# Detecting the Greedy Spectrum Occupancy Threat in Cognitive Radio Networks

Songjun Ma[†], Yunfeng Peng[‡], Tao Wang[§], Xiaoying Gan[†], Feng Yang[†], Xinbing Wang[†], Mohsen Guizani[§§]
[†]Dept. of Electronic Engineering, Shanghai Jiao Tong University, China
[‡]Antai College of Economics and Management, Shanghai Jiao Tong University, China
[§]CECA, School of EECS, Peking University, China
[§§]Qatar University, Doha, Qatar
Email: {masongjun, pengyf, ganxiaoying, yangfeng, xwang8}@sjtu.edu.cn, wangtao@pku.edu.cn[§], mguizani@ieee.org[§§]

***Abstract*—Recently, security of cognitive radio (CR) is becoming a severe issue. There is one kind of threat, which we call greedy spectrum occupancy threat (GSOT) in this paper, has long been ignored in previous work. In GSOT, a secondary user may selfishly occupy the spectrum for a long time, which makes other users suffer additional waiting time in queue to access the spectrum and leads to congestion or breakdown. In this paper, a queueing model is established to describe the system with greedy secondary user (GSU). Based on this model, the impacts of GSU on the system are evaluated. Numerical results indicate that the steady-state performance of the system is influenced not only by average occupancy time, but also by the number of users as well as number of channels. Since a sudden change in average occupancy time of GSU will produce dramatic performance degradation, the greedy second user prefers to increase its occupancy time in a gradual manner in case it is detected easily. Once it reaches its targeted occupancy time, the system will be in steady state, and the performance will be degraded. In order to detect such a cunning behavior as quickly as possible, we propose a wavelet based detection approach. Simulation results are presented to demonstrate the effectiveness and quickness of the proposed approach.**

## I. Introduction

Cognitive Radio (CR) is a promising technology that relieves spectrum shortage problem, and there are many works focus on this topic during these years [1]–[5]. However, the security issues of CR cannot be neglected. These issues have received increasingly attention recently. Surveys about it can be found in [6]. Ever since the security of CRN has been paid attention, there has been a large number of works focus on two kinds of attack, i.e. primary user emulation [7]–[9] and false report in cooperative spectrum sensing [10]–[13].

But there is another threat in cognitive radio networks (CRN) that must never be ignored, which we call **Greedy Spectrum Occupancy Threat (GSOT)**. In CRN, if there are more secondary users than available channels, a problem may arise. Secondary users have to queue to access the channels. So they are supposed to immediately release the channels when they finish transmission. Thus, users behind would have the opportunities to access the networks. However, a smart GSU may find out the truth that if it vacates the channel, it would queue again when its next transmission task comes. This user is not willing to bear long-time waiting. So it comes up with a strategy. It occupies the channel for a longer time in case it has another communication demand during this period. The greedy behavior would degrade the performance of CRN, i.e. additional waiting time for normal secondary users (NSUs) and congestion for the system. What's worse, suppose the user is not only a GSU but also a malicious one, the networks can be attacked by means of long term occupancy in an intentional manner. Such attack poses great threat to the system, and lead to breakdown of the networks. This threat, to some extend, is similar with Denial of Service (DoS) attack in computer networks. Both of them target to exhaust the resources.

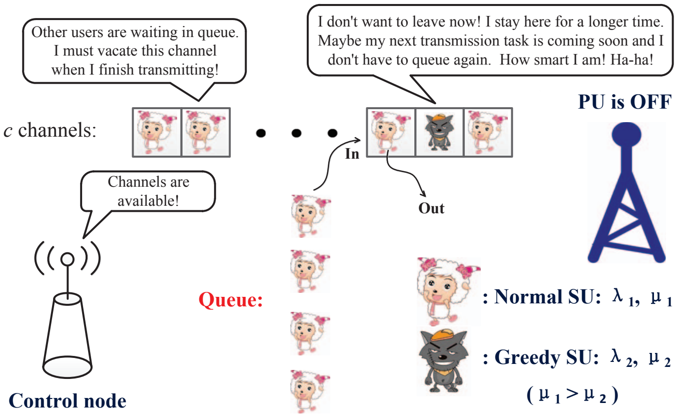

Other users are waiting in queue. I must vacate this channel when I finish transmitting!
I don't want to leave now! I stay here for a longer time. Maybe my next transmission task is coming soon and I don't have to queue again. How smart I am! Ha-ha!
PU is OFF
c channels:
In
Out
Channels are available!
Queue:
Control node
: Normal SU: λ 1, μ 1
: Greedy SU: λ 2, μ 2
( μ 1 > μ 2 )

Fig. 1: An illustration of the greedy spectrum occupancy threat to CRN.

