A Primary User Emulation Attack Countermeasure Strategy and Energy-Efficiency Analysis in Cognitive Radio Networks

Yunchuan Wang, Xiaorong Xu, Weiwei Wu, and Jianrong Bao
College of Telecommunication Engineering, Hangzhou Dianzi University, Hangzhou, Zhejiang 310018, China
Email: waynetjlg@foxmail.com; xuxr@hdu.edu.cn; 15968138729@163.com; baojr@hdu.edu.cn

Abstract—Due to the fact that security and energy efficiency are investigated separately in the conventional Primary User Emulation Attack (PUEA) countermeasure strategy in Cooperative Spectrum Sensing (CSS) process, the tradeoff between security and energy efficiency is discussed in this paper. CSS can improve detection performance whereas energy consumption will dramatically boost up with the increasing of cooperative users. To tackle this problem, we set CSS energy efficiency in the presence of PUEA as optimal objective, whereas secure detection performance and secure false alarm threshold as the constraint conditions. The optimal problem is resolved to achieve a trade-off between energy efficiency and security in the presence of PUEA attack. The optimal fusion threshold K and optimal cooperative user numbers can be obtained in secure CSS with energy efficiency maximization, which guarantees energy efficiency as well as secure CSS detection performance. The proposed PUEA countermeasure strategy detection performance is presented and compared with traditional Maximum Ratio Combining (MRC) fusion rule. Simulation results show that, the proposed strategy is immune to PUE interference power, and it provides high robustness to PUEA attack, which implements the trade-off between security and energy efficiency in Cognitive Radio Network (CRN) effectively.

Index Terms—Cooperative Spectrum Sensing (CSS), Primary User Emulation Attack (PUEA), countermeasure strategy, energy efficiency, detection performance

I. Introduction

Cognitive Radio (CR) is a promising technique that enables a smart exploitation of the unused portions of the licensed spectrum. In Cognitive Radio Networks (CRN), Secondary User (SU) can adaptively adjust the operational parameters (such as the transmit power, carrier frequency and modulation method) via sensing the external wireless environments. SU can access to the authorized spectrum to realize dynamic spectrum sharing by overlay or underlay approaches with the premise of not affecting the authorized Primary User (PU) normal communications. CR technology has greatly reduced the constraints of spectrum and bandwidth for the development of wireless technology. It has become one of the potential key technologies in the 5G standards [1], [2].

CRN is one of the key technologies of 5G [3], However, CRN is an open network environment, which is particularly vulnerable to malicious user attack. CRN not only faces the conventional wireless network security threats, such as eavesdropping attack, tampering data, etc [4], [5], but also confronts with some new threats such as PUEA [5] and Spectrum Sensing Data Falsification (SSDF) [6]. The traditional wireless network security problems could be mainly solved by the encryption of transmitting signals [3], [4], [7]. However, energy consumption was significantly increased in secure transmission due to the complexity of encryption algorithm and key management mechanism. Hence, physical layer (PHY) security was regarded as complement or substitution of conventional encryption techniques, which had drawn much attention by network security researchers [8]-[10]. The basic idea of PHY security is to make use of the random feature of the noisy channel to ensure that malicious users can not obtain transmit message from the channel. In other words, PHY security uses the inherent uncertainty of the noisy channel, in order to ensure CRN data security. PHY security considered the security from information theory and signal processing perspectives [8], [9]. PHY security contained two aspects. On the one hand, CRN security capacity was theoretically analyzed from the information theory perspective. On the other hand, secure transmit rates to achieve security capacity was investigated from signal processing and optimization perspective [9], [10].

However, CRN requires more on energy efficiency and system security in the pursuit of high spectrum utilization and high transmission efficiency. Recent research showed that, energy consumed in spectrum sensing phase and data transmission phase were the main energy cost in CRN [11]. With the increasing of SU density and the expansion of network coverage area, CRN energy consumption problem has drawn much attention. Namely, "Green Communications" has become one of the

Manuscript received August 3, 2016; revised January 21, 2017.
This work was supported in part by the Program of Zhejiang Provincial Natural Science Foundation of China (Grant No. LY15F010008, LZ14F010003), National Natural Science Foundation of China (Grant No. 61471152), the Graduate Scientific Research Foundation of Hangzhou Dianzi University in 2016 (ZX160602308035) and Young Talent Cultivation Project of Zhejiang Association for Science and Technology (Grant No. 2016YCGC009).
Corresponding author email: xuxr@hdu.edu.cn.
doi: 10.12720/jcm.12.1.1-7

development trends for CRN in the future. "Green CRN" is the research hotspot in CR at present. It is also one of the key techniques to realize future energy efficiency wireless communications [11], [12]. In addition, due to two different network architectures existed in CRN, namely, primary network and cognitive network, data transmission security issue has become a new research direction in the field of CRN [7]-[9].

