Defense Against Selfish PUEA in Cognitive Radio Networks Based on Hash Message Authentication Code

Walid Ramadan Ghanem, Mona Shokair, and Moawad I. Dessouky

(Corresponding author: Walid Ramadan Ghanem)

The Department of Electronic and Electrical Communication, Menoufia University, Egypt

(Email: walid.ghanem.eng@ieee.org)

(Received Dec. 11, 2015; revised and accepted Dec. 26, 2015)

Abstract

Cognitive radio network (CRN) is a very astute technology developed to solve the spectrum shortage problem in wireless communication by utilizing the unused bands, where a secondary user (SU) utilizes the free spectrum of the primary user (PU) in an opportunistic manner. The CRN defines the free spectrum sessions using an intelligent and sophisticated process called a spectrum sensing. The spectrum sensing encounters a security problem called primary user emulation attack (PUEA). In this problem, an attacker mimics the PU signal to force the SUs to leave the free band. In this paper, a proposed model based on hash message authentication code (HMAC) is used to detect the PUEA in CRN. HMAC is used to trusting the PU transmission, which is not clarified until now. A shared secret key is used between the SU and the PU to achieve an accurate identification of the PU signal from the attacker. The effectiveness of the proposed approach is analyzed through both theoretical analysis and Simulation. Results show that the proposed method is completely defeated the selfish PUEA and achieves efficient spectrum sharing, moreover, it provides a good detection of the PU when error correcting codes are used.

Keywords: Cognitive radio network (CRN), hash message authentication code (HMAC), physical layer authentication, primary user emulation Attack (PUEA)

1 Introduction

Cognitive radio (CR) has attracted a strong attention recently to solve the spectrum shortage problem [19]. Spectrum scarcity becomes a serious challenge to the emerging wireless technologies. In licensed networks, the primary users operate in their allocated licensed bands. It is recognized that the licensed bands are generally underutilized and their occupation fluctuates temporary and geographically in the range of 15-85%. In a typical Cognitive Radio (CR) system, the PU is the spectrum license holder and the SU is an unlicensed user who intends to use the spectrum opportunistically. CR is based on Dynamic Spectrum Access (DSA), where the Priority is given to the PU in the sense that SU can only transmit, if its transmission is deemed to be a harmless to the PU. The SU is not allowed to transmit when the PU is transmitting [1] . Unused bands (White spaces) are identified through spectrum sensing process [24], then they are used by the SUs for data transmission, the spectrum sensing process is continuously performed to determine the white spaces, if the primary user is detected, then the SU must vacate the band for him. The CR networks are exposed to many attacks one of these attacks is called PUEA. The PUEA is considered as a physical layer attack, where a selfish user (attacker) mimics the PU signal to confuse the SUs to leave the band for him. This leads to low spectrum utilization in CRN.

PUEA has been studied in many researches. R. Chen proposed to use the location of the primary user to identify the PUEA in [9] . S. Annand made an analytical model based on Fenton's approximation and Markov inequality in [4]. Z. Jin et al. Presented a NeymanPearson composite hypothesis test in [15]. and a Wald's sequential probability ratio test to detect the PUEA was described in [16]. Z. Chen showed how the attacker can emulate the PU signal to confuse the SU and used an advanced strategy called variance detection to mitigate the effect of an attacker using the difference between the communication channel of PUEA and PU in [10]. C. Chen et al made a joint position verification method to enhance the positioning accuracy in [14] . Cooperative Spectrum Sensing in CRN in the Presence of the PUEA is proposed in [8] . Feign Bao et al studied the PUEA with national secondary users in CRN and using a hybrid method based on Energy Detection (ED) and Variance Detection in [5] . Kapil M. Borle has developed a physical layer authentication scheme for wireless communication in [7]. Advanced encryption standard was used to mitigate PUEA in [2]. More researches discussed this problem will be found in [3, 6, 12, 13, 21, 22].