The GSU can be very intelligent that it stealthy and deliberately increases the occupancy time in a slow pace, which makes naive central control node get used to this slow change gradually and makes it difficult to discover anomalous user. Once it reaches its targeted occupancy time without discovered, the system would be in steady state and other users would have to be subjected to long-term negative influence.

To the best knowledge of us, there is little study on greedy spectrum occupancy threat in cognitive radio networks. In reference [14], the authors presented a kind of selfish attack which enabled selfish attackers to occupy all or a part of the available channels. Although both of us defined selfish or greedy occupancy threats, the two threats are different from each other. That is because in [14], selfish user attacked networks by sending fake PU (primary user) signals or broadcasting fake channel allocation information. These

978-1-4799-2003-7/14/$31.00 ©2014 IEEE

attacks, actually, are similar with PUE attack and false report attack in cooperative sensing respectively, and are totally different from our threat model. Nevertheless, the greedy spectrum occupancy is indeed a critical threat in CRN which is necessary to be studied.

In this paper, we treat this CRN as a queueing system. The queueing process is established through state-transition-rate diagrams. We analyze the steady-state performance of the system using average queue size and waiting time. Three factors, which are average occupancy time of GSU, number of channels and number of users, are taken into account to investigate impacts of GSU on the system. In order to detect the stealthy threat as quickly as possible, we propose a detection strategy based on wavelet. Wavelet transform is used in signal processing traditionally, and has been confirmed that it applies to detecting similar threat in [15].

## II. System Model

### A. CRN model without GSU

The system is illustrated in Fig.1. It contains $m$ secondary users and $c$ licensed channels, where $m > c$. We assume all of the channels are identical. A centralized system is considered, where there is a control node which manages the spectrum access. When channels are not occupied by primary users, control node would notify the SUs. SUs who need to transmit information queue up to use the resources in sequence. After finishing transmission, SU vacates the channel. And the first one in queue replaces it. When this retiring user wants to access network again, it is supposed to queue again.

We model the traffic as two Poisson processes. The arrival traffic of each second user is modeled as a Poisson process with average arrival rate $\lambda_1$. That is to say, interval time of adjacent arrival is negative-exponentially distributed with expectation $1/\lambda_1$. Similarly, departure of each user is modeled as the same process with average service rate $\mu_1$.

### B. Threat model

We model the traffic of GSU as Poisson processes. The arrival traffic is modeled as a Poisson process with service rate $\lambda_2$, and departure is modeled as a Poisson process with service rate $\mu_2$, where $\mu_2$ should be lesser than $\mu_1$ (Fig. 1).

A sudden change in $\mu_2$ would cause an obviously performance degradation, and the control node can easily detect the threat. So the smart GSU comes up with a stealthy strategy that increases the average occupancy time in a slow pace. We assume the strategy is launched by GSU who starts its greedy behavior with an initial mean occupancy duration $t_s^0 = 1/\mu_1$, which is same with that of NSUs. Then it periodically increases current average occupancy time slowly following $t_s^n = t_s^{n-1} + \Delta t$, where $\Delta t$ is the increment of mean occupancy time at each variation period. We assume the GSU holds mean occupancy duration in the period of every $N$ access times. The GSU can take a large $N$ and small $\Delta t$ to obtain long term benefit as well as hide its greedy behavior. Since the greedy behavior produces adverse impacts on system performance gradually, a quick detection is of badly need. And as GSU is usually minority, for simplicity, we assume there is 1 greedy user in the system.

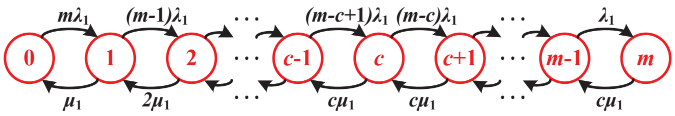


Fig. 2: State-transition-rate diagram for the system with no greedy user.

## III. Queueing Analysis

### A. Queueing Modeling

We assume there are $m$ secondary users and $c$ idle channels. Thus, it is an **M/M/c/m/m** queueing system.

*1) System without GSU:* Number of users *in queue and under service* (IQ&US) is regarded as the state of the system. The state-transition-rate diagram is established as Fig.2. Probabilities of steady state are calculated as [16]

$$P_j = \begin{cases} (\frac{\lambda_1}{\mu_1})^j \binom{m}{j} P_0, & 0 \le j \le c \\ P_j = (\frac{\lambda_1}{\mu_1})^j \binom{m}{j} \frac{j!}{c!} c^{c-j} P_0, & c+1 \le j \le m. \end{cases} \tag{1}$$

Moreover, the sum of each steady state equals 1. Therefore, all of the steady-state probabilities can be obtained.