PHY security is the emphasis in energy-efficient CRN. In [12], the authors pointed out that there is an optimal trade-off between energy efficiency and transmission security in CRN. The system adopts different PHY security strategies in accordance with different malicious attacks, thus energy consumption varies for different security schemes. Therefore, in order to ensure secure and reliable transmission, it is necessary to discuss the optimal energy-efficient security strategy for a specific attack. Ref. [8] and Ref. [9] investigated the common malicious attacks and the corresponding countermeasure strategies in CRN.

In CRN spectrum sensing phase, SUs firstly identify legitimate SUs and malicious SUs. The presence of malicious SUs will influence the accuracy of secure cooperative spectrum sensing [5], [6]. A proposed scheme in [6] mainly studied the trade-off between energy efficiency and security for SSDF attack. The scheme effectively detected channel availability through reporting message authentication code (MAC) to the fusion center. However, Hash function was required to generate MAC in this scheme, which inevitably resulted in the increasing of complexity. Furthermore, the proposed scheme didn't consider the influence of legitimate SUs' reporting error rate as well as reporting distance to CSS energy consumption [6].

In [5], the authors studied effective CSS in the presence of PUEA. Local sensing information from different SU was weighted at the fusion center. The weights could be optimized by maximizing the detection probability under a constraint of false alarm probability. Meanwhile, the influence of channel estimation error on CSS detection performance was also discussed. In [13], the authors investigated PUEA attack and its countermeasure strategy in mobility CRN scenario. A hybrid strategy based on PUEA countermeasure with CSS detection was proposed, which was satisfied the requirements of false alarm probability and the detection performance in PUEA attack with lower energy consumption. At the same time, the overall performance of PUEA problem with game theory analysis was presented in the conditions of different attack overhead and detection overhead, which could reduce the total resource consumption and increase CRN throughput [13], [14].

At present, PHY security in spectrum sensing phase mainly focuses on the PUEA or SSDF countermeasure strategies [4], [5], [7]-[9], [13], [14]. Aimed to the trade-off between security and energy efficiency in CRN, the paper mainly focuses on energy-efficient PUEA countermeasure strategy with performance analysis [3], [6], [12], [15]. Specifically, energy efficiency of the proposed PUEA countermeasure strategy is derived in detail. Energy efficiency is set as the optimal objective, whereas secure detection probability and secure false alarm threshold as the constraint conditions. Then, the optimal fusion threshold K and optimal SU number N are presented to achieve the maximization of energy efficiency by resolving the optimization problem, which guarantees energy efficiency as well as secure CSS detection performance.

The rest of this paper is organized as follows, Section II describes the system model. Secure CSS under PUEA is described in detail in the Section III. Section IV describes the proposed countermeasure strategy against PUEA and analyzes its energy efficiency performance. Simulation results are presented and discussed in Section V. Finally, conclusions are drawn in Section VI.

II. System Model

In this paper, we consider CSS in a CRN where N SUs trying to access a target spectrum. As shown in Fig. 1, to avoid conflict with the PU, each SU detects the target spectrum within a specific period and judges whether the spectrum is occupied by PU or not. Then, SUs report local detection results to the Fusion Center (FC). Finally, the FC makes global detection to decide whether the spectrum is occupied by PU via specific fusion rule. The PUE attacker mimics the feature of PU and launches the PU signal to deceive SUs, which makes SUs to judge that PU is occupying the authorized spectrum. Therefore, SUs are forced to switch to another spectrum holes. The key issue to defend PUEA is that SUs should identify PU and PUEA, and make right judgment on PU and PUEA signals [5], [13], [14]. In this paper, energy detection is implemented in SU local detection, and hard fusion with *K-out-of-N* fusion rule is applied at FC. It is assumed that the report channels from SUs to the FC are noisy.