In this paper, a proposed Physical layer authentication based on hash message authentication code (HMAC) is used to detect the PUEA in cognitive radio networks which is not clarified until now. Moreover, different coding techniques will be applied. The HMAC is used to generate a tag at the transmitter, this tag is appended to the message and sent over the channel. At the receiver the secondary user separates the message and tag and regenerates a new tag from the shared key and the received message. By comparing the two tags, the SU determines if the signal comes from the PU or from the attacker. The proposed method provide a good detection of the PU and it is completely defeated the PUEA under any condition and ables a high spectrum usage and high efficiency. The performance of the system is measured using the probability of false alarm and probability of detection.

The rest of this paper is organized as follows In Section 2, the problem formulation will be explained. In Section 3, the system model of the system is introduced. In Section 4 the performance metrics will be presented. In Section 5, the analytical Model Evolution will be explained. In Section 6 numerical and simulation results will be included. Finally conclusions will be drawn in Section 7

2 Problem Formulation

The PUEA is considered one of the main threats in CRNs. In this problem, an attacker emulates the PU signal to confuse the SU to leave the free spectrum session as shown in Figure 1. The attacker receives the signal from the primary user and emulates it and retransmits the signal again to the SUs. The SUs suppose that the transmission comes from the PU and therefore, they leave the free spectrum. The PUEA destroys the spectrum sensing process. In Figure 1, there are three users as follow:

- **Primary User**: A user who has higher priority or legacy rights for the usage of a specific part of the Spectrum.
- **Secondary User**: A user who has a lower priority and therefore exploits the spectrum in such a way that it does not cause any interference to PUs.
- **Selfish PUEA**: the aim of this attacker is to maximize the spectrum usage for himself, by taking the free band and preventing the others SUs from using it.

This attacker can mimic the primary user power, modulation, signal characteristics and any characteristics of the PU signal. Thus the detection of the attacker becomes extremely difficult. The authentication is a proper method to solve this problem. By authenticating the transmission between the PU and the SU, this problem will be solved easily.

3 System Model

In this section, the system model will be described, then the block diagram of the proposed system, which includes the attackers will be explained. Finally the flow chart of the system will be done as shown in figure 2. The PU message runs into the HMAC algorithm to produce the first HMAC (TAG A) [23], then this tag is padded with the message using TDMA, both of them are encoded, modulated and transmitted to the SUs as shown in figure .2. The SU intern runs the message portion of the transmission through the HMAC algorithm using the same key that was used by the PU, producing a second HMAC (TAG B), The SU compares the two tags. If they are identical the transmission is assumed to be from the PU and the SU must stop its transmission, otherwise a PUEA is in progress. The attacker don not have the same key used by the PU and assumed to be not intelligent enough to extract the key, therefore, he cannot authenticate his transmission. If the attacker uses another key, the SU defines him correctly.

In Figure 3, the flow chart of the proposed model is described as follows, first, a random data represents the PU message is generated, this data is applied to the HMAC function to generate the TAG A. The TAG A and the message are added together using TDMA, then the message is encoded, modulated and transmitted on the channel. The SU receives the data demodulates and decodes it. Then SU separates the TAG from the message, and applies the message part to HMAC to produces a second tag (TAG B). And compares the two tags, if the two tags are identical, then the data is considered from the PU, otherwise, the attacker is in progress and the SU must punish him.