*2) System with GSU:* The state-transition-rate diagram that characterizes this scenario is depicted in Fig.3. The existence of GSU makes state transition of the queueing system more complex. Whether there is GSU IQ&US and which position is the GSU located in the queue pose significant influence on the queue system. Each state is denoted as ($k_1$,$k_2$,$k_3$). $k_1$ indicates how many users (including NSUs and GSU) are IQ&US. $k_2$ implies whether the GSU is IQ&US, where $k_2$ equals 0 or 1. $k_2 = 0$ means GSU is not IQ&US and otherwise, $k_2 = 1$. The value of $k_3$ depends on the value of $k_2$. When $k_2 = 0$, $k_3$ can only be valued as 0. If $k_2 = 1$, $k_3$ represents the location the GSU at, and it can be valued from 0 to $m - c$. That $k_3$ is valued from 1 to $m - c$ indicates which position is the GSU located in the queue. When $k_3 = 0$ and $k_2 = 1$, it implies that the GSU is under service.

In Fig.3, arrowed segment represents state-transition direction. And each segment is tagged transition intensity. The vertical dashed lines which connect states of row 1 and that of row 0 also indicates state-transition direction. We call the system is at state $(x, y)$ if the state is at row $x$ and column $y$.

Based on this diagram, we can compose a transition intensity matrix $\mathbf{A}$. Then, we have $\mathbf{\Pi A} = \mathbf{0}$, where $\mathbf{\Pi}$ is the steady-state probability vector contains all of the states.

### B. Average Waiting Time and Queueing Size

In queueing analysis, we intend to find out how the GSU degrades performance of the systems. Average waiting time and average queueing size are good indicators of performance.

*1) System without GSU:* Average queue size is:

$$\bar{N}_q = \sum_{j=c}^{m} (j - c) P_j. \tag{2}$$

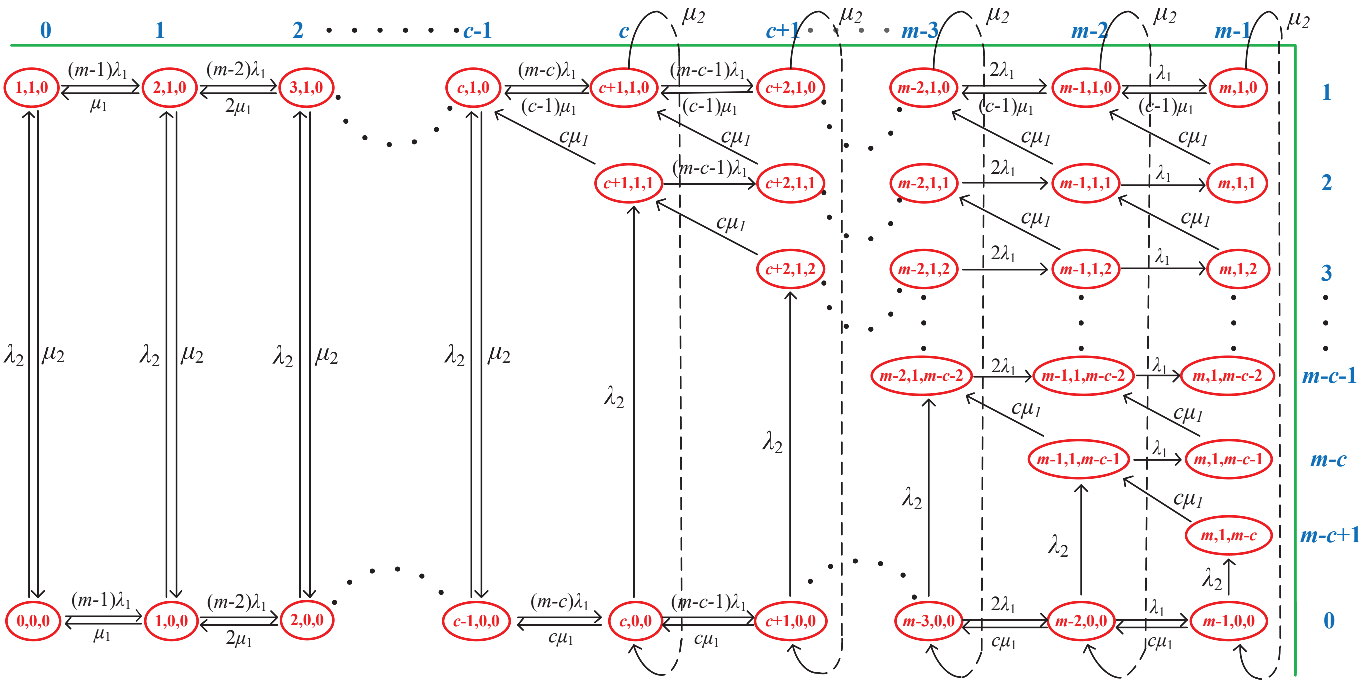


Fig. 3: State-transition-rate diagram for system with one greedy user.