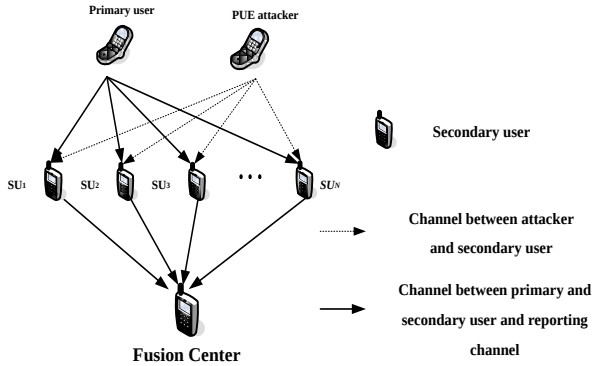

Fig. 1. System model of cooperative spectrum sensing with PUEA in CRN.

III. Cooperative Spectrum Sensing in the Presence of PUEA

SU local spectrum sensing consists of three common techniques. Namely, energy detection, matched filtering

detection and cyclo-stationary feature detection [1], [2]. In this paper, we use energy detection to judge the authorized spectrum utilization. Due to the presence of PUEA, for $1 \le j \le N$, the signal received by the *j*th SU at the *i*th ($1 \le i \le M$) time instant [5] can be written as

$$y_j(i) = \begin{cases} P_m h_{m,j} x_{m,j}(i) + w_j(i), & H_0 \\ P_p h_{p,j} x_{p,j}(i) + P_m h_{m,j} x_{m,j}(i) + w_j(i), & H_1 \end{cases} \quad (1)$$

We denote that when PUEA is present, the absence and presence of PU can be expressed as two hypotheses respectively, that is, H_0 and H_1. Signals transmitted by PU and PUE attacker with power P_p and P_m are $x_{p,j}(i)$ and $x_{m,j}(i)$ respectively. PU signal $x_{p,j}(i)$ is assumed to be independently and identically distributed (i.i.d) complex Gaussian random variable with zero mean and unit variance. Due to the similarity between malicious and primary signal in PUEA, the attacker's signal $x_{m,j}(i)$ also follows the complex Gaussian distribution. $h_{p,j}$ and $h_{m,j}$ denote the instantaneous channel gain from primary user to the *j*th secondary user and from PUE attacker to the *j*th secondary user, respectively. In addition, all the channel links are assumed as block fading channel, that is, $h_{p,j}$ and $h_{m,j}$ are constant within one time interval. $w_j(i)$ denotes the additive white Gaussian noise at the *j*th secondary user with zero mean and variance $\sigma_{w_j}^2$. The signal-to-noise ratio (SNR) received at the *j*th SU can be expressed as $\gamma_j = h_{p,j}^2 / \sigma_{w_j}^2$.

In this paper, we adopt energy detection method in which *M* samples of signal energy are added during one detection interval, the power detected by the *j*th SU can be expressed as $Y_j = \sum_{i=1}^{M} |y_j(i)|^2$. Due to $x_{p,j}(i)$ and $x_{m,j}(i)$ follow the complex Gaussian distribution with zero mean and unit variance, the decision statistic Y_j is subject to the central Chi-square (χ^2) distribution with 2*M* degrees of freedom [16]

$$Y_j = \sum_{i=1}^{M} \left| y_j(i) \right|^2 = \begin{cases} Y_0 \sim \chi_{2M}^2(\sigma_0^2) \\ Y_1 \sim \chi_{2M}^2(\sigma_1^2) \end{cases} \quad (2)$$

where σ_0^2 and σ_1^2 are the variance for H_0 and H_1 respectively

$$\begin{aligned} \sigma_0^2 &= P_m^2 h_{m,j}^2 + \sigma_{w_j}^2 \\ \sigma_1^2 &= P_p^2 h_{p,j}^2 + P_m^2 h_{m,j}^2 + \sigma_{w_j}^2 \end{aligned} \quad (3)$$

In spectrum sensing, false alarm probability $\Pr_f$ and detection probability $\Pr_d$ over one detection interval are defined as

$$\begin{aligned} \Pr_f &= \Pr\left\{ Y_j \ge \lambda \middle| H_0 \right\} \\ \Pr_d &= \Pr\left\{ Y_j \ge \lambda \middle| H_1 \right\} \end{aligned} \quad (4)$$

where λ is detection threshold. Hence, the false alarm probability $\Pr_f$ and detection probability $\Pr_d$ at the *j*th SU are expressed as [1], [2], [17]

$$\begin{aligned} \Pr_f &= \Gamma(M, \frac{\lambda}{\sigma_0^2}) \\ \Pr_d &= \Gamma(M, \frac{\lambda}{\sigma_1^2}) \end{aligned} \quad (5)$$

