Copyright ⓒ 2015 KSII

Behave Well: How to Win a Pop Vacant Band via Cooperative Spectrum Sensing

Jingyu Feng[1, 2], Guangyue Lu[1] and Hong Chang[1]
[1] Department of Communication Engineering, Xi'an University of Posts & Telecommunications
Xi'an 710121, China
[e-mail: tonylugy@163.com]
[2] State Key Laboratory of Information Security (Institute of Information Engineering), Chinese Academy of Sciences, Beijing 100093, China
*Corresponding author: Guangyue Lu

Received November 12, 2014; revised February 4, 2015; revised February 8, 2015; accepted March 15, 2015; published April 30, 2015

Abstract

Cooperative spectrum sensing (CSS) for vacant licensed bands is one of the key techniques in cognitive radio networks. However, current CSS schemes focus on ensuring an efficient cooperation among secondary users (SUs), but ignoring their competition. At the same time when several SUs want to a vacant band, how to win this pop vacant band for an SU becomes more and more important. Inspired by the idea that an SU who always behaves well will win a pop vacant band more easily, we propose a competition scheme called BehaveWell (BW) in this paper. By analyzing the main threats against CSS, competitive coefficient is introduced to evaluate each SU's past behaviors in CSS. A higher competitive coefficient is very helpful for an SU to win a pop vacant band. This BW scheme can not only enhance a healthy competition among SUs, but also improve the security of CSS. Simulations verify the effectiveness of the proposed scheme.

Keywords: Cognitive radio, cooperative spectrum sensing, competitive coefficient, security.

This research was supported in part by the National Science Foundation of China (61301091, 61271276), the China Postdoctoral Science Foundation(2013M541013), the National Science Foundation of Shaanxi Province (2014JQ8321, 2014JM8299, 2012JQ8011), the Science Foundation of Shaanxi Provincial Education Office (14JK1681), the Open Foundation of State Key Laboratory of Information Security(2015-MS-14), the New Star Team of Xi'an University of Posts & Telecommunications.

http://dx.doi.org/10.3837/tiis.2015.04.003 **ISSN : 1976-7277**

1. Introduction

With the rapid development of wireless communication technologies and the huge demand of the capacity for wireless applications, the wireless frequency spectrum has become increasingly scarce. However, a large portion of the assigned spectrum bands are not utilized efficiently. According to the Federal Communications Commission (FCC), temporal and geographical variations in the utilization of the assigned spectrum range from 15% to 85% [1]. To solve the contradiction between the spectrum scarcity and low spectrum utilization, cognitive radio have been considered as a useful technology, which allow the licensed users to share their vacant bands with unlicensed users who are not assigned bands, thereby increasing the efficiency of the spectrum utilization [2]. The licensed users are also called the primary users (PUs) and the unlicensed users are the secondary users (SUs) in cognitive radio networks.

Cooperative spectrum sensing (CSS) is a key to the opportunistic use of assigned spectrum bands in cognitive radio network, since it enables SUs to find the vacant bands in the case of deep shadowing and multipath fading. The main idea of CSS is to ensure the sensing performance by exploiting spatial diversity via the observations of spatially located SUs [3]. By cooperation, CSS can eliminate the negative effect from deep shadowing and multipath fading by sharing sensing data and make a reliable cooperative decision.

