from primary user received by cognitive users is stability related to the distance between Primary User and cognitive users. Thus, when the primary user is stationary, this

relationship can be used to detect the PUE attack. This paper presents the PUE detection method based on BP neural networks. At first, we collect the samples which associate with the primary user. Then we use these samples for the BP neural network of training and testing. At last, we detect the PUE attacks in the CR network.

### A. The BP neural network for Collecting Samples and Training

At first, according to the need of this paper, we designed the structure of BP neural network [13] as follow:

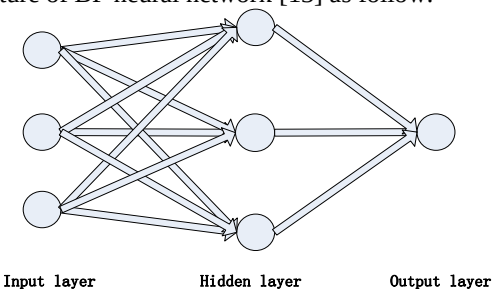


Figure 1. the structure of BP neural network.

Figure 1 shows that the BP neural network has three layers: input layer, hidden layer and output layer. The input layer has three units, the hidden layer also has three units, the output layer only has one unit.

Then, we collected the samples under the situation which the signal source is the primary user. We arranged a measuring point which can measure the signal strength of the primary user in the CR network, and randomly changed the position of measurement point in the network. Finally, we selected N samples from the group of measurement results, and marked as $P^R$. And the two-dimensional coordinates which changed with the measuring point are known, respectively marked as $P^x$ and $P^y$ .So: $P^R = [RSS_1, RSS_2 ... RSS_n]^T$ , $P^x = [x_1, x_2 ... x_n]^T$ , $P^y = [y_1, y_2 ... y_n]^T$. We use as the input of the BP neural network. At this time, since the measured signal is the primary user, we think that corresponds to the expected response of the BP neural network is $T = [1,1...1]^T$ ($T$ is the n-dimensional vector). Because the samples are collected under the situation that the signal is the primary user, and we are lack of the samples under the situation which the signal is PUE attacks signal. Then we will be horizontal and vertical coordinates of all measurement points were taken opposite number, marked as $\hat{P}^x = [-x_1, -x_2 ... -x_n]^T$ , $\hat{P}^y = [-y_1, -y_2 ... -y_n]^T$ .We use $f = \{P^R, \hat{P}^x, \hat{P}^y\}$ as the input of the BP neural network again. Since now the coordinates and the received signal strength is not matching, that can be considered a signal source is PUE attack, we think that corresponds to the expected response of the BP neural network is $\hat{T} = [-1, -1 ... -1]^T$ ( $\hat{T}$ is the n-dimensional vector), so finally the training model of BP neural network is $M$ .Then we record the BP neural network training model's correct rate.

### B. Detect Primary User Emulation Attacks

Similar to the above steps, we use the two dimensional coordinate of each CR node and the received signal strength as the input of BP neural network. The single CR node will get determination results of the signal. If the output of the BP neural network is 1, the CR node identified the signal is the primary user; if the output is -1, the CR node decided signal is the PUE attack. Then each CR node submitted determination results of the respective to a fusion center in CR network, according to the voting rules, the fusion center make the final decision: If the number of determinations that the single CR node identified signal is the primary user are more than the number of decisions which the single CR node identified signal is PUE attack, then eventually decides the signal is actually primary user; otherwise, it ultimately determines the signal is the PUE attack signal.

## III. PUE ATTACK DETECTION METHOD WHEN PRIMARY USER IS MOBILE

When the primary user is moving, the PUE attack detection method is much more complicated. Because the signal node is moving, we measured RSS of signal are also time-varying. Beside we must consider the moving of the signal and the change of the surrounding environment's influence on the RSS measurements, eventually we will be seriously interfered with the stability of the PUE attack signal detection. So we use the Kalman filter algorithm[14] to smooth the received signal strength (RSS) value, it not only reduces the error due to the moving of signal and environmental changes, but also improves the accuracy of detecting the PUE attacks. At first, we use the Kalman filtering for processing the RSS. Then we collect the samples which are used for the BP neural network of training and testing. At last, we detect the PUE attacks in the CR network.