Each SU issues a local binary decision $d_j \{1,0\}$ about the spectrum status. If $Y_j > \lambda$, then $d_j = 1$, which denotes that the spectrum is occupied by PU. Otherwise, the spectrum is identified as unused by PU [1], [2], [17].

$$d_j = \begin{cases} 1 & Y_j > \lambda \\ 0 & Y_j < \lambda \end{cases} \quad (6)$$

All local decisions are reported to the FC via reporting channels. At the FC, a specific fusion rule (FR) is employed to process these decisions in order to make the final global decision. In this paper, we use *K-out-of-N* rule, where *K* is a predefined threshold on the number of SUs who detect PU on the spectrum ($1 \le K \le N$). The idea behind this rule is to compare the number of SUs that report 1 with *K*. If it is less than *K*, then the spectrum is unused by PU. Otherwise, the spectrum is used by PU.

In this paper, the reporting channel between SU and FC is assumed to be noisy, which can be modelled as binary symmetric channel with error probability $\Pr_e$, hence, we can modify the expression of $\Pr_f$ and $\Pr_d$ as below [18].

$$\begin{aligned} \Pr_x &= \Pr_d (1 - \Pr_e) + (1 - \Pr_d) \Pr_e \\ \Pr_y &= \Pr_f (1 - \Pr_e) + (1 - \Pr_f) \Pr_e \end{aligned} \quad (7)$$

The overall detection probability (Q_d) and overall false-alarm probability (Q_f) can be expressed respectively as follows

$$\begin{aligned} Q_d &= \sum_{j=K}^{N} \binom{N}{j} \Pr_x^j (1 - \Pr_x)^{N-j} \\ Q_f &= \sum_{j=K}^{N} \binom{N}{j} \Pr_y^j (1 - \Pr_y)^{N-j} \end{aligned} \quad (8)$$

IV. Energy Efficiency Analysis of PUEA Countermeasure Strategy

Energy efficiency (μ) can be defined as the ratio of average throughput in *bits* to average energy consumption in *Joule*. The average throughput is defined as average number of successfully transmitted bits, and the average consumed energy is the energy consumed during CSS and reporting results transmission in the reporting phase. The average throughput can be expressed as follows

$$Th = \Pr_0 (1 - Q_f) R \quad (9)$$

where $\Pr_0$ is the probability that the spectrum is not occupied by PU. R denotes the data rate, and T is the data transmission time interval. The factor $(1-Q_f)$ in (9) represents the probability of successful delivering the transmit data.

The average energy consumption by all SUs is given as follows

$$E = Ne_s + \Pr_{unused}\, e_t \tag{10}$$

where e_s is the energy consumed during CSS by one SU, and e_t is the energy consumed during reporting phase. Note that transmission occurs only if the spectrum is identified as unused. Thus, $\Pr_{unused}$ can be given as follows

$$\begin{aligned}\Pr_{unused} &= \Pr_0(1-Q_f) + \Pr_1(1-Q_d) \\ &= 1-\Pr_0 Q_f - \Pr_1 Q_d\end{aligned} \tag{11}$$

where $\Pr_1 = 1-\Pr_0$. Therefore, energy efficiency of defense strategy against PUEA can be expressed as follows

$$\mu = \frac{\Pr_0(1-Q_f)RT}{Ne_s + e_t(1-\Pr_0 Q_f - \Pr_1 Q_d)} \tag{12}$$

The optimization of K for energy efficiency in the proposed PUEA countermeasure strategy with constraint conditions on the Q_d and Q_f , which can be stated as below

$$\begin{aligned}&\max_K \mu \equiv \max_K \frac{\Pr_0(1-Q_f)RT}{Ne_s + e_t(1-\Pr_0 Q_f - \Pr_1 Q_d)} \\ &\text{s.t.}\, Q_d \ge \alpha \;\; and \;\; Q_f = \beta\end{aligned} \tag{13}$$

