TELKOMNIKA, Vol. 11, No. 7, July 2013, pp. 3905 ~ 3914
e-ISSN: 2087-278X

Primary User Emulation Attacks Analysis for Cognitive Radio Networks Communication

WANG Shan-shan*, LUO Xing-guo, LI Bai-nan
National Digital Switching System Engineering & Technological R&D Center
Jinshui, Zhengzhou, 450001, China, Ph./Fax: +86-03176663266
*Corresponding author, e-mail: beaklee@hotmail.com

Abstract

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 (PUEAs) are typically easy and largely affecting. PUEAs come from both malicious misbehavior secondary users (MMUs) and selfish misbehavior secondary users (SMUs). The former is studied much more deeply than the later one. Distinguishing MMU and SMU, we propose a Four Dimensional Continuous Time Markov Chain model to analyze the communication performance of normal secondary users under PUEAs, and typically affected by SMUs. Furthermore, we compare several PUEA detection schemes. The emulation results indicate that the SMU detection mechanism is essential for the PUEA detection schemes, which can improve the detection effects largely.

Keywords*: CRN, Performance Analysis, PUEA, Malicious User, Selfish User*

1. Introduction

With the wireless communication requirement increasing dramatically, radio spectrum is becoming much more crowded and the fixed allocation mechanism seems unreasonable, which has caused very low spectrum utilization in some areas [1]. Cognitive radio (CR) has emerged as a feasible technique to resolve the above problem [2]. CR networks (CRN) take spectrum sensing and dynamical spectrum resource allocation to make secondary users (SUs) using licensed radio spectrum, which is authorized to primary users (PUs). This new technique can dramatically enhance spectrum efficiency. In CRN, spectrum sensing needs to reliably detect primary signals to find the idle primary bands referred to as spectrum holes. Then the SUs access to these holes. And SU must vacate the spectrum occupying instantly, when the PU begins to transport data on the same spectrum [3]. This principle can protect PUs from the SUs' interference, and also be advantage to extend the available spectrum scope for SU. But it's can be also utilized by some misbehavior secondary users (MUs) to launch denial of service attacks, i.e., primary user emulation attack (PUEA) [4].

In order to realize PUEA, MUs usually send signals which have the same characteristic with those from PU. After detecting these signals, SUs consider that the PU will communicate on the channel, then vacate from the channel, and switch another idle channel. If there are no available channel, the SU drop communication and leave the CRN.

Research on PUEA has attracted more and more attentions. Most of them are interest in the detection and elimination techniques [5, 6]. There are few articles analyze PUEA performance on CRN. Reference [7] explores the numbers of SU, MU, PU to simulate channel occupation, and discusses the communication blocking and dropping rates of CRN under PUEA firstly.

MU can be divided into two parts, malicious MU (MMU) and selfish MU (SMU) [8, 9]. MMU can affect the CRN largely by cheating SUs, and damaging the normal communication. Therefore, SUs must switch channels frequently or have to leave the network. In order to maximize its own communication efficiency, SMU makes use of the vacation principle, and acquires priority over other normal SUs by emulating PU's behavior, which could force SUs to leave the concerned channel. However, when SMU occupies the aimed channel, it will transmit data as a normal SU. After finishing the transmission, SMU quits the occupying channel for other SUs transmission. The selfish behavior of SMU can increase the blocking rate and

Received February 2, 2013; Revised April 22, 2013; Accepted May 8, 2013

dropping rate of normal SUs. Since the reason and performance of attack are different between MMU and SMU, the design of actual network should exploit different measurements to solve above problems. There have been many literatures referring to PUEA detecting algorithms for MMU, while few for SMU. References [7], [10] proposed two performance analyses on PUEA for CRN, but neither considers specials of SMU. We utilize a model of four dimensional continuous time Markov chain (FDMC) to analyze MMU and SMU.

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

2. System Model

2.1. Assumptions

The assumptions made in this paper are listed below.

- There are N_c channels in the system. Every communication process needs one channel.
- There is no waiting queue in the system. Therefore, when no channel is available, SU is blocked.
- When a PUEA or a normal PU communication is detected, the SU related has to vacate the occupying channel and sensing another idle channel for the rest data transmission. If no channel can be found, the SU would drop the transmission.
- Each SU can detect PUs exactly. And the successful rate of PUEA is 100%.
- The requests for channels from PUs and SUs accord to Poisson processes with arrival rates, λ_p, λ_s, respectively, and occupy the channels for a time which are exponential distributed with means, $1/\mu_p$, $1/\mu_s$.
- The PUEAs launched by MMU and SMU accord to Poisson processes with arrival rates, λ_{mm}, λ_{sm}, respectively, and occupy the channels for a time which are exponential distributed with means, $1/\mu_{mm}$, $1/\mu_{sm}$.
- $N_s(t)$, $N_{mm}(t)$, $N_{sm}(t)$, and $N_p(t)$ represent the occupying channel number of SU, MMU, SMU and PU at the moment t respectively. And we use N_s, N_{mm}, N_{sm} and N_p to replace them for simplification.