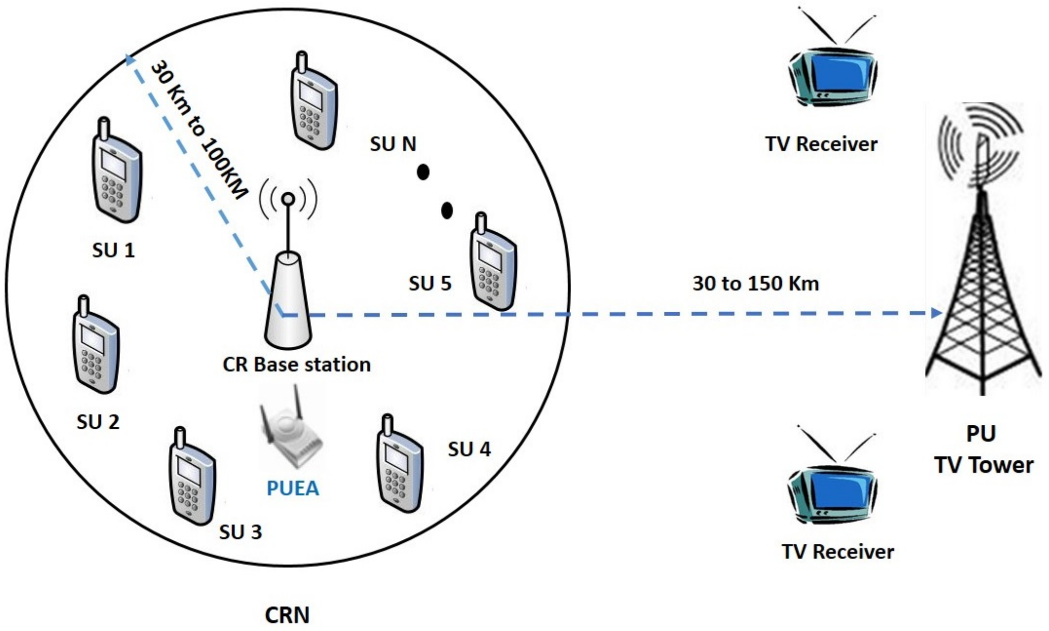

Figure 1: The basic concept of PUEA in CRN

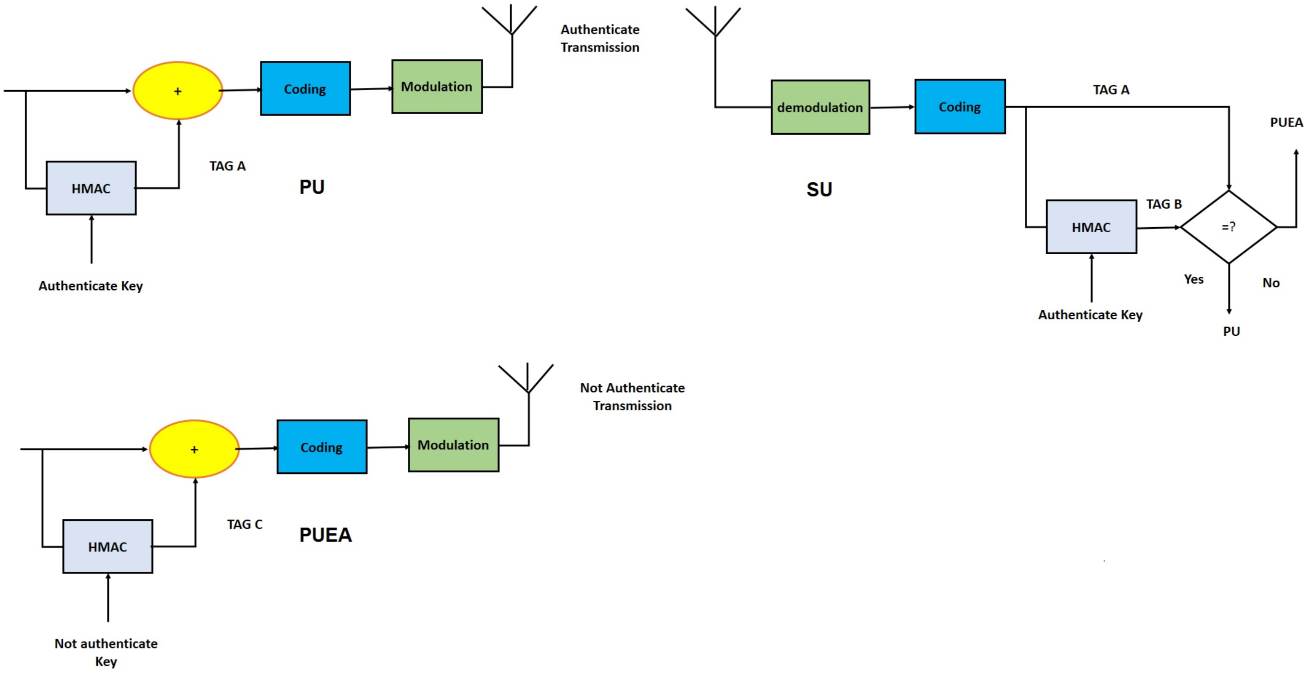

Figure 2: Block diagram of the proposed system

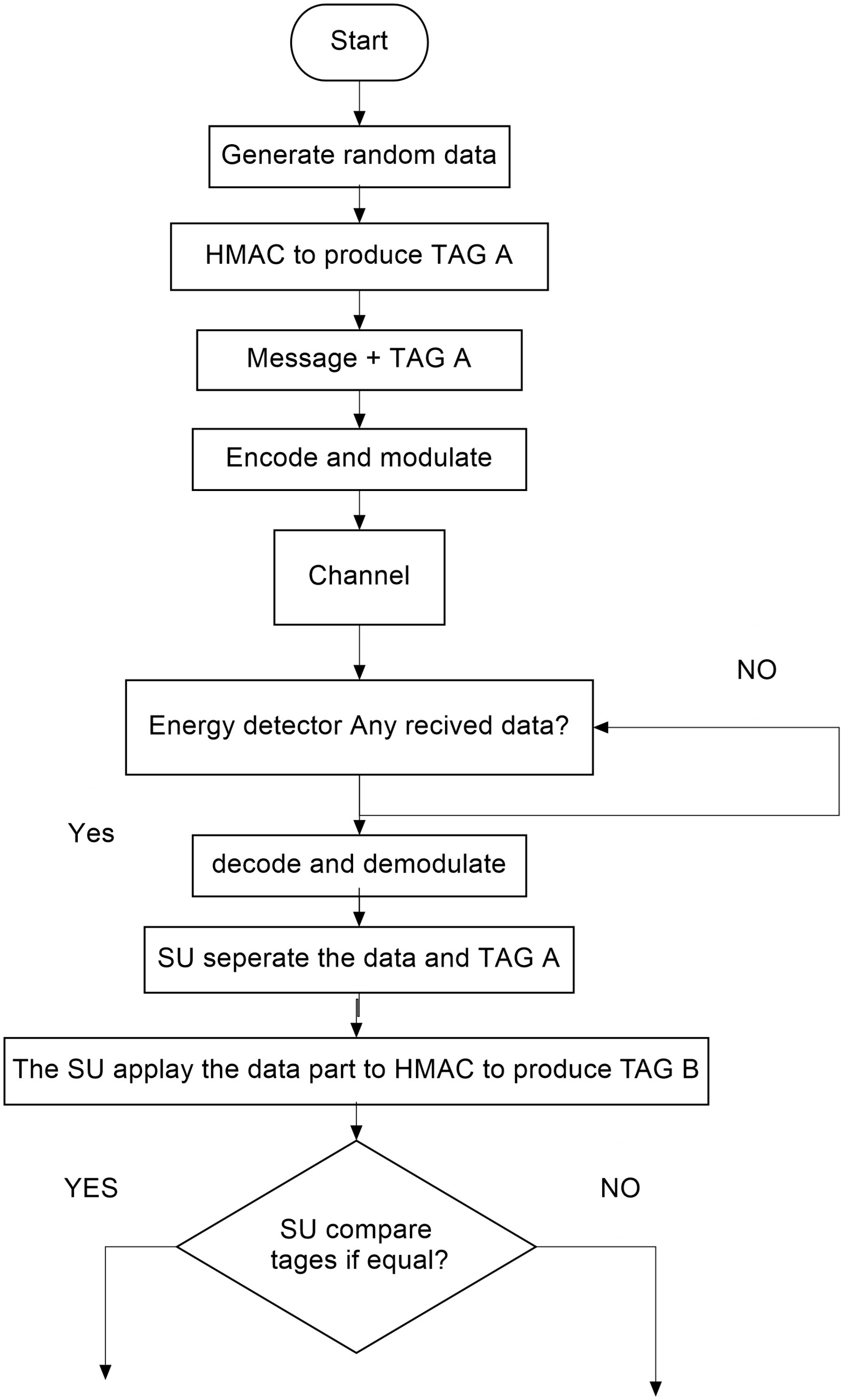

Figure 3: Flow chart of the proposed model

4 Performance Matrices

In this section, the system performance is analyzed by using false alarm probability and detection probability [10]. Most existing works on cognitive sensing focused on performing a hypothesis testing to decide the presence of the primary user. H0: the signal is from the primary user H1: the signal is from the attacker

- **Probability of false alarm (PFA)**: When the signal is considered from the primary user, the probability that the SU falsely Identify the signal as from the attacker is defined by [10]:

  $$P_{FA} = Pr(H_1 \backslash H_0). \tag{1}$$

  If this case happens, the SU will attempt to access the network and cause interference to the PU. Then the SU may be punished as an attacker. Hence the SU may use a strategy to make PFA as small as possible while the attacker wants to make PFA as large as possible.