The K value that satisfies (13) without the constraint can be obtained by the derivative of objective μ into zero, namely

$$\begin{aligned}&\frac{-\Pr_0 RT\dfrac{\partial Q_f}{\partial K}}{Ne_s + e_t(1-\Pr_0 Q_f - \Pr_1 Q_d)} + \\ &\frac{\Pr_0(1-Q_f)RTe_t\left(\Pr_0\dfrac{\partial Q_f}{\partial K} + \Pr_1\dfrac{\partial Q_d}{\partial K}\right)}{\left[Ne_s + e_t(1-\Pr_0 Q_f - \Pr_1 Q_d)\right]^2} = 0\end{aligned} \tag{14}$$

The derivatives of Q_f and Q_d can be written approximately as follows

$$\begin{aligned}\frac{\partial Q_f}{\partial K} &= Q_f(K+1) - Q_f(K) = \binom{N}{K}\Pr_y^K(1-\Pr_y)^{N-K} \\ \frac{\partial Q_d}{\partial K} &= Q_d(K+1) - Q_d(K) = \binom{N}{K}\Pr_x^K(1-\Pr_x)^{N-K}\end{aligned} \tag{15}$$

Substitute (15) into (14) with some mathematical calculations, the optimal K that maximizes the energy efficiency can be presented in a closed form shown as below

$$K_1 = \frac{\ln\left(\dfrac{Ne_s + \Pr_1 e_t(1-Q_d)}{\Pr_1 e_t(1-Q_f)}\right) + N\ln\left(\dfrac{1-\Pr_y}{1-\Pr_x}\right)}{\ln\left(\dfrac{\Pr_x(1-\Pr_y)}{\Pr_y(1-\Pr_x)}\right)} \tag{16}$$

Hence, for a given N and a given false alarm probability, the detection probability decrease as K increases, the optimal K that maximizes energy efficiency while fulfilling the detection probability requirements can be written as below.

$$K_{opt} = \min\{K_1, K_2\} \tag{17}$$

where the value of the K that satisfies the constraint condition in CSS detection. From [17], we can get the approximated expression of K_2 shown as below.

$$K_2 \approx Q^{-1}(\alpha)\sqrt{N\Pr_x(1-\Pr_x)} + N\Pr_x + 0.5 \tag{18}$$

V. Simulation Results and Analysis

In this section, we analyze the simulation performance of the proposed PUEA countermeasure strategy with energy efficiency optimization. We assume that there is one PUE attacker in the proposed scheme. Sensing channels and reporting channels are i.i.d. The number of samples within a detection interval is $M = 3$ [5]. All simulation parameters are summarized in Table I. These parameters are assumed to be identical among all SUs.

TABLE I: SIMULATION PARAMETERS

Parameters	Values	Parameters	Values
N	10	Q_d	≥ 0.6
Q_f	0.1	$\Pr_0$	0.5
e_s	10^{-2} Joule	e_t	1 Joule
T	0.3 sec	R	100 Kbps

Fig. 2 shows the receiver operation characteristics (ROC) performance when the FC uses hard FR for CSS in the presence of PUEA. In this figure, the average SNR is set to be 0 dB and the transmitting power of primary user and PUE attacker are identical $P_p = P_m = 1$. From Fig. 2, we find that the detection probability of non-cooperation scheme is severely reduced by PUEA attack. When we use *K-out-of-N* FR in FC, a significant detection performance improvement is achieved, even better than the non-cooperation scheme when the PUE attacker is absent. From Fig. 2, we can find that when we use *K-out-of-N* rule, for a given *N*, the threshold *K* also have great impact on the detection performance. When the false alarm probability is fixed, the overall detection performance shows better with the decreasing of threshold *K*. The reason is that the FR approaches to OR rule with the decreasing of *K*, so that the overall detection performance is enhanced.

Fig. 3 shows energy efficiency of the proposed PUEA countermeasure strategy with a set of different threshold K and SU nodes N. In this figure, the average SNR is set to be 0 dB, the constraint conditions are $Q_d \geq 0.6$ and $Q_f = 0.1$. It is shown that, the maximum energy efficiency of the proposed PUEA countermeasure strategy achieves to $\mu \approx 7.8\times10^4$ bit/ Joule with $N = 5$ and $K = 2$. As shown in Fig. 3, we can also find that the threshold K that achieves to the maximum energy efficiency increases with the increasing of SU nodes in CSS. In addition, with the increasing of SU nodes, the achievable maximum energy efficiency is lower. The reason is that, more SU nodes will increase the energy consumption in the process of CSS and reporting phase, which will decrease energy efficiency.

