Prevention of Emulation Attack in Cognitive Radio Networks Using Integrated Authentication

[1]Mr. Dharmesh Dhabliya, [2]Prof. Ojaswini Ghodkande
[1]R & D, Yashika Publications Wardha India
[2]Professor, Department of Computer Engineering, A.S. Polytechnic Pipri Wardha India
[1]dharmeshdhabliya@gmail.com

Article History

Article Submission
18 August 2016
Revised Submission
30 October 2016
Article Accepted
22 November 2016
Article Published
31st December 2016

Abstract

Security is the prominent problem in emerging cognitive radio. Protecting the chief user's and sub-ordinate user's right to use the spectrum results in the correct cognitive radio operation. The major user emulation attack is a physical layer attack which disrupts the secondary user's operation. An Advanced Encryption Standard scheme is used in this work that aims to defeat the chief User Emulation Attack by the correct detection of the chief user. The reference signal is encrypted and transmitted along with the Digital TV signal. Using a shared secret the receiver regenerates the reference and the cross association and the auto correlation are calculated which helps in the accurate detection of the chief user as well as the malicious user. The simulations were carried out and the results show that the detection scheme results in zero misdetection and also false alarm which is below a set threshold.
Keywords: *Cognitive radio network; Security attacks; chief user emulation attack.*

I. Introduction

Cognitive radio is the promising answer to the ever increasing demand for spectrum. In wake of the spectrum shortage problem Federal Communication Commission (FCC) is considering giving unlicensed users access to the licensed bands through the Cognitive Radio Network (CRN). Here the unlicensed user i.e., secondary users can use the licensed band opportunistically in a way that it does not interfere with the operation of the incumbent user i.e., primary user [1][3].

A white space is a set of frequency bands allotted to a primary user. The concept of cognitive radio allows the inferior user to utilize that particular spectrum hole without causing any disturbance to the primary. Since the CR networks are basically unwired in nature and they face the common wireless network security threats. Due to the inherent nature of the cognitive radio network in addition to these threats they also face threats specific to CRNs. The attacks common in the physical layer are the Primary User Emulation Attack (PUEA) and the Spectrum Sense Data Falsification attacks (SSDF). Beacon Falsification (BF) attack is an attack on the medium access layer [2][4].

II. Related Work

The chief user emulation attack is where the unlicensed malicious user tries to mimic the signals of the primary so as to make the white space(s) unavailable for the secondary. This results in lower spectrum utilization and inefficiency in the cognitive radio operation [5][6]. The FCC mandate states that the defense mechanism proposed should make no changes to the primary user's signal. Except Borle et al [7], all the other papers chosen for the survey have followed the FCC mandate. A study of five previously existing work has been carried out. The mechanisms used in each of the defense method, their advantages and their disadvantages. This method is based on belief propagation and works well for high SNR environments. When malicious user position is able to transmit with same signal power as the primary user then the algorithm does not distinguish between the two [8].

ISSN: 2250-0839

Transmitter verification scheme – location based defense. Location is determined by estimating location and observing signal characteristics. When malicious user position is near the primary user – same direction of arrival- the algorithm does not distinguish between the two. Primary user use primary key for encryption. Secondary users verify the signature. Need for secure certification authority which is not possible in decentralized DSA network. The two stage primary user authentication mechanism Generate authentication tag using one way hash function Embed tag in primary user signal. This method is similar to the digital watermarking [9].

III. PROPOSED PREVENTION OF EMULATION ATTACK SCHEME IN CR NETWORK

In this paper we propose a defense mechanism against the PUEA in the Digital TV system. The 8-level VSB signal has the following frame structure as shown in Fig 1. In this system the segment sync will consist of the AES encrypted reference signal. This reference signal will be the output of the maximal extent sequence produced from a LFSR. The maximal length sequence can be produced by the use of the primitive polynomial. A sequence thus produced will be of length 2m-1 when the degree of the primitive polynomial used is m. After the generation of the maximal length sequence it is fed as the input to the AES algorithm. The AES algorithm used here has the 128-bit key length. The choice of AES encryption is justified as it provides maximum possible security. Various attacks on CR are shown below in figure 1.