### A. the Kalman filtering Process of RSS

The Kalman filtering process of RSS is simply that: First, the time is divided into k moments, due to the adjacent moment RSS value is relevant, so we according to the RSS at the moment k - 1 to predict the RSS at the moment k, called as the predicted value at the moment k. Then we employed the measured value of RSS at the moment k. Finally, taking into account their respective noise error into account, we will get the Kalman estimate value of RSS at k moment. The predict and update stages for the Kalman filter as follows.

*1) Predict stage for the Kalman filter.*

$$\bar{x^k} = Fx^{k-1} \tag{1}$$

$$\bar{P^k} = FP^{k-1}F^T + Q \tag{2}$$

*2) Update stage for the Kalman filter.*

$$K^{\mathrm{k}} = P^{\bar{k}} H^T \left( H P^{\bar{k}} H^T + R \right)^{-1} \quad (3)$$

$$x^k = x^{\bar{k}} + K^k \left( z^k - H x^{\bar{k}} \right) \quad (4)$$

$$P^k = \left( I - K^k H \right) P^{\bar{k}} \quad (5)$$

In the formula "(1)", $x^{\bar{k}}$ is the predicted result of the last state, $x^{k-1}$ is the optimum result. In the formula "(2)", $P^{\bar{\mathrm{k}}}$ is the corresponding covariance of $x^{\bar{k}}$ , $P^{k-1}$ is the corresponding covariance of $x^{k-1}$ , the formula "(1)" and "(2)" are the prediction of system. Combined with the predicted value and the measured value, we can get the optimal estimate value $x^k$ in formula"(3)" and"(4)". This is what we ultimately want to get the value of $RSS^{\mathrm{k}}$ at the moment k. The formula "(5)" means that in order to make the Kalman filter constantly run down until the end of the process system, we need renew the covariance of $x^k$ at k moment.

### *B. The BP neural network for Collecting Samples and Training*

We need divide the time into k moments when the signal is moving, and collected samples at every moment. The measuring point measured the RSS at k moment, we marked it as $P^{R(\mathrm{k})} = \left[ RSS_1^{\mathrm{k}}, RSS_2^k \ldots RSS_n^k \right]^T$ (k = 0,1,2…k-1). Then combine with the two-dimensional coordinates of the measuring point, we use $f^k = \left\{ P^{R(k)}, P^{\mathrm{x}}, P^y \right\}$ as the input of the BP neural network at k moment. So we will get the expected response of the BP neural network at this moment, marked as $T^{\mathrm{k}} = \left[ 1,1 \ldots 1 \right]^T$ ( $T^k$ is the n-dimensional vector). Same as the stationary signal source, we also take opposite number of horizontal and vertical coordinates of all measurement points, use $f^k = \left\{ P^{R(\mathrm{k})}, \hat{P}^{\mathrm{x}}, \hat{P}^y \right\}$ as the input of the BP neural network again, we will get the expected response of the BP neural network at this moment, marked as $\hat{T}^k = \left[ -1,-1 \ldots -1 \right]^T$ ( $\hat{T}^k$ is the n-dimensional vector). Finally, we get the training model of BP neural network $M^k$ (k = 0,1,2…k-1).

Then, we use the $f^k$ as the test samples input into $M^k$, checking whether the response of the BP neural network in accordance with $T^k$ and $\hat{T}^k$ at the k moment. At last we record the BP neural network training model's correct rate.

### *C. Detect Primary User Emulation Attacks*

Each moment in this period of time, each CR node should submit the judgment result of the mobile signal to the CR network fusion center. Also, every moment the fusion center must make judgment on the signal source, then the fusion center has k decision results: $C^{\mathrm{k}}$ (k = 0,1,2…k-1). In the k decision results, the fusion center also employ the voting rules: if the number of 1 is more than the number of -1, the fusion center final decides mobile signal is the primary user, otherwise, treat it as the PUE attack signal.