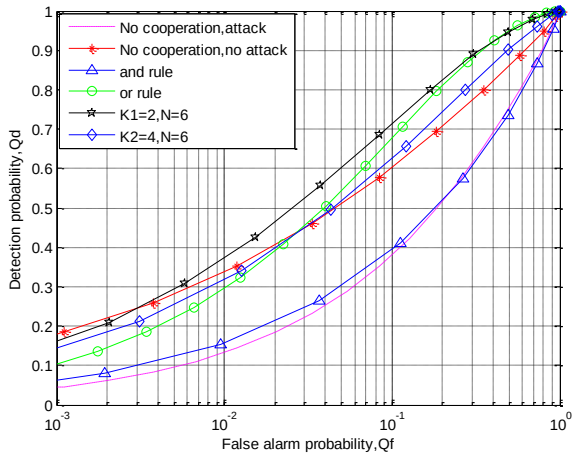

Fig. 2. ROC of CSS with hard fusion rule in the presence of PUEA.

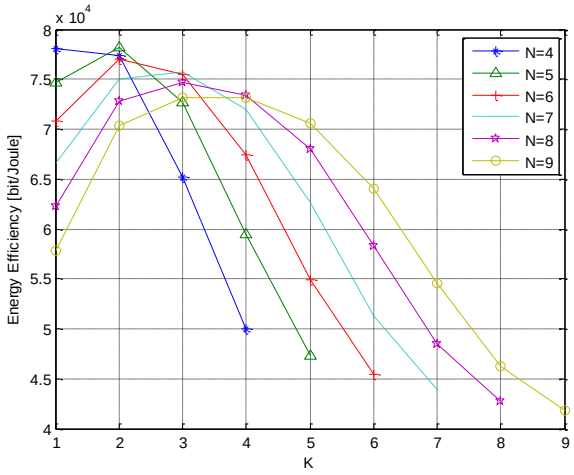

Fig. 3. Energy efficiency of the proposed strategy with different K and N.

From performance analysis in Fig. 3, we found that the proposed PUEA countermeasure strategy can achieve the maximum energy efficiency with SU number $N = 5$ and the optimal threshold $K = 2$. Fig. 4 shows the ROC performance of non-cooperation, *K-out-of-N* rule and MRC with/without PUEA attack. For the same FR, ROC performance without PUEA is better than that with PUEA. When the PUE is present, for the same false alarm probability, the detection probability of the proposed PUEA countermeasure strategy with *K-out-of-N* FR outperforms the MRC scheme. When $Q_f > 0.02$, the detection performance of the proposed strategy shows even better than the non-cooperation scheme without PUEA. However, false alarm probability increases with the increasing of detection probability. Hence, it's necessary to make a trade-off between false alarm probability and detection probability to ensure the ROC performance of secure CSS.

Fig. 5 shows secure CSS detection performance of the proposed PUEA countermeasure strategy in the presence of PUEA with different power ratio between PUE and PU. We define the transmit power ratio between PUE and PU as

$$p = \frac{P_m^2}{P_p^2} \tag{19}$$

Eq. (19) normalizes PUE attacker's power in terms of PU's power. A larger value of p indicates PUE attacker has more transmit power. In this figure, for a given false alarm probability threshold $\Pr_f = 0.1$, the SNR thresholds for each SU are identical.

Secure CSS detection performance of the proposed scheme is compared with MRC scheme whereas p is set to be 0.1/1/10 respectively. As p increases from 0.1 to 10, detection performance of both schemes are decreased. $p = 10$ indicates PUE power is dominant over the noise power. Hence, the detection performance is deteriorated even when the average SNR is very high. We also find that the detection performance of the proposed secure CSS scheme based on *K-out-of-N* FR outperforms MRC FR significantly. What's more, the detection performance of proposed scheme is almost independent of the value p. That is, PUE power has hardly affected the proposed PUEA countermeasure strategy, which indicates the proposed scheme ensures the security of CSS effectively, and the proposed scheme has robustness to defend PUEA attack.