2.2. Descriptions

This section shows details of SUs, MMUs, SMUs, and PUs as follows.

1) SUs:

a) Access: It has nothing to do with the channel occupying status of system that whether a SU access, which all depends on its own communication demand. Thus, the SU access probability is λ_s.

b) Leave: A SU leaving the system is mainly caused by three reasons that finishing the transmission, or to avoid affecting the PU, or cheated by MUs. The probability of first case is $N_s\mu_s$, and the happening probabilities of other cases are related with the present probabilities of PU and MUs.

2) MMUs:

a) Access: The MMU behaviors can be divided into two types. One type is that MMUs attack on idle channels to prevent potential USs from using the channels. The other type is that MMUs attack on the channel occupying by SU to drop the transmitting process. MMUs wouldn't attack only when all channels are occupied by PUs (i.e., $N_p = N_C$). MMUs may be more than two for blocking all channels in the spectrum interested. Generally, there exists a cooperating scheme among the MMUs. Therefore, spoofs and grabs are not considered, and the access probability of MMU is $(N_C - N_p - N_{mm})\lambda_{mm}$.

b) Leave: If a PU needs transmit data, MMUs will stop attacking the related channel, as that the attacks object is SUs, but not PUs. And when MMUs have reached their goal, they would also

stop attacking and leave. The former probability is related to the primary communication demands, and the latter probability is $N_{mm}\mu_{mm}$.

3) SMUs:

a) Access: SMUs can acquire a channel immediately if idle channels exist (i.e., $N_s + N_{mm} + N_{sm} + N_p < N_C$). If there don't exist idle channels or SUs or other SMUs (i.e., $N_{mm} + N_p = N_C$), then the SMU exits. If there doesn't exist idle channel (i.e., $N_s + N_{mm} + N_{sm} + N_p = N_C$), but exist SU (i.e., $N_s \geq 1$) or SMU (i.e., $N_{sm} \geq 1$), then the SMU starts PUEA. Once a SMU gets a channel, it will stop emulating PU and communicate normally as a SU. SMUs usually don't cooperate with each other, as their goal is to maximize own benefit. Therefore, a SMU couldn't know other SMUs' true identification, so cheats and grabs may happen among SMUs. The access probability of SMUs is $(N_C - N_p - N_{mm})\lambda_{sm}$.

b) Leave: If a PU needs transmit data, SMUs will vacate related channels for the same reason as MMUs. And when SMUs send signals as normal SUs, they may be spoofed by MMUs or other SMUs. When the communication demands are met, SMUs will exit channels occupied. The former two probabilities is related to primary communication demands and appearance of MUs, and the third probability is $N_{sm}\mu_{sm}$.

4) PU:

a) Access: If all the channels have already been used by PUs (i.e., $N_p = N_C$), a PU will not access. If not (i.e., $N_p < N_C$), the PU will access, and the probability is $(N_C - N_p)\lambda_p$.

b) Leave: When the PU finish its communication, it will exit the channel, and the probability is $N_p\mu_p$.

5) Other:

a) Handover: When a PU is detected, SUs and MUs will quit current channels immediately, and try to switch another channel to continue unfinished transmissions or attacks. When SUs are cheated by MUs and SMUs are cheated by MMUs, they will exit and switch channels. A successful handover depends upon whether available idle channels and users that can be cheated exist or not.

b) *Equivalent process:* For the case that a current user quits channel Ch_1 and switch channel Ch_2 successfully, we ignore the handover time. Therefore, the above case can be considered as the case that the current user uses Ch_1 still while the grabber uses Ch_2 directly, as we have interests in whether channels are occupied and how many users use the channels, but not who utilize these channels. When $N_s \geq 1$, $N_{sm} \geq 1$ and $N_s + N_{mm} + N_{sm} + N_p = N_C$, if SMUs are forced abandon their channels, they will grab SUs' channels. For the same reason, we can regard this process as that PUs or MMUs grab SUs' channels directly.

3. Performance Analysis

In this section, model characteristic will be analyzed, and communication performance will be evaluated.

3.1. Model Characteristic Analysis

Theorem 1. Let $X(t) = (N_s, N_{mm}, N_{sm}, N_p)$, then stochastic process $\{X(t), t \geq 0\}$ is a continuous time Markov process.