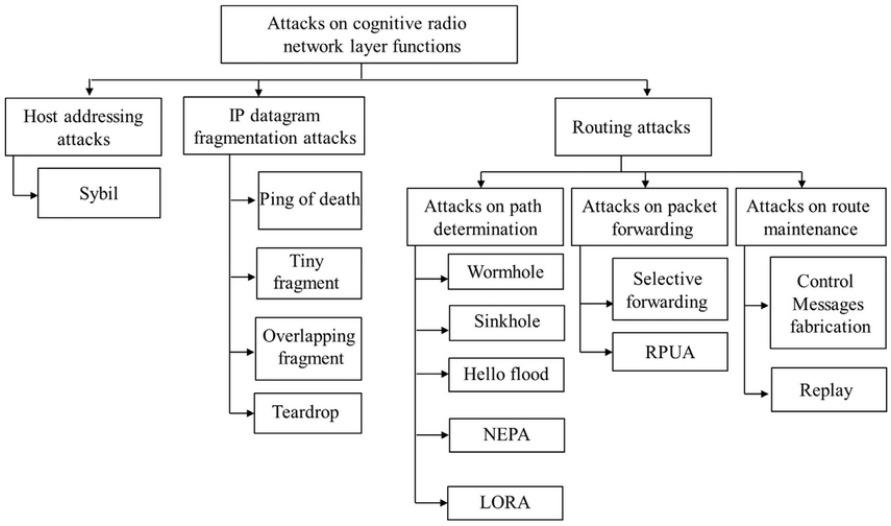

Fig 1: Various CR emulation attacks

A sequence thus produced will be of length 2m-1 when the degree of the primitive polynomial used is m. After the generation of the maximal length sequence it is fed as the input to the AES algorithm. The AES algorithm used here has the 128-bit key length. The choice of AES encryption is justified as it provides maximum possible security. The above procedure is better understood with the help of an equation and a block diagram.

$$x = AES(s, k) \qquad (1)$$

where x denotes the output of the AES encryption scheme which will be used as the sync bits in the 8-level VSB signal, AES(.,.) denotes the 128-bit AES encryption scheme, s denotes the output of the Linear Feedback Shift Register and k is the 128-bit key used for encryption. The efficient implementation of this system shown in Fig 2 depends upon the confidentiality of these two parameters. The receiver will be able to identify the primary transmitter with the regeneration of the sync bits with the help of the above mentioned parameters.

The correlation path used for the identification of the primary user and the malicious user. The reference signal is regenerated by the receiver using the shared secret of the initialization vector and the encryption key. The cross relationship between the regenerated reference signal and the received reference signal is calculated. After

which the autocorrelation of the received reference signal is calculated. This value is compared to the predefined optimal threshold which will identify the presence of the malicious both in the presence as well as the absence of the primary signal. At the receiver the received signal can be modeled as:

$$y = \alpha x + \beta m + n \qquad (2)$$

where x denotes the transmitted primary reference signal, m denotes the malicious signal that is trying to perform PUEA, n denotes the noise component

$$R_{yx} =< y, x >= E\{yx*\}$$

$$= \alpha < x, x > +\beta < m, x > + < n, x >$$

$$= \alpha\sigma_x^2 \qquad (3)$$

where the σ_x^2 represents the power of primary user signal. Since the primary user signal, the malicious user signal and the noise are all uncorrelated to one another the mean value of the signals with one another can be equated to zero. After the calculation of the R_{yx} the value is compared to the predefined threshold. Here two cases can be presented When the cross correlation is below the threshold value

$$R_{yx} < \gamma$$

The receiver uses the predefined thresholds of γ_1 and γ_2 for comparison to the calculated auto- correlation for detection of the malicious user. The choice between γ_1 or γ_2 for the comparison depends of the previously detected presence of primary user($\alpha = 0$ or $\alpha = 1$). The comparison may result in one of the four following results: In the absence of the primary user($\alpha = 0$) , the auto-correlation value is lesser than the threshold