VI. Conclusions

This paper investigates secure CSS strategy that ensures energy efficiency and PHY layer security in CSS spectrum sensing under the presence of PUEA in the CRN. We obtain the optimal threshold K and optimal SU numbers N of secure CSS based on *K-out-of-N* FR via the solution of energy efficiency optimization problem, in order to ensure the CSS detection performance simultaneously. In addition, we analyze the ROC performance with the consideration of optimal energy efficiency. With the comparison of MRC FR, it is apparent that secure detection performance of the proposed scheme with *K-out-of-N* FR outperforms MRC FR scheme in terms of the same false alarm probability scenario. Detection performance of the proposed PUEA countermeasure strategy can be significantly enhanced in

high SNR region. The proposed scheme is almost immune to PUE interference power, which ensures CSS security. Therefore, the proposed strategy has higher robustness to PUEA attack, and it makes a trade-off between energy efficiency and detection performance effectively.

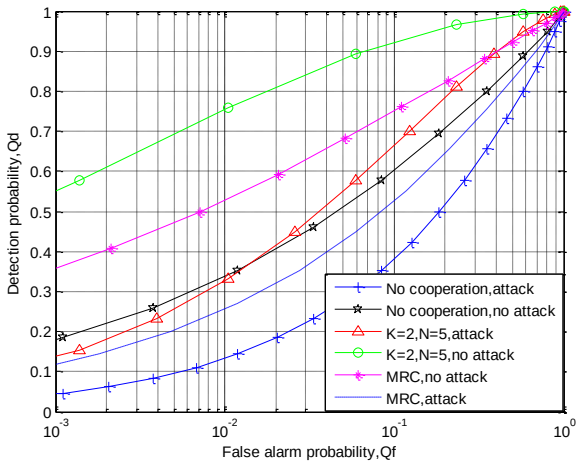

Fig. 4. ROC performance of non-cooperation K-out-of-N rule and MRC with/without PUEA attack.

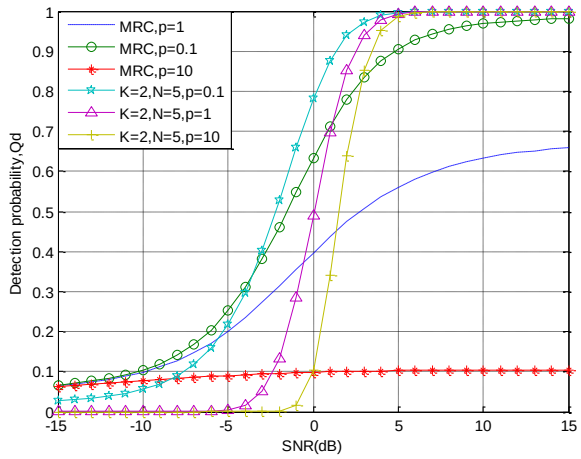

Fig. 5. Detection performance of the proposed PUEA countermeasure strategy with different power ratios.

ACKNOWLEDGMENT

The authors would like to greatly appreciate anonymous reviewers for their valuable comments and constructive suggestions in helping to improve the quality of this paper.

REFERENCES

[1] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks*, vol. 50, no. 13, pp. 2127-2159, September 2006.

[2] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan. "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communications*, vol. 4, no. 1, pp. 40-62, March 2011.

[3] X. Hong, J. Wang, and C. X. Wang. "Cognitive Radio in 5G: A perspective on energy-spectral efficiency tradeoff," *IEEE Communication Magazine*, vol. 52, no. 7, pp. 46-53, 2014.

[4] T. Chen and G. Wei. "Study on physical layer security of wireless networks," *Doctoral Dissertation of South China University of Technology*, 2013.

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

[6] S. Althunibat, V. Sucasas, H. Marques, J. Rodriguez, R. Tafazolli, and F. Granelli, "On the tradeoff between security and energy efficiency in cooperative spectrum sensing for cognitive radio," *IEEE Communications Letters*, vol. 17, no. 8, pp. 1564-1567, 2013.

[7] H. N. Li. "Research on security and privacy in cognitive radio networks," *Doctoral Dissertation of Xidian University*, 2013.

[8] Z. Shu, Y. Qian, and S. Ci. "On physical layer security for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 28-33, 2013.

[9] J. Li, Z. Feng, Z. Feng, and P. Zhang, "A survey of security issues in cognitive radio networks," *China Communications*, vol. 12, no. 3, pp. 132-150, 2015.

[10] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multi-user scheduling in cognitive radio networks," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 5103-5113, 2013.