Proof. For N_s、N_{mm}、N_{sm}、$N_p \in [0, N_C]$, and N_C is a constant, so for any signless integral n, the state set of $\{X(t), t \geq 0\}$, i.e., $I = \{i_n = X(t_n), n \geq 0, t_n \geq 0\}$, is a countable set. For any $0 \leq t_n < t_{n+1}$, $X(t_{n+1}) = X(t_n)+$ access number in time $(t_n, t_{n+1}]$- leave number in time $(t_n, t_{n+1}]$. So the user number at moment t_{n+1} is only related with the number at moment t_n, not related with the number at moments before t_n. Therefore, Markov property is met. Let $p_{ij}(s,t) = P\{X(s+t) = j \mid X(s) = i\}$, where $i, j \in I$, $s, t \geq 0$. It's easy to know that transition probabilities only depend on initial state *i*, target state *j*, and consume time t, but have nothing

to do with initial moment s, i.e., $p_{ij}(s,t) = p_{ij}(t)$. Therefore, the process is homogeneous. From the above, it can conclude that $\{X(t), t \geq 0\}$ is a continuous time homogeneous Markov process.

Theorem 2. If $\{X(t), t \geq 0\}$ is positive recurrent, the stationary distribution, $\{P(N_s, N_{mm}, N_{sm}, N_p),\ (N_s, N_{mm}, N_{sm}, N_p) \in I\}$, exists.

Proof. The states of idle channels consist of three cases. The first case is that the total number of idle channels is zero, i.e., $N_s + N_{mm} + N_{sm} + N_p < N_C$, the state transition is shown in Figure 1. The second case is that there has no idle channel but some SUs, i.e., $N_s + N_{mm} + N_{sm} + N_p = N_C$ and $N_s \geq 1$, both of MU and PU can access normally, the state transition is shown in Figure 2. And the third case is that neither of idle channel nor SUs exist, i.e., $N_{mm} + N_{sm} + N_p = N_C$, MMUs can grab SMUs' channels, and PU can grab MUs' channels, this state transition is shown in Figure 3. In conclusion, the theorem is proved.

According to the principles given by Figure 1~3, the state transition figure for $N_C = 2$ is derived as Figure 4. For this homogeneous Markov chain, we can obviously conclude as follows:

i. In Figure 1:

$$\begin{aligned} P(N_s,N_{mm},N_{sm},N_p) &= \lambda_s P(N_s-1,N_{mm},N_{sm},N_p) \\ &+ (N_C-N_p-N_{mm}+1)\lambda_{mm} P(N_s,N_{mm}-1,N_{sm},N_p) \\ &+ (N_C-N_p-N_{mm}+1)\lambda_{sm} P(N_s,N_{mm},N_{sm}-1,N_p) \\ &+ (N_C-N_p+1)\lambda_p P(N_s,N_{mm},N_{sm},N_p-1) \\ &+ (N_s+1)\mu_s P(N_s+1,N_{mm},N_{sm},N_p) + (N_{mm}+1)\mu_{mm} P(N_s,N_{mm}+1,N_{sm},N_p) \\ &+ (N_{sm}+1)\mu_{sm} P(N_s,N_{mm},N_{sm}+1,N_p) + (N_p+1)\mu_p P(N_s,N_{mm},N_{sm},N_p+1) \end{aligned} \quad (1)$$

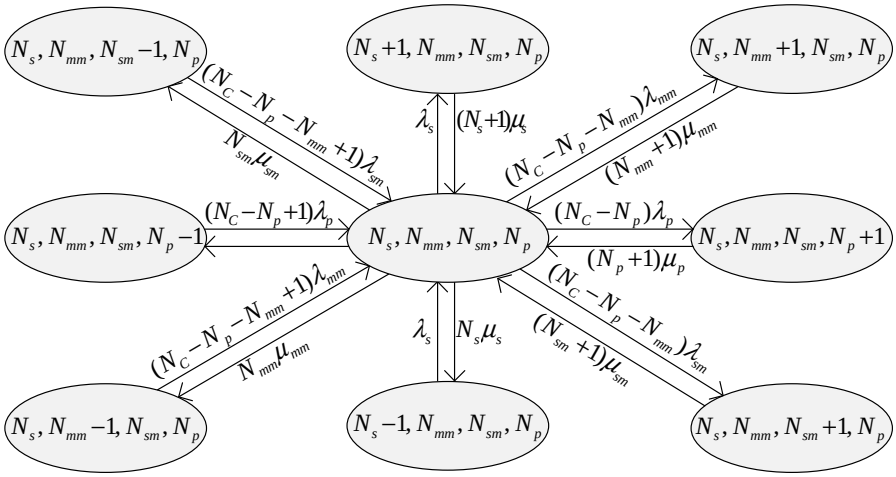

Figure 1. State transition for $N_s + N_{mm} + N_{sm} + N_p < N_C$

i. In Figure 2:

$$\begin{aligned} P(N_s,N_{mm},N_{sm},N_p) &= \lambda_s P(N_s-1,N_{mm},N_{sm},N_p) \\ &+ (N_C-N_p-N_{mm}+1)\lambda_{mm} P(N_s,N_{mm}-1,N_{sm},N_p) \\ &+ (N_C-N_p-N_{mm}+1)\lambda_{sm} P(N_s,N_{mm},N_{sm}-1,N_p) \\ &+ (N_C-N_p+1)\lambda_p P(N_s,N_{mm},N_{sm},N_p-1) \end{aligned} \quad (2)$$

ii. In Figure 3:

$$\begin{aligned} P(N_s,N_{mm},N_{sm},N_p) &= (N_C - N_p - N_{mm} + 1)\lambda_{mm} P(N_s,N_{mm}-1,N_{sm},N_p) \\ &+ (N_C - N_p - N_{mm} + 1)\lambda_{sm} P(N_s,N_{mm},N_{sm}-1,N_p) \\ &+ (N_C - N_p + 1)\lambda_p P(N_s,N_{mm},N_{sm},N_p - 1) \end{aligned} \quad (3)$$

iii. In Figure 4:

$$\sum_{(N_s,N_{mm},N_{sm},N_p)\in I} P(N_s,N_{mm},N_{sm},N_p) = 1 \quad (4)$$

As shown above, $P(N_s,N_{mm},N_{sm},N_p)$ can be derived from (1)-(4) for any $(N_s,N_{mm},N_{sm},N_p)\in I$.

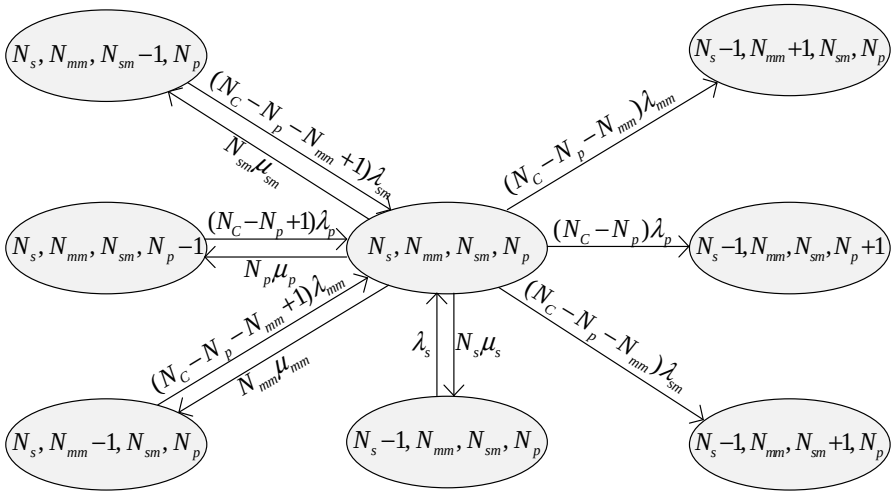

Figure 2. State transition for $N_s + N_{mm} + N_{sm} + N_p = N_C$ and $N_s \geq 1$