- **Probability of Primary User detection (PDP)**: When the signal is deeded from the PU, the probability that the SU classifies it as from the primary use,

  $$P_{DP} = Pr(H_0 \backslash H_0) = 1 - P_{FA}. \tag{2}$$

  If this case happens, the SU will attempt to access the network and cause interference to the PU. Then the SU may be punished as an attacker. Hence the SU may use a strategy to make PFA as small as possible while the attacker wants to make PFA as large as possible.

- **Probability of Misdetection (PMD)**: When the signal is counted from the attacker, the probability that the SU classifies falsely it as from the primary user is detonated by,

  $$P_{MD} = Pr(H_0 \backslash H_1). \tag{3}$$

  If this happens, the victim will give up accessing the network, although the spectrum band is vacant, and the attacker launches a successful PUEA and takes the spectrum resources. Another widely matrices is the probability of detection of the attacker PDA.

  $$P_{DA} = Pr(H_1 \backslash H_1) = 1 - P_{MD}. \tag{4}$$

  The SU should take a strategy to make the PDA as large as possible.

5 Analytical Model Evolution

The authentication tag is formed using a Key based HMAC, even a single bit in the tag or the message will destroy the authentication between the SU and the PU. The probability of false alarm is calculated analytically for the uuencoded BPSK under AWGN.

The Probability of False Alarm for Uuencoded BPSK Under AWGN

The probability of false alarm is related to the probability of one bit occurs in the tag or the data. Assume the channel is a binary symmetric channel with error probability equal to P, the bit error occurs independently. Hence, the probability of m errors in a block of n bits is given by [20].

$$P(m,n) = \binom{n}{k} P^m (1-P)^{n-m} \tag{5}$$

The probability of false alarm is measured by calculating the probability of one error occur and more, therefore, the probability of false alarm is given by

$$\begin{aligned} P_{FA} &= Pr(atleastonebiterror) & (6)\\ &= \sum_{m=1}^{n} \binom{n}{k} P^m (1-P)^{n-m} & (7) \end{aligned}$$

The channel error rate of BPSK under AWGN is given by [20]:

$$P = 0.5erfc(\sqrt{\frac{E_b}{N_o}}). \tag{8}$$

The probability of false alarm of uuencoded BPSK is done by put Equation (8) into Equation (6):

$$P_m = \sum_{m=1}^{n} \binom{n}{k} (0.5erfc(\sqrt{\frac{E_b}{N_o}})^m)(1-(0.5erfc(\sqrt{\frac{E_b}{N_o}})))^{n-m} \tag{9}$$

For Coded BPSK Using a Linear Block Coding (BCH Code)

$$P_{CW}^{tag} \leq \sum_{i=t^{tag}+1}^{n} \binom{n^{tag}}{i} P^i(1-P)^{n-i} \tag{10}$$

$$P_{b}^{tag} \leq \frac{1}{n^{tag}} \sum_{i=t^{tag}+1}^{n} i\binom{n^{tag}}{i} P^i(1-P)^{n-i} \tag{11}$$

For simplicity equally will be used the probability of false alarm is given by:

$$\begin{aligned} P_{FA} &= 1-(1-P_{CW}^{tag})^{\frac{L}{K^{tag}}} \\ &= 1-(1-\sum_{i=t^{tag}+1}^{n} \binom{n^{tag}}{i} * P^i(1-P)^{n-i})^{\frac{L}{K^{tag}}} \end{aligned} \tag{12}$$

The probability of False Alarm of BPSK under AWGN using block code is done by substitute Equation (6) into Equation (12):

$$P_{FA} = 1-(1-\sum_{i=t^{tag}+1}^{n} \binom{n^{tag}}{i} (0.5erfc(\sqrt{\frac{E_b}{N_o}}))^m(1-(0.5erfc(\sqrt{\frac{E_b}{N_o}}))^{n-i})^{\frac{L}{K^{tag}}} \tag{13}$$