As always, we ignore an issue that the number of SUs is far more than PUs in cognitive radio network. So, the vacant bands are very scarce, and it is often the case that a few SUs compete for a vacant band at the same time. In this case, how to win this pop vacant band via CSS becomes more and more important. On the other hand, CSS is being compromised by malicious threats. False sensing, one of the most famous threats, is launched by malicious SUs to deceive other SUs to acquire a wrong cooperative decision via CSS. Many efforts have been made to suppress this threat, such as outlier detection [4], shadow-fading correlation [5], expectation maximization [6], goodness-of-fit [7], trust or reputation [8-11], etc. However, these methods fail to address selfish sensing threat. There may exist some selfish SUs who are unwilling to cooperate but enjoy sensing data from others. Such threat may seriously degrade the performance of CSS and even make a well designed CSS scheme useless [12]. To suppress selfish threat, recent efforts are mainly paid to game theory [13-15]. Additionally, SUs must never interfere with PUs in CSS [2]. Some SUs may long occupy vacant bands even though PUs come back, which is prone to causing harmful interference to PUs. Currently, false sensing, selfish sensing and long occupation are the main threats against CSS, but not a method can suppress them together with a scheme. From the perspective of competition, the SUs who launch these threats in CSS will be punished to obtain a lower competitive coefficient which can reduce their opportunities or even make them have no chances to get any vacant band, whereas the SUs behave well in CSS will have a chance to get a vacant band.

In this paper, we propose a competition scheme called BW to enhance a healthy competition among SUs. As we know, each SU plays two roles in the CSS environment, the role of cooperating SU reporting sensing data and the role of initiator SU enjoying sensing data. Noticing this, our design idea is that an SU can win a pop vacant band more easilier than others if he always behaves well while playing the role of cooperating SU. The main contributions of this paper are as follows.

- The concept of competitive coefficient is introduced in CSS. If an SU behaved well in the past, he would get a higher competitive coefficient and thus win a pop vacant band more easilier in the future. That is, this SU must rarely launch malicious threats, or else he will fail to win a pop vacant band and even get nothing from CSS.
- Noting that the SUs who launch the main three threats in CSS show a binary behavior, three types of individual competitive coefficients corresponding to these threats can be uniformly evaluated based on beta function, resulting in less mathematical analysis and computation.
- A general evaluation framework is designed to fuse individual competitive coefficients. Such framework has a good expandability to incorporate new individual competitive coefficients into the evaluation of competitive coefficient.

The organization of this paper is as follows. In section2, preliminaries related on CSS are described. We construct the BW scheme in section 3 and describe its implementation strategies in section 4. Simulation analysis of BW is given in section 5. Finally, we conclude this paper in section 6.

2. Preliminaries

The CSS process can be viewed as a parallel fusion network [16]. As shown in **Fig. 1**, a central authority called fusion center (FC) controls the process of CSS: individual sensing, data reporting and data fusion [3].

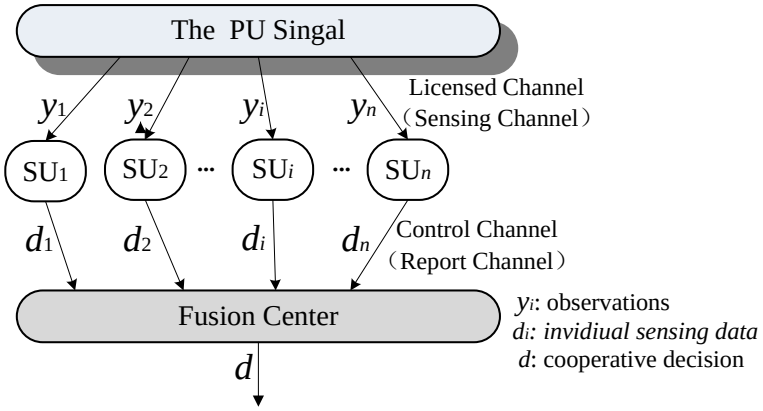

Fig. 1. Modeling CSS as a parallel fusion network.

- **Individual sensing**: Each SU senses the vacant band of a PU via the licensed channel individually. In this process, each SU abstracts its sensing data as “1” or “0” which denotes the hypothesis of the absence (H_1) and the presence (H_0) of the PU band respectively [17].
- **Data reporting**: All SUs send their sensing data to FC via the control channel.
- **Data fusion**: FC combines the received sensing data and determines the presence of a PU with a fusion rule, such as “AND”, “OR” and “Majority” rule [17].