In order to obtain the average waiting time, we first give the following lemma. And we omit proof due to limited space.

***Lemma* 1.** *Let $P_j^-$ represent there has been $j$ users IQ&US when a user is going to join the queue. Then we have [17]*

$$P_j^- = \frac{m-j}{m-\bar{N}} P_j, \ j = 0, 1, 2, \cdots, m-1, \tag{3}$$

*where $\bar{N}$ is average number of users IQ&US.*

The average waiting time in queue follows:

$$\bar{W}_q = \sum_{j=c}^{m-1} \frac{j-c+1}{c\mu_1} P_j^- . \tag{4}$$

*2) System with GSU:* Average queue size is computed as:

$$\begin{aligned}\bar{N}_q = &\sum_{j=c+1}^{m-1} P_{(0,j)}(j-c) + \sum_{j=c}^{m-1} P_{(1,j)}(j-c+1) \\ &+ \sum_{i=2}^{m-c+1} \sum_{j=i+c-2}^{m-1} P_{(i,j)}(j-c+1),\end{aligned} \tag{5}$$

where $P_{(0,j)}$, $P_{(1,j)}$ and $P_{(i,j)}$ represent steady-state probabilities in Fig.3. When calculating the average waiting time, there are 4 different cases to be considered: 1) case 1, there is no GSU IQ&US and an NSU is going to join the queue; 2) case 2, there is no GSU IQ&US and a GSU is going to join the queue; 3) case 3, there is a GSU under service and an NSU is going to join the queue; 4) case 4, there is a GSU in queue and an NSU is going to join the queue.

We derive each case's averaging waiting time and we obtain:

$$\begin{aligned}PA = &\sum_{i=0}^{m-2} P_{(0,i)}(m-1-i)\lambda_1 + \sum_{i=0}^{m-1} P_{(0,i)}\lambda_2 \\ &+ \sum_{i=0}^{m-2} P_{(1,i)}(m-1-i)\lambda_1 \\ &+ \sum_{i=2}^{m-c} \sum_{j=i+c-2}^{m-2} P_{(i,j)}(m-1-j)\lambda_1,\end{aligned} \tag{6}$$

*case* 1:

$$P_{(0,j)(1)}^- = \frac{P_{(0,j)}(m-1-j)\lambda_1}{PA}, \tag{7}$$

$$\bar{W}_{q(1)} = \sum_{j=c}^{m-2} \frac{j-c+1}{c\mu_1} P_{(0,j)(1)}^-, \tag{8}$$

*case* 2:

$$P_{(0,j)(2)}^- = \frac{P_{(0,j)}\lambda_2}{PA}, \tag{9}$$

$$\bar{W}_{q(2)} = \sum_{j=c}^{m-2} \frac{j-c+1}{c\mu_1} P_{(0,j)(2)}^-, \tag{10}$$

*case* 3:

$$P_{(1,j)(3)}^- = \frac{P_{(1,j)}(m-1-j)\lambda_1}{PA}, \tag{11}$$

$$\bar{W}_{q(3)} = \sum_{j=c-1}^{m-2} T_1 P_{(0,j)(3)}^-, \tag{12}$$

where

$$T_{j(1)} = \begin{cases} \frac{1}{a}, & j = c-1 \\ u_{j(1)} + vT_{(j-1)(1)}, & j \geq c, \end{cases} \tag{13}$$

$$u_{j(1)} = \frac{1}{a} + \frac{(j-c+1)\mu_2}{ac\mu_1},\ v = 1 - \frac{\mu_2}{a}, \tag{14}$$

$$a = (c-1)\mu_1 + \mu_2, \tag{15}$$

*case* 4:

$$P^-_{(i,j)(4)} = \frac{P_{(i,j)}(m-1-j)\lambda_1}{PA}, \tag{16}$$

$$\bar{W}_{q(4)} = \sum_{i=2}^{m-c} \sum_{j=i+c-2}^{m-2} (\frac{i-1}{c\mu_1} + T_2)P^-_{(i,j)(4)}, \tag{17}$$

where

$$T_{j(2)} = \begin{cases} \frac{1}{a}, & j = i+c-2 \\ u_{j(1)} + vT_{(j-1)(2)}, & j \geq i+c-1 \end{cases} \tag{18}$$

$$u_{j(2)} = \frac{1}{a} + \frac{(j-i-c+2)\mu_2}{ac\mu_1},\ v = 1 - \frac{\mu_2}{a}. \tag{19}$$

$P^-_{(0,j)(1)}$, $P^-_{(0,j)(2)}$, $P^-_{(1,j)(3)}$, $P^-_{(i,j)(4)}$ are derived with similar approach in the proof of Lemma 1. And average waiting time in queue $\bar{W}_q = \bar{W}_{q(1)} + \bar{W}_{q(2)} + \bar{W}_{q(3)} + \bar{W}_{q(4)}$.