## IV. THE SIMULATION AND ANALYSIS

We use MATLAB software to simulate the procedure of detect the PUE attacks. We conduct our simulations under the assumption of a randomly place the primary user and secondary users in a given area (1000m × 1000m). And there is no mutual interference between each user. In this context, we respectively simulated in this two cases: SNR = 10dB or SNR = -10dB.

At first, we simulate the procedure of the BP neural network testing when the primary user is stationary. We record the BP neural network training model's correct rate as follow:

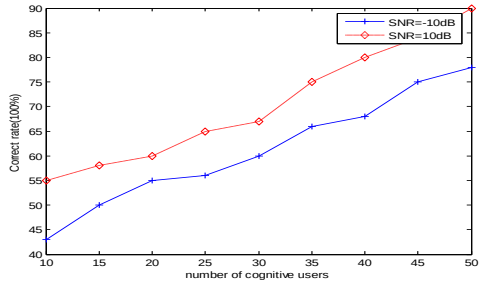


Figure 2. the comparison of BP neural network testing.

As shown in Figure 2, it mans the correct rate of the BP neural network model when the SNR is 10dB or -10dB under the situation of different number of cognitive users. The results show that the correct rate of both the two signal-to-noise ratio will increase when the number of users increases, also we can see signal-to-noise ratio is the greater, the correct rate is higher. From the result, we can see the BP neural network training model can be very useful to make CR nodes identify PUE attack when the primary user is stationary.

Then, we simulate the procedure of the Kalman filter. The procedures of the simulation are as follows:

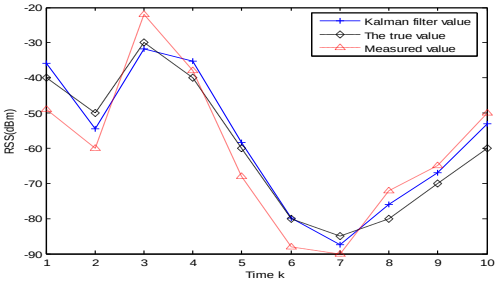


Figure 3. the comparison of three kinds of RSS value.

As shown in Figure 3, single node detects the RSS value which deal with the Kalman filter is closer to the true value

than the measured value. Their error analysis as shown in the figure below:

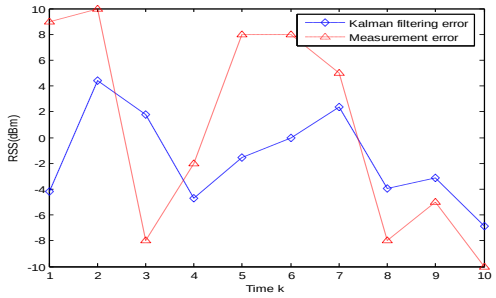


Figure 4. the comparison of error.

Figure 4 shows that the Kalman filtering error significantly is less than the measurement error, so using Kalman filter algorithm to process the RSS value to mobile signal is very necessary. The simulation procedure of the BP neural network testing when the primary user is moving as showed in Figure 5 and Figure 6:

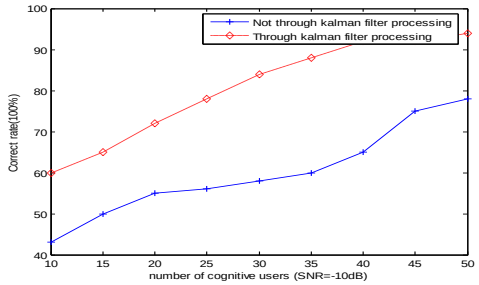


Figure 5. the comparison of BP neural network testing when SNR=-10dB.

As shown in Figure 5, we can see that the correct rate of the BP neural network which use the Kalman filter is higher than correct rate which does not use the Kalman filter when the SNR = -10dB. Also we know that the more cognitive users participate in the training, the correct rate of the BP neural is higher.