In the CSS process, licensed channel is the selected licensed frequency band where a physical point-to-point link between the PU transmitter and each SU for observing the vacant band, and control channel is a physical point-to-point link between each SU and FC for

sending individual sensing data [3]. It can be seen that the two types of channels are given by cognitive radio network. Thus, the CSS process among SUs seems not waste any more spectrums.

Additionally, the CSS process will work when at least one SU send a CSS request to FC since these SUs cannot distinguish a vacant band from a deep shadowing effect and multipath fading. However, at the same time when several SUs want to the vacant band of a PU, how FC choose an SU to use this pop vacant band. In this paper, our main task is to help FC to make a choose decision that the SU who behave well in the CSS process will get a pop vacant band more easily.

3. Proposed Competition Scheme

In this section, we first describe some related definitions of the BW scheme, and then present an individual scheme to evaluate individual competitive coefficients by analyzing three threats in CSS. Finally, a general evaluation framework is designed to incorporate them as a single value.

3.1 Related Definitions

Some definitions are introduced in the BW scheme. To understand the design of our scheme better, we describe these new definitions in advance.

- **Pop vacant band**: the vacant band of a PU that there are many SUs who want to win it at the same time.
- **Individual competitive coefficients**: evaluate the degree of each threat launched by an SU. For SU_i, its jth individual competitive coefficient corresponding to jth threat can be be represented as c_{ij}. If SU_i rarely launches jth threat, he will get a high c_{ij}.
- **Competitive coefficient**: incorporate individual competitive coefficients as this value. For SU_i, its competitive coefficient can be represented as C_i. A higher C_i means SU_i can win a pop vacant band easilier than other SUs.
- **Local area**: i.e. cognitive radio area. FC is usually a base station and its management area is local, so an FC can be only responsible for a local area. It means that cognitive radio network may be devided into many local areas.
- **Threshold**: δ is the threshold of competitive coefficient. For $C_i \geq \delta$, SU_i has a chance to get a pop vacant band. But $C_i < \delta$, it is impossible for SU_i to get any vacant band. In the BW scheme, $C_i=1$ if SU_i always behaves well. Unfortunately, this ideal behavior is impossible in practical network. To select an optimal δ, two aspects should be considered. On the one hand, some SUs may report false sensing data occasionally due to channel fading. So, δ cannot be set to 1. On the other hand, a smaller value is unsuitable for δ since it would incerase the chance of malicious SUs for getting vacant bands. So, a moderate value is necessary to δ. The optimal value of δ shoud be in [0.5, 1]. In our scheme, δ is dynamically allocated during [0.5, 1] according to the level of competition for a period of time. Let L denotes the number of PUs and U is the number of SUs in a local area. When $U >> L$ for a period of time, the competition for licensed bands may be very great, and thus δ is allocated to be large. Additionally, even if $U \leq L$ for a period of time, but a large number of SUs often request a pop vacant band at the same time, δ should also be allocated to be large.
- **E3C**: an electronic certificate is introduced to maintain competitive coefficient for SUs when they move a local area to another one.

3.2 Evaluation of Individual Competitive Coefficients

From the perspective of competition, our scheme is designed to inspire SUs behave well. That is, if an SU rarely launches threats against CSS, he will have more chances to get a vacant band. Currently, there are three threats that are mainly damaging the performance of CSS.

- **FS**: false sensing threat. To monopolize the vacant band usage, malicious SUs may try to report false sensing data to indicate that the PU exists even when there is no PU singal, thereby misguiding other SUs to give up their opportunities. Since the individual sensing data of each SU is a binary variable "1" or "0", it is very easy for malicious SUs to fake "1" as "0" during the process of CSS. If there are a sufficient number of false sensing data, they can make FC result in a wrong cooperative decision successfully.
- **SS**: selfish sensing threat. To save energy or transmission time, some selfish SUs may refuse to provide sensing data, while still enjoying those from other SUs via CSS. If sensing data are scarce, a well designed CSS scheme may become useless.
- **LO**: long occupation threat. To cherish their opportunities to get vacant bands, some SUs may occupiy vacant bands too long to interfere with PUs, To protect their rights, PUs would send complaints to FC.