## IV. Quick Detection Scheme

A simple and intuitive idea of discovering threat is to check the variation of the average occupancy time of each user. If one of the user's average occupancy time grows, a GSU is possible in the system. However, GSU's attack behavior we proposed is unnoticeable. The simple and intuitive idea is not efficient, which will be demonstrated in Section V. In order to quickly identify abnormality in system, we leverage wavelet analysis due to its sensitivity to slight change. 1-level Daub4 [18] transform in Discrete Wavelet Transform (DWT) is introduced in this paper. It is a simple and effect approach for detecting gradual changed signal confirmed in [15] by comparing Daub4 approach with Hellinger distance (HD) approach.

The average occupancy time of $j$-th user in a certain time period is denoted by $S_j$. Then the input sampling signal $S$ is defined as $(S_1, S_2, ..., S_l)$. Daub4 decompose $S$ into an approximation subsignal $A$ and a detail subsignal $D$. We examine the ratio of energy corresponding to $D$ for detection. The scaling numbers in Daub4 are shown as belows:

$$\alpha_1 = \frac{1+\sqrt{3}}{4\sqrt{2}},\ \alpha_2 = \frac{3+\sqrt{3}}{4\sqrt{2}},\ \alpha_3 = \frac{3-\sqrt{3}}{4\sqrt{2}},\ \alpha_4 = \frac{1-\sqrt{3}}{4\sqrt{2}}. \tag{20}$$

With these scaling numbers, we obtain scaling signals:

$$\begin{aligned} \mathbf{V}_1 &= (\alpha_1, \alpha_2, \alpha_3, \alpha_4, 0, 0, ..., 0) \\ \mathbf{V}_2 &= (0, 0, \alpha_1, \alpha_2, \alpha_3, \alpha_4, 0, 0, ..., 0) \\ &\vdots \\ \mathbf{V}_{l/2-1} &= (0, 0, ..., 0, \alpha_1, \alpha_2, \alpha_3, \alpha_4) \\ \mathbf{V}_{l/2} &= (\alpha_3, \alpha_4, 0, 0, ..., 0, \alpha_1, \alpha_2). \end{aligned} \tag{21}$$

The wavelet numbers are related to the scaling numbers by equations: $\beta_1 = \alpha_4, \beta_2 = -\alpha_3, \beta_3 = \alpha_2, \beta_4 = -\alpha_1$. Daub4 wavelets follows:

$$\begin{aligned} \mathbf{W}_1 &= (\beta_1, \beta_2, \beta_3, \beta_4, 0, 0, ..., 0) \\ \mathbf{W}_2 &= (0, 0, \beta_1, \beta_2, \beta_3, \beta_4, 0, 0, ..., 0) \\ &\vdots \\ \mathbf{W}_{l/2-1} &= (0, 0, ..., 0, \beta_1, \beta_2, \beta_3, \beta_4) \\ \mathbf{W}_{l/2} &= (\beta_3, \beta_4, 0, 0, ..., 0, \beta_1, \beta_2). \end{aligned} \tag{22}$$

Then, we have

$$A_j = \sum_{i=1}^{\frac{l}{2}} (\sum_{k=1}^{l} S_k V_{i(k)}) V_{i(j)},\ j \in \{1, 2, ..., l\}, \tag{23}$$

$$D_j = \sum_{i=1}^{\frac{l}{2}} (\sum_{k=1}^{l} S_k W_{i(k)}) W_{i(j)},\ j \in \{1, 2, ..., l\}, \tag{24}$$

which are named approximation signal and detail signal respectively. The ratio of energy corresponding to $D$ is

$$r^d = \frac{\sum_{j=1}^{l} (D_j)^2}{\sum_{j=1}^{l} (A_j)^2 + \sum_{j=1}^{l} (D_j)^2}. \tag{25}$$

When there is no GSU, the system operates in a steady way, and $r^d$ keeps low. Once a user becomes greedy, $r^d$ will have a rapid increase. That makes it possible to discover whether there is a GSU.

A threshold $h$ is required to be determined. If $r^d$ is greater than $h$, the system is assumed to be affected by the GSU and otherwise, there is no GSU. We define a dynamic threshold through Exponential Weighted Moving Average (EWMA) in a similar way of reference [19].

As is defined in EWMA, $R^d_{n+1} = (1-\alpha)R^d_n + \alpha r_n$, where $R^d_{n+1}$ and $R^d_n$ represent estimation value $r^d$ of current and next detection round. Let $s_n$ measure how much the estimated value $R^d_n$ deviates from the actual value $r_n$, i.e. $s_n = \left|R^d_n - r_n\right|$.