The overall probability of detection of the primary user of BPSK under AWGN when error correcting block code block code is done by:

$$P_{DP} = (1-\sum_{i=t^{tag}+1}^{n} \binom{n^{tag}}{i} (0.5erfc(\sqrt{\frac{E_b}{N_o}})))^m(1-(0.5erfc(\sqrt{\frac{E_b}{N_o}}))^{n-i})^{\frac{L}{K^{tag}}} \tag{14}$$

More about authentication and encryption will be found in [11, 17, 18].

6 Simulation And Numerical Results

In this section, the effectiveness of the HMAC authentication method will be validated through analytical and simulation. The simulation parameters of the system will be tabulated in table 1. First the data is generated by the PU as a random data of length 18bytes, this data is prepared first to apply as the input of the HMAC function to produce an output with a length of 20 bytes by taking the left 18 bytes in the output to produce TAG A. The TAG A is appended to the message using TDMA algorithm, then encoded, modulated and sent both of them on the channel. The SU separates the message and TAG A. The received message is applied to HMAC to produce TAG B. The SU compares the two tags. If the two tags are identical, then the transmission is represented by PU, otherwise is done by the attacker. Mont Carol simulation is used, for every packet we run 10000 times and calculate the probability of the false alarm and detection.

In Figure 4 the probability of false alarm varies by changing the SNR dB using BPSK under AWGN channel model. As the SNR increases the probability of the PFA decreases. The simulation and the analytical solution gives the same results. It is also show that, using a good error correcting code decreases the PFA. At SNR=2dB, the PFA=100% for the uuencoded BPSK, when using BCH (7, 4, 1) the PFA is decrease by 15%, when using BCH (31, 16, 3) the PFA is decreased by 60%.

In Figure 5, the probability of false alarm varies by changing the SNR dB under AWGN channel model when the error correcting code is a reed solomn code. As the SNR increases the probability of the PFA is decreases. At

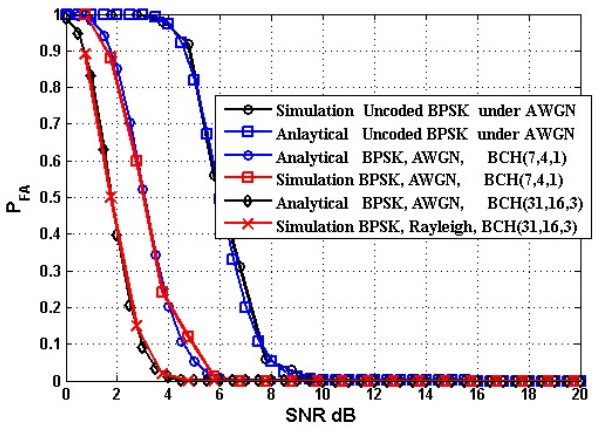

Figure 4: The PFA versus the SNR for a different BCH codes

Table 1: Simulation parameters

Simulation parameters	N=1000
Data length of the PU	16bytes
HMAC code length	16 bytes
Total PU data	36 bytes
Channel	AWGN
Modulation type	BPSK
S/N dB	0:20 dB
Encoding types	BCH, Reed solomn
Hash method used	SHA-1

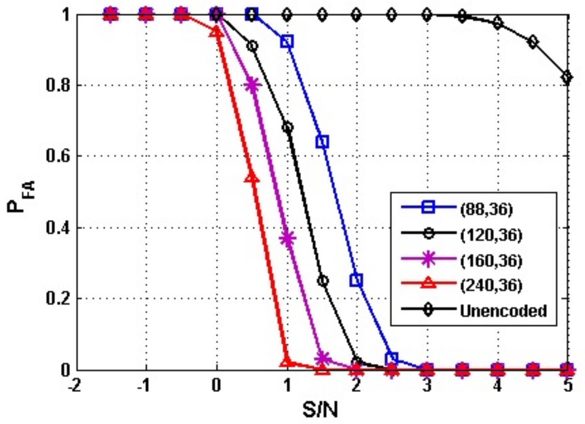

Figure 5: PFA V.s SNR for Uuencoded and encoded using RS (n, k) codes

SNR=1dB the PFA=100% for the uuencoded, when using RS (88, 36), RS (120, 36), RS (160, 36) and RS (240, 36) the PFA is decrease by 10%, 30 %, 60% and 98% respectively.