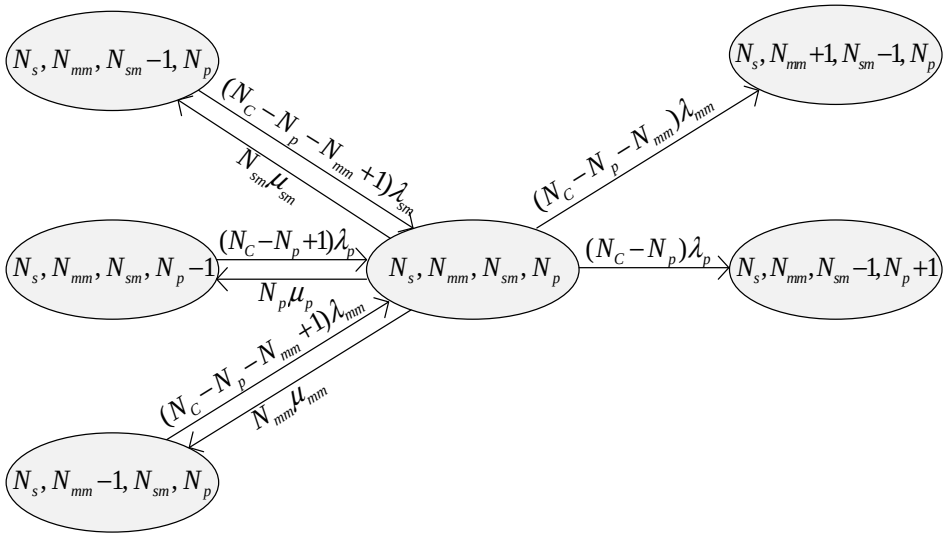

Figure 3. State transition for $N_{mm}+N_{sm}+N_p=N_C$

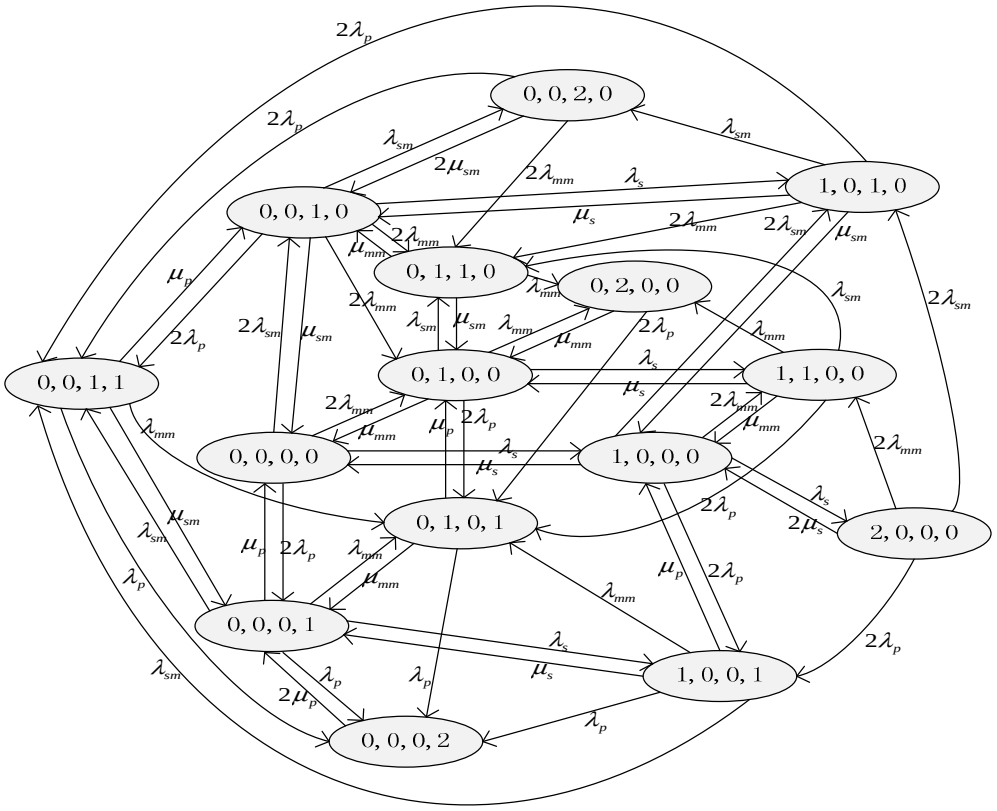

Figure 4. State transition for $N_C = 2$

3.2. Communication Performance Evaluation for SUs

In order to evaluate different kinds of PUEA detection schemes, following performance variables are defined:

Blocking rate of a SU, p_b:

If a SU needs to communicate but there is no idle channel, then it's blocked. The blocking rate can be obtained by

$$p_b = \sum_{N_s=0}^{N_C} \sum_{N_{mm}=0}^{N_C} \sum_{N_{sm}=0}^{N_C} \sum_{N_p=0}^{N_C} [P(N_s, N_{mm}, N_{sm}, N_p) \cdot \gamma(N_s + N_{mm} + N_{sm} + N_p = N_C)] \quad (5)$$

in which $\gamma(N_s + N_{mm} + N_{sm} + N_p = N_C)$ satisfies that

$$\gamma = \begin{cases} 1, & N_s + N_{mm} + N_{sm} + N_p = N_C \\ 0, & N_s + N_{mm} + N_{sm} + N_p < N_C \end{cases} \quad (6)$$

iv. Dropping rate of a SU, p_d:

Because of evading PUs or spoofed by MUs, a SU has exited from the former channel. If it cannot get a new idle channel, then it will leave the system and the former SU communication is disrupted. The dropping probability can be obtained by:

$$\begin{aligned} p_d = & \frac{(N_C - N_p)\lambda_p + (N_C - N_p - N_{mm})(\lambda_{mm} + \lambda_{sm})}{\lambda_s + (N_C - N_p)\lambda_p + (N_C - N_p - N_{mm})(\lambda_{mm} + \lambda_{sm})} \\ & \cdot \sum_{N_s=1}^{N_C} \sum_{N_{mm}=0}^{N_C} \sum_{N_{sm}=0}^{N_C} \sum_{N_p=0}^{N_C} [P(N_s, N_{mm}, N_{sm}, N_p) \gamma(N_s + N_{mm} + N_{sm} + N_p = N_C)] \end{aligned} \quad (7)$$

v. Detection factor, p_{detect}, and PUEA success factor, p_{PUE}:

In actual system, PU detection by SUs may be affected by various factors, which will result in that the detection cannot succeed every time. Therefore, a detection factor, p_{detect}, is utilized to perfect (5) and (7), in which λ_p is replaced by $p_{\text{detect}}\lambda_p$, and the value of p_{detect} is designed as actual demands. Similarly, the actual PUEA cannot all succeed, especially when the system has PUEA detection schemes. PUEA success factor, p_{PUE}, is used as $p_{\text{PUE}}\lambda_{mm}$ and $p_{\text{PUE}}\lambda_{sm}$ to replace λ_{mm} and λ_{sm} in (5) and (7), respectively. Under the same condition, $(1-p_{\text{PUE}})$ is used to describe PUEA detection schemes. And if there is no PUEA, i.e., $\lambda_{mm}=\lambda_{sm}=0$ and $\mu_{mm}=\mu_{sm}=0$, then $p_{\text{detect}}=p_{\text{PUE}}=0$。

vi. Affection factor of SMUs, μ_{sm}:

SMUs will initiate attacks when there is no idle channel, i.e., $\gamma=1$. And when there has some idle channels, SMUs won't initiate attacks. Therefore, the blocking probability of SUs because of SMUs, p_b^{sm}, can be obtained as $p_b^{sm}=p_b\cdot\frac{N_{sm}}{N_{mm}+N_{sm}}$. As the same reason, the dropping probability of SUs because of PUEA from SMUs, p_d^{sm}, is derived by $p_d^{sm}=p_d\cdot\frac{N_{sm}}{N_{mm}+N_{sm}}$. Let $\mu_{sm}=\frac{N_{sm}}{N_{mm}+N_{sm}}$, where μ_{sm} represents the performance affection factor of SMUs to SUs.

4. Simulation Result

We assume that $\lambda_p=1$ per hour, $\lambda_s=600$ per hour, $1/\mu_p=24$s, $1/\mu_s=36$s, $N_{mm}=30$, $\zeta_{sm}=0.4$, $\lambda_m=\lambda_{mm}+\lambda_{sm}=150$ per hour, $1/\mu_{mm}=80$s, and $\mu_{sm}=\mu_s$ for simulation.

The blocking and dropping rates of SUs varying with channel increase in three conditions are shown in Figure 5~6. The three conditions are PUEAs do not exist, MMUs exist but SMUs do not exist, both MMUs and SMUs exist. We compare the SUs' dropping rates varying with the increasing number of PUEAs for no PUEA, PUEAs exist but no PUEA detection scheme, both PUEAs and independent PUEA detection scheme [11] exist, independent PUEA detection scheme including SMU test [12], cooperative PUEA detection scheme [13], cooperative PUEA detection scheme including SMU test [12-14] in the condition of $N_C=10$. The results are given in Figure 7.

It is observed from Figure 5 that the theoretical and experimental curves are almost alike, which prove that the blocking analysis proposed is reasonable. We can see that when there is no PUEA, the blocking rate is not equal to zero, for that once all channels are occupied by PUs and SUs, another SU couldn't access. When the available channels is less than 6, PUEAs affect the blocking rates heavily, and when the channel number becomes larger, the rate curves go down. Especially when $N_C>12$, p_b is close to zero. Similarly, when the channel number is small, p_b is affected seriously by SMUs. The blocking rate for the condition which SMUs exist in is nearly 80 percent larger than that for the condition which only MMUs exist in.

Figure 6 displays that the drop computing method proposed is valid. And when all the channels are occupied, if a PU appears, then a SU will quit immediately, which will result in the SU interrupted even there is no PUEA. When the idle channel number, N_c, is less than 5, the dropping rates grow with the increasing channels. This is because that the channel number is so small to meet SUs' communication demands, the slightly increasing channels are occupied shortly, and once PUEAs come, many SUs will be forced to switch channels. But at this moment, for the channels total number is small, it's difficult that idle channels exist, which will cause many drops. When $N_C>5$, the SUs switching demands are met, so the dropping rates decline, and when $N_C>16$, the p_d curves are close to zero. It's obvious that SMUs affect SUs seriously, especially when the channel number is small. SMUs' selfish behaviors will interfere with normal SUs' communication, therefore, the researches on SMU detection is necessary.

Figure 7 shows that the performances of various PUEA detection schemes are of very difference. With λ_m growing, the dropping rates for SUs go up rapidly. Note that cooperative schemes can reduce the affection of PUEAs and the SMU testing scheme are important, which can improve the PUEA detection scheme for 40 percent when $\lambda_m < 160$. The experimental result agrees with $\zeta_{sm} = 0.4$. When attacks strength is strong, the SMU testing scheme's affection is not obvious.