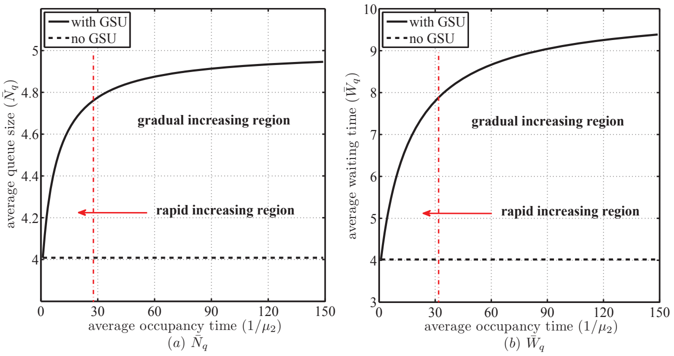
And we estimate deviations $S_{n+1}$ as follows:

$$S_{n+1} = (1-\beta)S_n + \beta s_n. \tag{26}$$

Then the estimate threshold is defined by

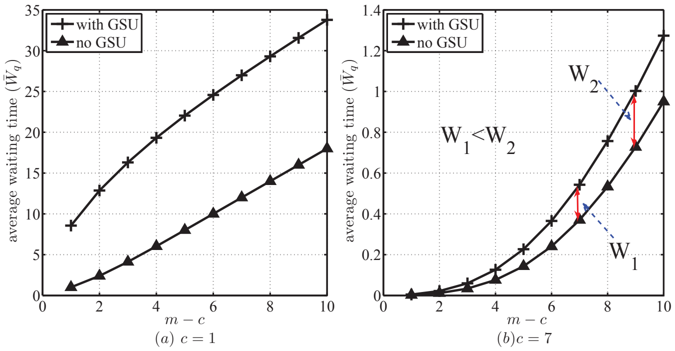
$$R^{Th}_{n+1} = \lambda R^d_n + \mu S_n. \tag{27}$$

$\alpha$, $\beta$, $\lambda$ and $\mu$ are alterable parameters. Meanwhile, we fix



$(a)$ $\bar{N}_q$ $(b)$ $\bar{W}_q$

Fig. 4: Average queue size and average waiting time versus average occupancy time of GSU.



$(a)$ $c = 1$ $(b)c = 7$

Fig. 5: Average waiting time $\bar{W}_q$ versus number of users $m$ with different number of channels $c$.

the threshold once $r^d$ is greater than it until $r^d$ reaches below the threshold again.

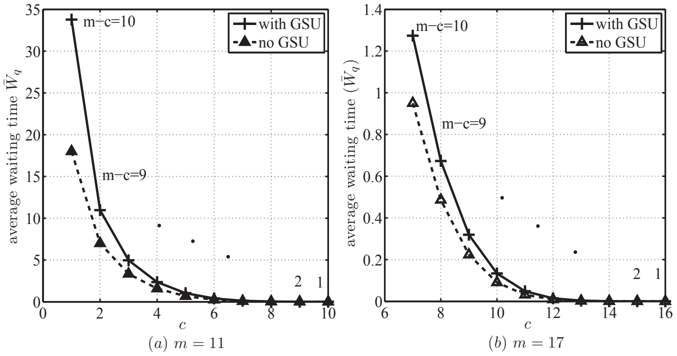
## V. Simulation Results

### A. *Performance Degradation with GSU*

In this subsection, we present simulation results for performance of the system with GSU. It is evaluated by average queue size and waiting time in queue. The data is analyzed through Matlab. We set average and departure traffic of each NSU to 0.5 (i.e. $\lambda_1 = 0.5$, $\mu_1 = 0.5$).

*1) Occupancy Time of GSU:* We first study how occupancy time of GSU influences the system. Fig.4 reflects average queue size $\bar{N}_q$ and waiting time $\bar{W}_q$ versus $1/\mu_2$ respectively, where $1/\mu_2$ varies from 2 to 150. It is easy to understand that $\bar{N}_q$ and $\bar{W}_q$ grow with increase of $1/\mu_2$. However, we can find out that in rapid increasing region, the values rise rapidly, but they increase gradually in gradual increasing region. An explanation of this is that if the average occupancy time is long enough (i.e. in gradual increasing region), one of the channels can be viewed as exclusive channel of GSU, and other users have little chance to access this channel. This makes NSUs use other channels with a relatively high probability, and the average waiting time remains nearly stable when $1/\mu_2$ grows.

Comparing these two figures, we discover that the curve of average queue size and waiting time follows similar trend. However, the average waiting time is more susceptible to the increasing $1/\mu_2$ than average queue size.



$(a)$ $m = 11$ $(b)$ $m = 17$

Fig. 6: Average waiting time $\bar{W}_q$ versus number of channels $c$ with different number of users $m$.