In summary, it can be seen that the SUs who launch these threats in CSS behave binary (i.e., positive or negative). Such binary behaviors can be described as

	Positive	***Negative***
FS:	*Real sensing data*	*False sensing data*
SS:	*Provide sensing data*	*Refuse to provide*
LO:	*No complaint*	*Complaint*

Recently, one of the most popular designs using binary input to evaluate a variable ranging from 0 to 1 is based on beta function. It first counts the number of positive and negative behaviors a user has conducted, and then calculates the variable with beta probability density functions (PDF) denoted by [18].

$$Beta(a,b)=\frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)}q^{a-1}(1-q)^{b-1} \tag{1}$$

where θ is the probability of sensing behaviors, $0\leq\theta\leq 1$, $\alpha>0$, $\beta>0$.

Without loss of generality, let $T=\{t_1, \ldots, t_k, \ldots, t_n\}$ denote the set of threats, where t_k is the k-th threat. The k-th individual competitive coefficient (c_{ik}) of an SU (Take SU_i as an example) corresponding to t_k can be evaluated with beta function as: $c_{ik}=Beta(pos_{ik}+1, neg_{ik}+1)$. pos_{ik} and neg_{ik} denote the number of positive sensing and negative sensing about the k-th threat launched by SU_i. Without any prior observations, $pos_{ik}=neg_{ik}=0$ and hence, $c_{ik}=$Beta(1, 1).

Consider the case $\Gamma(x)=(x-1)!$ when x is an integer [19]. It can be deduced that the expectation value of the beta function is given by: $E[Beta(\alpha, \beta)]=\alpha/(\alpha+\beta)$. Thus, c_{ik} can be further described as

$$c_{ik}=\frac{1+pos_{ik}}{2+pos_{ik}+neg_{ik}} \tag{2}$$

In our scheme, we marke the CSS threats {FS, SS, LO} as $\{t_1, t_2, t_3\}$. Then (pos_{i1}, neg_{i1}) represent the number of real and false sensing respectively, c_{i1} is the individual competitive coefficient of SU_i corresponding to FS. Similarily, c_{i2} and c_{i3} denote the individual competitive coefficient corresponding to SS and LO respectively, which can be evaluated by (pos_{i2}, neg_{i2}) and (pos_{i3}, neg_{i3}) successively.

3.3 General Evaluation Framework

From the perspective of suppressing threats, we can evaluate individual competitive coefficients for each SU. Then, a general evaluation framework is necessary to incorporate these coefficients as a single value. In our scheme, the competitive coefficient (C_i) of SU_i corresponding to T can be evaluated as

$$C_i = f\left(c_{i1}, \cdots c_{ik} \cdots c_{in}\right) \tag{3}$$

To promote a healthy competition in cognitive radio network, $f(\cdot)$ should satisfy three requirements.

1) *Expandability*. Until now, we have mainly found three threats: FS, SS and LO. Maybe, other threats would appear in the future. $f(\cdot)$ should have the ability to incorporate new individual competitive coefficients into the evaluation of C_i.
2) *Comparability*. It is necessary to ensure that C_i is between 0 and 1. Otherwise, some SUs may be assigned arbitrarily high values (much more than 1), and arbitrarily low values (much less than 1) to another SUs, which brings difficulty in comparing them. In [0, 1], we can compare whether several SUs (such as SU_x and SU_y) behave well by $C_x > C_y$.
3) *Fairness*. Malicious SUs will get nothing from CSS, whereas the SUs who always behave well can win vacant bands easily.

Based on the above requirements, we consider the following scenarios {*prior*, *common*, *zero*} for evaluating C_i.