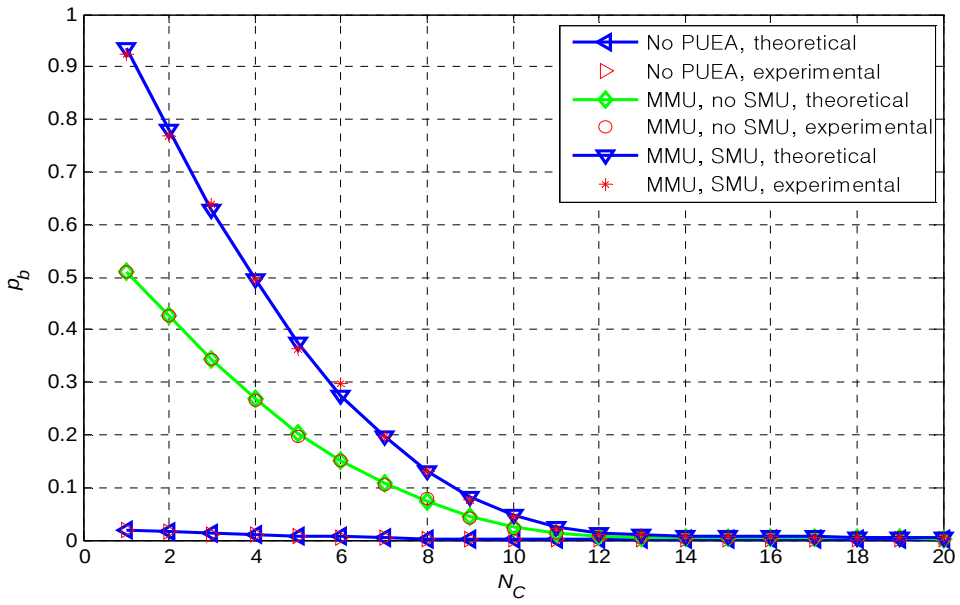

Figure 5. Blocking rates vary in three conditions

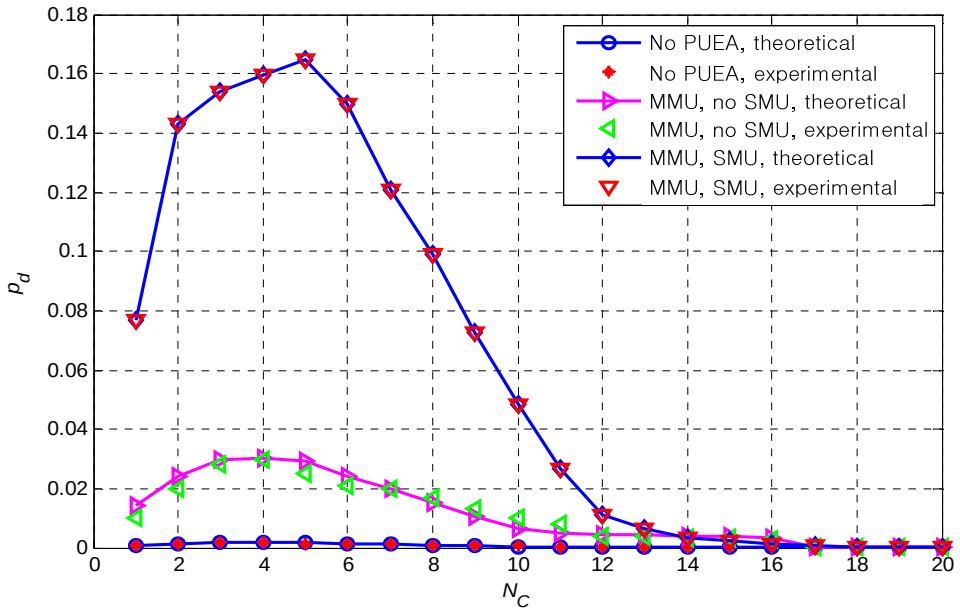

Figure 6. Dropping rates vary in three conditions

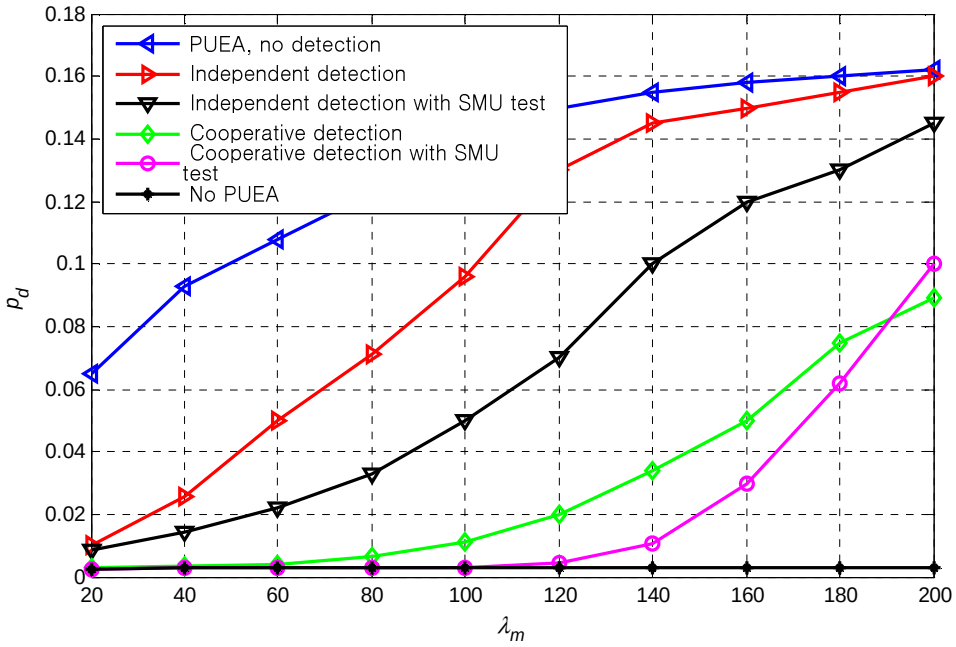

Figure 7. Different PUEA detection schemes comparison

5. Conclusion

This paper studies on the communication analysis of SUs for CRN under PUEA. And we proposed a FDMC analysis model, which has considered four parameters, i.e., PU amount, SU amount, MMU amount and SMU amount. States and varieties of the four parameters are also described in detail. The blocking and dropping rates of SU under PUEA are derived. Several PUEA detection schemes are simulated for comparison. The results depicted that the SMU test is of very importance for PUEA detection, which can decrease blocking and dropping rates greatly.

Acknowledgement

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

References

[1] J Mitola, GQ Maguire. Cognitive Radio: Making Software Radios More Personal. *IEEE Personal Communication Magazine*. 1999; 6(4): 13-18.
[2] Federal Communications Commission. *Notice of Proposed Rule Making and Order: Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies.* USA FCC. 2005; Report number: 03-108.
[3] Nicola Baldo, Alfred Asterjadhi, Lorenza Giupponi, Michele Zorzi. *A Scalable Dynamic Spectrum Access Solution for Large Wireless Networks*. 5th IEEE International Symposium on Wireless Pervasive Computing. Palazzo Estense Modena. 2010: 430-435.
[4] Baldini G, Sturman T, Biswas A, Leschhorn R, Godor G, Street M. Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead. *IEEE Communications Surveys & Tutorials.* 2011; 7(3): 1-25.
[5] Z Jin, S Anand, KP Subbalakshmi. *Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks*. International Conference on Communications. Dresden. 2009: 1-5.