$$R_{yy} < \gamma_1$$

Now the receiver will predict that the malicious user is absent($\beta = 0$). In the absence of the primary user ($\alpha = 0$) , the auto-correlation value is greater than the threshold

$$R_{yy} \geq \gamma_1$$

Now the receiver will predict that the malicious user is present($\beta = 1$). In the presence of the primary user ($\alpha = 1$) , the auto-correlation value is greater than the threshold

$$R_{yy} < \gamma_2$$

Now the receiver will predict that the malicious user is present($\beta = 0$). In the absence of the primary user ($\alpha = 1$) , the auto-correlation value is greater than the threshold

$$R_{yy} \geq \gamma_2$$

IV. SIMULATION RESULTS

The simulations are performed using MATLAB. The parameters used for the performance evaluation include the false alarm rate and the misdetection probability. Here the hypothesis of H_0 and H_1 stand for the absence and the presence of the primary user. The 7 bit initialization vector is used as input to the linear feedback shift register. The usage of the corresponding primitive polynomial will produce the maximal length sequence of length 128. This sequence is encrypted using the 128-bit secret key and the 128 bit output is obtained.

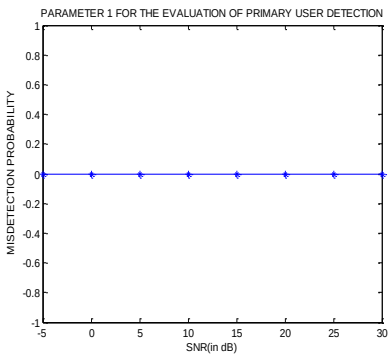

Fig 2: Misdetection probability in primary user detection.

A suitable modulation scheme is set in place. The simulations can be performed for various SNR levels. The auto-correlation and the cross-correlation are calculated for each case and the performance is analyzed using the false alarm rate and the misdetection probability and they are represented graphically. The graph in Fig 2 shows that there has been no misdetection since the values of the cross correlation of the received signal in the presence of the primary user always exceeds the threshold.

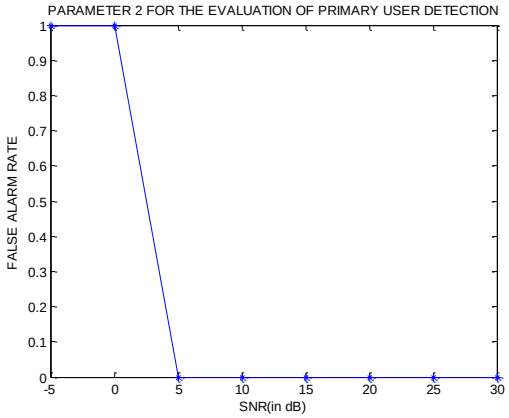

Fig 3: False alarm rate in primary user detection.

As seen from Fig 3 for SNR levels below 5dB the values of the cross correlation in the absence of the primary user are well below the threshold. But the SNR levels of 0dB and -5dB result in false alarm as the noise power exceeds the signal power. The increased noise power pushes the cross correlation above the threshold causing a false alarm. The threshold calculated for the value of δ=10-1 are shown in the table I below

TABLE 1: Optimized Threshold

SNR(dB)	γ_1	γ_2
30	$4.9458*10^{-4}$	0.9996
25	0.0016	1.0047
20	0.0049	1.0087
15	0.0157	1.0226
10	0.0497	1.0502
5	0.1578	1.1733
0	0.4932	1.5222
-5	1.5400	2.6392

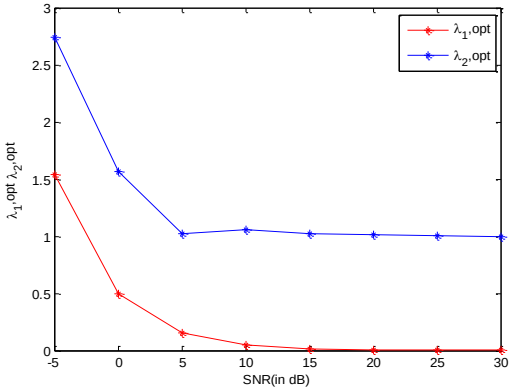

Fig 4: Optimized threshold versus SNR(in dB).