[11] J. Wang, J. H. Zhao, and J. J. Du, "Survey on cognitive radio green networks with cross-layer technology," *Telecommunication Science*, vol. 30, no. 3, pp. 114-119, 2014.

[12] S. Eryigit, G. Gur, S. Bayhan. "Energy efficiency is a subtle concept: Fundamental tradeoffs for cognitive radio networks," *IEEE Communication Magazine*, vol. 51, no. 7, pp.30-36, 2014.

[13] F. J. Bao. "Research on primary user emulation attack and countermeasures with mobile secondary users in cognitive radio networks," *Master Dissertation of Zhejiang University*, 2013.

[14] F. Bao, L. Xie, and H. Chen, "Analysis of primary user emulation attack with motional secondary users in cognitive radio networks," in *Proc. IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications*, September 2012, pp. 956-961.

[15] C. Comaniciu and H. V. Poor, "On energy-secrecy tradeoffs for Gaussian wiretap channels," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 314-323, 2013.

[16] J. Yang, Y, Chen, W. Shi, X. Dong, and T. Peng. "Cooperative spectrum sensing against attacks in cognitive radio networks," in *Proc. IEEE International Conference on Information and Automation*, 2014, pp. 71-75.

[17] S. Althunibat, M. Di Renzo, and F. Granelli, "Optimizing the K-out-of-N rule for cooperative spectrum sensing in cognitive radio networks," in *Proc. IEEE Global Communications Conference (IEEE Globecom 2013) Communications QoS, Reliability and Modeling Symposium*, 2013, pp. 1607-1611.

[18] X. Xu, J. Bao, Y. Luo, and H. Wang, "Cooperative wideband spectrum detection based on maximum

likelihood ratio for CR enhanced VANET," *Journal of Communications*, vol. 8, no. 12, pp. 814-821, 2013.

Yunchuan Wang is with the College of Telecommunication Engineering, Hangzhou Dianzi University (HDU), Hangzhou, China, as master. He received the B. Eng. degree in Communication Engineering from Tianjin University of Technology, Tianjin, China, in 2015. He is currently working toward his Master degree in the College of Telecommunication Engineering, HDU. His research interests emphasize on energy efficiency and PHY security in Cognitive Radios (CR).

Xiaorong Xu is with the College of Telecommunication Engineering, Hangzhou Dianzi University (HDU), Hangzhou, China, as associate professor and master supervisor. He received the B. Eng. degree in Communication Engineering and M. Eng. degree in Communication and Information System from HDU, Hangzhou, China, in 2004 and 2007, respectively. He received Ph.D. degree major in Signal and Information Processing from Nanjing University of Posts and Telecommunications (NJUPT), Nanjing, China, in 2010. Previously, from 2011 to 2013, he was working as a postdoctoral researcher in the Institute of Information and Communication Engineering, Zhejiang University (ZJU), Hangzhou, China. During 2013-2014, he served as a research scholar with the Electrical and Computer Engineering Department, Stevens Institute of Technology (SIT), Hoboken, NJ, USA. Currently, he is working as an associate professor and master supervisor in HDU. Dr. Xu's research interests emphasize on energy efficiency and PHY security in Cognitive Radios (CR) and energy efficiency in cooperative communications, etc.

Weiwei Wu is with the College of Telecommunication Engineering, Hangzhou Dianzi University (HDU), Hangzhou, China, as master. He received the B. Eng. degree in Communication Engineering from Anhui University of Technology, Anhui, China, in 2015. He is currently working toward his Master degree in the College of Telecommunication Engineering, HDU. His research interests emphasize on energy efficiency and optimal resource allocation in Cognitive Radios (CR).

Jianrong Bao is with the College of Information Engineering, Hangzhou Dianzi University (HDU), Hangzhou, China, as associate professor, He received the B. Eng. degree in Polymer Material Engineering and M. Eng. degree in Communication and Information System from Zhejiang University of Technology, Hangzhou, China, in 2000 and 2003, respectively. He received Ph.D. degree major in Communication and Information System from Tsinghua University, Beijing, China, in 2009. Previously, from 2011 to 2013, he was working as a postdoctoral researcher in the Institute of Information and Communication Engineering, Zhejiang University (ZJU), Hangzhou, China. Currently, he is working as associate professor in HDU. Dr. Bao's research interests emphasize on energy efficiency in Cognitive Radios (CR) and cooperative communications, etc.