TABLE I: $r^d$ and $\bar{t}$ around the moment the threat is injected.

| period | 38 | 39 | 40 | dp |
|---|---|---|---|---|
| $r^d(\times 10^{-3})$ | 0.0181 | 0.0059 | 0.0070 | 1.1 |
| $\bar{t}$ | 2.2520 | 2.1765 | 1.8606 | 6.2032 |

*2) Number of users and channels:* Fig. 5 illustrates the variation tendency of average waiting time in accordance with number of users $m$. When there is only 1 available channel (Fig. 5 (a)), the trend of $\bar{W}_q$ is like a straight line, while when $c$ is bigger (Fig. 5 (b)), $\bar{W}_q$ grows in an exponent-like trend. When observing these two figures, we find that the difference between $\bar{W}_q$ in case with GSU and that in case without GSU increases with $m$ growing, and When $m$ is larger, the rise speed of $\bar{W}_q$ is faster. These results implies: 1) large amount of users will badly affect performance of the system. When the number of $m$ is larger, impacts on the system induced by GSU are more obvious; 2) number of channels $c$ is also a significant factor to the performance.

In Fig. 6, it is obviously that the difference between $\bar{W}_q$ in case with GSU and that in case without GSU decreases with $c$ growing or $m - c$ droping. When $c$ is larger than 6 and 12 respectively, the average waiting time is nearly to 0. That means if number of available channel is large enough, GSU could produce little influence on the system.

Consequently, the performance is a comprehensive result of the three factors in the system with GSU.

### B. *Threat Detection*

*1) Detection of Sudden Threat:* We first verify the validity of the proposed scheme in detecting traditional sudden threat, where GSU's average occupancy duration suddenly rise at the very beginning it becomes greedy. $1/\mu_2$ is set to 20 and the threat last for 30 detection periods. In each sampling period, control node records 100 occupancy times of every user. We set $\alpha$, $\beta$, $\lambda$ and $\mu$ to 0.1, 0.25, 10, 1 respectively. Fig. 7 illustrates the fluctuation of $r^d$ versus sampling period. When the threat is injected (40th sampling period), the curve presents a step response. If the threat is end (70th sampling period), the curve returns to a low value. This indicates that our approach has desirable performance in detecting traditional threat.

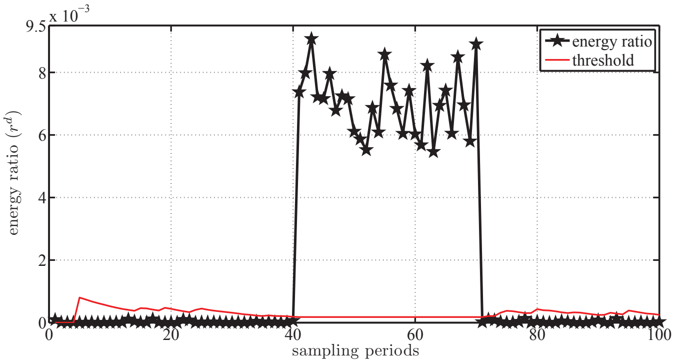


Fig. 7: Detection of sudden threat.

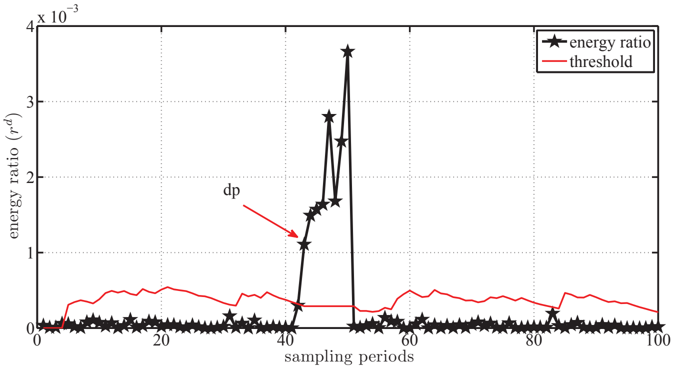


Fig. 8: Detection of stealthy threat.

*2) Detection of Stealthy Threat:* The smart GSU prefers to gradually increase its average occupancy time for the reason we mentioned before. We inject a stealthy threat, where the GSU gradually increases its occupancy duration as Section II-B describes. We set $\Delta t$ to 1 per variation period and $N = 100$. At the 41th sampling period, the threat begins. We can find in Fig. 8 that the curve displays a sharp rise in a short time. After only 3 sampling period, the detection value $r^d$ exceeds the threshold, and the threat in the networks is detected (dp is detected point in Fig. 8). We compare this approach with the simple and intuitive idea of detecting threat. This idea just checks the trend of average occupancy time. When it turns to be longer than previous average time and exceeds a threshold, we will consider the system is under threat. Table I presents the value of $r^d$ and average occupancy time $\bar{t}$ around the moment threat is injected through simulation. We find at the moment the threat is detected by our proposed approach, $r^d$ is nearly 60 to 180 times larger than that before threat, while $\bar{t}$ grows to 6.2032, which is only 3 time to that before threat. Moreover, average occupy time in a sampling period is fluctuant. So the deviation is inconspicuous and the method is not a effective one. Overall, wavelet transform is more sensitive to imperceptible changes and the proposed approach is an effective way in detecting stealthy threat.