[6] Yao Liu, Peng Ning, Huaiyu Dai. *Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures*. IEEE Symposium on Security and Privacy. Oakland. 2010: 286-301.

[7] Z Jin, S Anand, KP Subbalakshmi. *Performance Analysis of Dynamic Spectrum Access Networks under Primary User Emulation Attacks*. IEEE Global Communications Conference, Exhibition & Industry Forum. Miami. 2010: 1-5.
[8] Ruiliang Chen, Jung-Min Park, Y Thomas Hou, et al. Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks. *IEEE Communications Magazine.* 2008; 46(4): 50-55.
[9] Li Zhang, Guoxin Zheng. Reliable Information Transmission: A Chaotic Sequence based Authentication Scheme for Radio Environment Maps Enabled Cognitive Radio Networks. *International Journal of Digital Content Technology and its Applications*. 2010; 4(4): 48-57.
[10] S Anand, Z Jin, KP Subbalakshmi. *An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks*. IEEE International Symposium on Dynamic Spectrum Access Networks. Chicago. 2008: 1-6.
[11] Md Shamim Hossain, Md Ibrahim Abdullah, Mohammad Alamgir Hossain. Hard Combination Data Fusion for Cooperative Spectrum Sensing in Cognitive Radio. *International Journal of Electrical and Computer Engineering.* 2012; 2(6): 811-818.
[12] Wenkai Wang, Husheng Li, Yan (Lindsay) Sun, Zhu Han. Research Article Securing Collaborative Spectrum Sensing against Untrustworthy Secondary Users in Cognitive Radio Networks. *EURASIP on Advances in Signal processing.* 2010; 4(1): 1-15.
[13] Chao Chen, Hongbing Cheng, Yu-Dong Yao. Cooperative Spectrum Sensing in Cognitive Radio Networks in the Presence of the Primary User Emulation Attack. *IEEE Transactions on Wireless Communications*. 2011; 10(7): 2135-2141.
[14] Dengyin Zhang, Kuankuan Li, Li Xiao. An Improved Cognitive Radio Spectrum Sensing Algorithm. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2013; 11(2): 583-590.