In Figure 6 the probability of detection (PDA) is varied according to SNR dB. The SU detect the attacker at each value of the SNR and achieve 100% detection of PUEA under all cases. In this simulation the attacker tries many keys to confuse the SU but he cannot. The two curves are identical.

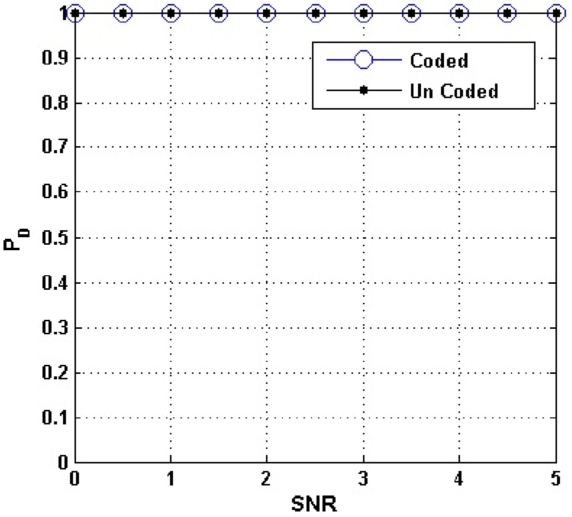

Figure 6: PDA of BPSK under AWGN

7 Conclusions

In this paper, a new method is proposed to solve the primary user emulation attack in cognitive radio networks. In this model, the primary user uses a hash message authentication code (HMAC) to authenticate its transmission. The new method helps the secondary user to defines the attackers, by appending a tag in the transmission and sends the tag and the message on the channel. At the receiver the SU separates the tag from the message and a new tag is generated from the received message and the shard key. If the two tags are the same, then the transmission is considered from the PU, otherwise, the PUEA is in progress. The simulation results show that the new method completely defeats the PUEA and provides good detection of the primary user. In future, more error correcting codes and channel models will be used.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, “Nextgeneration/dynamic spectrum access/cognitive radio wireless networks,” *Computer Networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[2] A. Alahmadi, M. Abdelhakim, J. Ren, and T. Li, “Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard,” *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 772–781, 2014.

[3] A. Alahmadi, T. Song, and T. Li, “Sub-band detection of primary user emulation attacks in ofdm-based cognitive radio networks,” in *2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP’14)*, pp. 1165–1169, Atlanta-GA, Dec. 2014.

[4] S. Anand, Z. Jin, and K. P. Subbalakshmi, “An analytical model for primary user emulation attacks in cognitive radio networks,” in *3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN’08)*, pp. 1–6, Chicago, USA, Oct. 2008.

[5] F. Bao, H. Chen, and L. Xie, "Analysis of primary user emulation attack with motional secondary users in cognitive radio networks," in *2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC'12)*, pp. 956–961, Sydney-NSW, Sept. 2012.

[6] J. Blesa, E. Romero, A. Rozas, and A. Araujo, "Pue attack detection in cwsns using anomaly detecttion techniques.," *EURASIP Journal on Wireless Communications and Networking,*, vol. 2013, no. 1, pp. 1154–1164, 2013.

[7] K. Borle, B. Chen, and W. Du, "A physical layer authentication scheme for countering primary user emulation attacks," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'13)*, pp. 2935–2939, Vancouver, BC, May 2013.

[8] C. Chen, H. Cheng, and Y. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack," *IEEE Transactions on Wireless Communication,*, vol. 10, no. 7, pp. 2135–2141, 2011.

[9] R. Chen, J. Park, and J. Reed, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *Proceedings of the IEEE Workshop Network Technology Software Defined Radio Networks(2006)*, pp. 110–119, Reston, USA, sept 2006.

[10] Z. Chen, T. Cooklev, C. Chen, and C. Plmalaza-Raez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in *IEEE International Conference on Communications (ICC'09)*, pp. 208–215, Scottsdale, AZ, Dec 2009.