## VI. Conclusion

In this paper, we presented greedy spectrum occupancy threat in CRN, which had long been ignored previously. A queueing model was established to describe the system with greedy secondary user. With numerical approach, we evaluated the impacts of greedy secondary user on the system. Results revealed that the performance is a comprehensive result of three factors: average occupancy time, number of users and number of channels. In addition, a detection approach based on wavelet was proposed. Simulation results showed that our method was effective to detect threat. Our future work will consider the case where there are more than one GSUs and the punishment to GSUs will be also taken into account.

## Acknowledgment

This work was supported by NSF China (No. 61202373, 61102052), SRF for ROCS by SEM, and Shanghai Basic Research Key Project (No. 13510711300, 12JC1405200).

## References

[1] L. Duan, L. Gao, and J. Huang, “Cooperative spectrum sharing: a contract-based approach,” *IEEE Trans. Mobile Comput.*, vol. 13, no. 1, pp. 174–187, Jan. 2014.

[2] R. Southwell, X. Chen, and J. Huang, “Quality of service games for spectrum sharing,” *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 3, pp. 1–12, Mar. 2014.

[3] W. Li, X. Cheng, T. Jing, and X. Xing, “Cooperative multi-hop relaying via network formation games in cognitive radio networks,” in *Proc. IEEE INFOCOM*, Turin, Italy, Apr. 2013.

[4] X. Xing, T. Jing, Y. Huo, H. Li, and X. Cheng, “Channel quality prediction based on bayesian inference in cognitive radio networks,” in *Proc. IEEE INFOCOM*, Turin, Italy, Apr. 2013.

[5] L. Sun and W. Wang, “Understanding blackholes in large-scale cognitive radio networks under generic failures,” in *Proc. IEEE INFOCOM*, Turin, Italy, Apr. 2013.

[6] T. C. Clancy and N. Goergen, “Security in cognitive radio networks: Threats and mitigation,” in *Proc. 3rd CrownCom*, Singapore, May 2008.

[7] S. Chen, K. Zeng, and P. Mohapatra, “Hearing is believing: Detecting mobile primary user emulation attack in white space,” in *Proc. IEEE INFOCOM*, Shanghai, China, Apr. 2011.

[8] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han, “Defeating primary user emulation attacks using belief propagation in cognitive radio networks,” *IEEE J. Select. Areas Commun.*, vol. 30, no. 10, pp. 1850–1860, Nov. 2012.

[9] H. Li and Z. Han, “Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systemsłpart ii: Unknown channel statistics,” *IEEE Trans. Wireless Commun.*, vol. 10, no. 1, pp. 274–283, Jan. 2011.

[10] ——, “Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks,” *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3554–3565, Nov. 2010.

[11] W. Wang, H. Li, Y. Sun, and Z. Han, “Attack-proof collaborative spectrum sensing in cognitive radio networks,” in *Proc. CISS*, MD, March 2009.

[12] ——, “Catchit: detect malicious nodes in collaborative spectrum sensing,” in *Proc. IEEE Globecom*, Honolulu, HI, Nov. 2009.

[13] X. He, H. Dai, and P. Ning, “A byzantine attack defender in cognitive radio networks: The conditional frequency check,” *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2512–2523, May 2013.

[14] M. Jo, L. Han, D. Kim, and H. P. In, “Selfish attacks and detection in cognitive radio ad-hoc networks,” *IEEE Network*, vol. 27, no. 3, pp. 46–50, May 2013.

[15] J. Tang and Y. Cheng, “Quick detection of stealthy sip flooding attacks in voip networks,” in *Proc. IEEE ICC*, Kyoto, Japan, Jun. 2011.

[16] L. Kleinrock, *Queueing systems*. Wiley-Interscience, 1975, vol. 1.

[17] R. B. Cooper, *Introduction to queueing theory*. North Holland New York, 1981, vol. 2.

[18] I. Daubechies *et al.*, *Ten lectures on wavelets*. SIAM, 1992, vol. 61.

[19] J. Tang, Y. Cheng, and C. Zhou, “Sketch-based sip flooding detection using hellinger distance,” in *Proc. IEEE Globecom*, Honolulu, HI, Nov. 2009.