The graph in Fig 4 shows the optimized threshold used in the detection of the malicious user being plotted against the SNR values. The auto-correlation values of the different SNR levels are tabulated below;

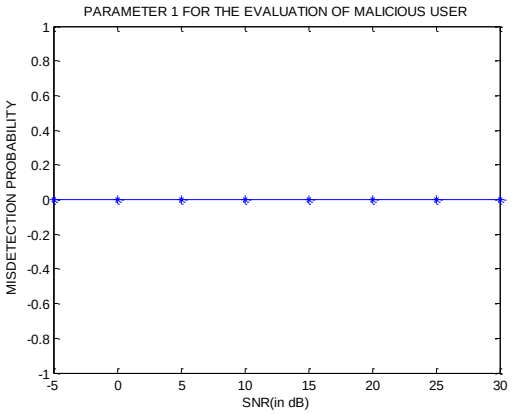

Fig 5: Misdetection probability in malicious user detection.

The graph in Fig 5 shows that there has been no misdetection since the values of the auto association of the received signal in the presence of the malicious user always exceeds the predefined optimized threshold. The graph in Fig 6 shows that the false alarm rate falls around the value of 10-1. This is the minimum false alarm rate that has been set in the calculation of the threshold. Thus the simulation results satisfy the threshold that has been set.

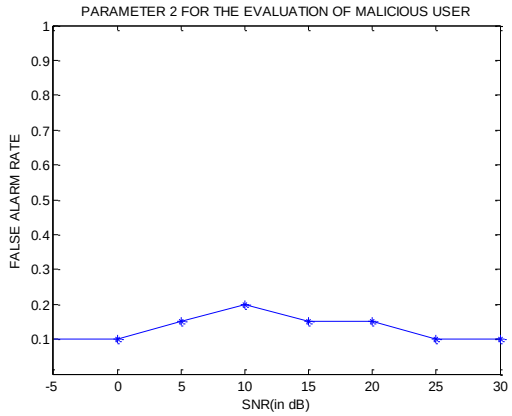

Fig 6: False alarm rate in malicious user detection.

V. CONCLUSION

In this paper a defense mechanism against the PUEA was discussed. An encryption based mechanism that makes use of the AES scheme to have a communal secret between the sender and receiver was presented. The correlation analysis gives us the accurate identification of the primary user. This method also results in low false alarm rate and zero misdetection probability. This method can be further improved by the use of a lightweight encryption scheme instead of the complex AES mechanism.

References

[1] S.Haykin, “Cognitive radio: Brain-empowered wireless communication,” IEEE J. Sel. Areas Commun., vol 23, no 2, pp. 201-220, Feb. 2005.

[2] R. Chen and J.-M. Park, “Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks,” in Proc, IEEE Workshop Netw. Technol. Softw. Defined Radio Netw., pp. 110-119, Sep. 2006.

[3] Z. Yuan, D. Niyato, H. Li, and Z. Han, “Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks,” in Proc. IEEE WCNC, pp. 599–604, Mar. 2011.

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

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

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

[7] R. Chen, J. Park, and J. Reed, “Defense against primary user emulation attacks in cognitive radio networks,” IEEE J. Sel. Areas Commun. ,vol. 26, pp. 25–37, 2008.

[8] Kaiyuan Liu, Y. Chen, Yanghuizi Li and Xingsheng Pang, "A primary user emulation attack with motional users in cognitive radio networks," 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015), Shanghai, 2015, pp. 1-6, doi: 10.1049/cp.2015.0665.

[9] T. N. Le, W. Chin and W. Kao, "Cross-Layer Design for Primary User Emulation Attacks Detection in Mobile Cognitive Radio Networks," in IEEE Communications Letters, vol. 19, no. 5, pp. 799-802, May 2015, doi: 10.1109/LCOMM.2015.2399920.

ISSN: 2250-0839