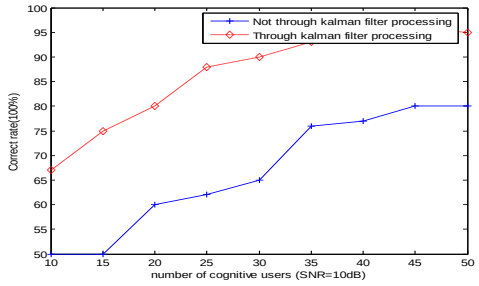


Figure 6. the comparison of BP neural network testing when SNR=10dB.

Figure 6 shows the result of the BP neural network model testing when the SNR = 10dB, it also indicates that the correct rate of the BP neural network which use the Kalman filter is higher than correct rate which does not use the Kalman filter.

Simulation results show that, we mentioned the new method to prevent PUE attacks which not only can reduce the measurement error due to the signal moving, but also can significantly improve the correct rate of the detecting PUE attacks. Therefore, our new method is feasible.

## V. CONCLUSION

Cognitive Radio Network is an effective technology and a hot research direction which can solve the problem of deficient resource and revolutionize utilization. And its safety technology attracts more and more researches. Primary user emulation attacks are typically easy and largely affecting. In this paper, we proposed a new method to detect the PUE attacks in CRNs. Simulations results show the goodness of the proposed method.

## ACKNOWLEDGMENT

This work is supported in part by the National Natural Science Foundation of China under (No.61370096 and 61173012), the Key Project of Natural Science Foundation of Hunan Province under (No. 12JJA005) and technology project of Hunan Province (No.2013GK3023).

## REFERENCES

[1] I.F. Akyildiz, W.-Y. Lee, M.C. Vuran, S. Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey, Computer Networks 50 (13) (2006) 2127–2159.

[2] C. Cordeiro, K. Challapali, D. Birru, N. Sai Shankar, IEEE 802.22: an introduction to the first wireless standard based on cognitive radios, Journal of Communications 1 (1) (2006) 38–47.

[3] O. León, J. Hernández-Serrano, M. Soriano, Securing cognitive radio networks, International Journal of Communication Systems

[4] R. Chen, J.-M. Park, J. Reed. Defense against primary user emulation attacks in cognitive radio networks, IEEE Journal on Selected Areas in Communications 26 (1) (2008) 25–37.

[5] Olga León, Juan Hernández-Serrano, Miguel Soriano. Cooperative detection of primary user emulation attacks in CRNs, Computer Networks 56 (2012) 3374–3384.

[6] Ruiliang Chen, Jung-Min Park. Ensuring trustworthy spectrum sensing in cognitive radio networks 2006.

[7] Xiongwei Xie ,Weichao Wang. Detecting Primary User Emulation Attacks in Cognitive Radio Networks via Physical Layer Network Coding, Procedia Computer Science Volume 21, 2013.

[8] Zesheng Chen, Todor Cooklev, Chao Chen. Modeling Primary User Emulation Attacks and Defenses in Cognitive Radio Networks.

[9] D. Pu, Y. Shi, A. Ilyashenko, A.M. Wyglinski, Detecting primary user emulation attack in cognitive radio networks, in: IEEE Global Telecommunications Conference (GLOBECOM), 2011, pp. 1-5.

[10] WANG Chao, LIU Tao, YANG Zhen, A new method for recognizing the primary user in cognitive radio, Journal of Radio Science (2009)

[11] XUE Nan, ZHOU Xian-wei, XIN Xiao-yu, Scheme for Primary User Emulation in Cognitive Radio Networks, Computer Science 2009.

[12] Fan lei, Zhang Yuntao, Chen Zhenjun. Application of Improved BP Neural Network Based on Matlab [J]. Journal of China West Normal University (Natural Sciences), 2005, 26(1):70-73.

[13] He Qingbi, Zhou Jianli. The convergence and improvements of BP neural network[J]. Journal Of ChongQing Jiao TTong University, 2005,24(1):143-145.

[14] Moriya, N. (2011). Primer to Kalman Filtering: A Physicist Perspective. New York: Nova Science Publishers, Inc. ISBN 978-1-61668-311-5.