[11] Y. Dou, W. Jiang, and C. Ma, "Improved fault attack against eta pairing," *International Journal of Network Security*, vol. 16, no. 1, pp. 71–77, 2014.

[12] W. R. Ghanem, M. Shokir, and MI Dessouky, "Investigation of puea in cognitive radio networks using energy detection in different channel model," *Circuits and Systems: An International Journal*, vol. 2, no. 2/3/4, pp. 1–11, 2015.

[13] M. Haghighat and S. M. S. Sadough, "Smart primary user emulation in cognitive radio networks: defence strategies against radioaware attacks and robust spectrum sensing.," *Transactions on Emerging Telecommunications Technologies,*, vol. 26, no. 9, pp. 1154–1164, 2015.

[14] L. Huang, L. Xie, H. Yu, W. Wang, and Y. Yao, "Anti-pue attack based on joint position verification in cognitive radio networks," in *2010 International Conference on Communications and Mobile Computing (CMC'10),* , pp. 169–173, Shenzhen, April 2010.

[15] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," in *IEEE International Conference on Communications (ICC'09)*, pp. 1–5, Dresden, USA, June 2009.

[16] Z. Jin and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *IEEE International Conference on Communications (ICC'09)*, pp. 1–5, Dresden, USA, June 2009.

[17] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol.," *International Journal of Network Security*, vol. 15, no. 1, pp. 64–67, 2013.

[18] C. Lin, Y. Lv K. Li, and C. C. Chang, "Ciphertext-auditable identity-based encryption.," *International Journal of Network Security*, vol. 17, no. 1, pp. 23–28, 2015.

[19] J. Mitola and G. Q. Maguire, "Cognitive radios: Making software radios more personal," *IEEE Personal Communication*, vol. 6, no. 4, pp. 13–18, 1999.

[20] J. G. Proakis and M. Salehi, *Digital Communications (5ed), English.* USA: McGraw-Hill Education, 2007.

[21] M. J. Saber and S. M. S. Sadough, "Optimal soft combination for multiple antenna energy detection under primary user emulation attacks," *AEU-International Journal of Electronics and Communications,*, vol. 69, no. 9, pp. 1181–1188, 2015.

[22] A. A. Sharifi, Morteza Sharifi, and Mir Javad Musevi Niya, "Secure cooperative spectrum sensing under primary user emulation attack in cognitive radio networks: Attack-aware threshold selection approach," *AEU-International Journal of Electronics and Communications,*, vol. 7, no. 2/3/4, pp. 95–104, 2016.

[23] W. Stallings, *Cryptography and Network Security: Principles and Practice (5ed).* USA: Prentice-Hall, 2010.

[24] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE*, vol. 55, no. 4, pp. 523–531, 1967.

Walid R Ghanem received the B.Sc. degree in communication engineering from Electronic Engineering, Menoufia University, Egypt, in May 2011, and he is currently working toward the MSc degree in Electrical communication engineering. His current research interests are cognitive radio networks, Localization, wireless security, encryption and optimization algorithms.

Mona Shokair received the B.Sc., and M.Sc. degrees in electronics engineering from Menoufia University, Menoufia, Egypt, in 1993, and 1997, respectively. She received the Ph.D. degree from Kyushu University, Japan, in 2005. She received VTS chapter IEEE award from Japan, in 2003. She published about 70 papers until 2014. She received the Associated Professor degree in 2011. Presently, she is an Associated Professor at Menoufia University. Her research interests include adaptive array antennas, CDMA system, WIMAX system, OFDM system, game theory, next generation networks and optimization algorithms.

Moawad I. Dessouky received the B.Sc. (Honors) and M.Sc. degrees from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 1976 and 1981, respectively, and the Ph.D. from McMaster University, Canada, in 1986. He joined the teaching staff of the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 1986. He has published more than 200 scientific papers in national and International conference proceedings and journals. He has received the most cited paper award from Digital Signal Processing journal for 2008. His current research areas of interest include spectral estimation techniques, image enhancement, image restoration, super resolution reconstruction of images, satellite communications, and spread spectrum techniques.