- **Prior scenario**

For each $c_{ik} > \delta$, it means SU_i behaved well in the past. FC should give SU_i a *prior* authority to use a pop vacant band. His competitive coefficient is evaluated as

$$C_i = \frac{1}{n}\sum_{k=1}^{n} c_{ik} \tag{4}$$

For a good expandability, new individual competitive coefficient must meet $0 \le c_{ik} \le 1$.

- **Common scenario**

For some $c_{ik} > \delta$, it means SU_i behaves well sometime. That is, this SU has launched some malicious threats before. FC should give SU_i a *common* authority. His competitive coefficient is evaluated as

$$C_i = \frac{1}{n}\left|\sum_{c_{ik} > \delta} c_{ik} - \sum_{c_j < \delta}^{j \neq k} c_{ij}\right| \tag{5}$$

It can be seen that the malicious behaviors will decay Ci severely, result in increasing his difficulty to win a vacant band. Of course, an opportunity should be offered to correct his misconduct. For instance, if SUi doesn't launch the k-th threat during a period of time, his cjk value will be increased by 0.1. But, once he is found to launch this threat again, more severe punishment will be given to him, such as his cik value will be decreased by 0.2 immediately.

- **Zero scenario**

For each cik<δ, it means SUi always behaves maliciously and launches all threats. FC has to give SUi a zero authority. His competitive coefficient is evaluated as

$$C_i = 0 \tag{6}$$

This SU is hopeless, and FC or even cognitive radio system should reject to his request for any vacant band. He can get nothing from CSS.

4. Implementation Strategies

The effectiveness of supporting competitive coefficient in CSS depends not only on the factors and metric for evaluating competitive coefficient, but also on the implementation of the BW scheme. Typical issues in implementing BW in cognitive radio network include "pop band allocation" and "competitive coefficient maintain for mobility environment".

4.1 Pop Band Allocation

When have known that competitive coefficient is used in the case when there are several SUs want to win a pop vacant band at the same time, such as time *h*. Procedure 1 is designed to describe how SUs can win a pop vacant band by their competitive coefficients. When several SUs send requests to ask a pop vacant band at time *h*, two issues should be addressed before performing Procedure 1. 1) They have different competitive coefficient (i.e. each $C_i \neq C_k$ for $i \neq k$) at time *h*. 2) They have the same competitive coefficient (i.e. each $C_i = C_k$ for $i \neq k$) at time *h*, how FC decides who will pop up?

For the first issue, it is easy for FC responds to these requests from the highest to the lowest according to their competitive coefficients. To address the second issue, three priority strategies can be introduced to help FC, including Good Behaviors Priority, TTL Priority and Random Priority.

- **Good Behaviors Priority**

For some cik>δ in the set T={t1, …, tk,…, tn}, as we know, that means SUi has launched some malicious threats before. Let mi denote the number of malicious threats launched by SUi. Specially, mi =0 when each cik>δ. Then, FC can compare the m values for different SUs to decide who will pop up. Take SUx and SUy as an example, if mx<my, SUx will win a pop vacant band even though both SUx and SUy have the same competitive coefficient at time h. This strategy is named as gbp() in Procedure 1.

- **TTL Priority**

In the BW scheme, TTLi (time-to-live) represents the life time of SUi from who joined cognitive radio network to time h. Obviously, TTLi =h-τi (the initial time when SUi joined cognitive radio network). When several SUs have the same competitive coefficient at time h, the SU with highest TTL would pop up. For an SU with a smaller TTL, he is likely to have fewer opportunities to launch malicious threats. Especially for TTLi =0, that means SUi is a

newcomer who has done nothing in the network and his competitive coefficient is 1. But, once he launches malicious threats in the future, his competitive coefficient will be decayed sharply by Eq.(5). For an SU with a higher TTL, he is likely to have more opportunities since he can maintain a higher competitive coefficient for a long time. Therefore, we should give a chance to the SU with highest TTL when several SUs have the same competitive coefficient at time h. This strategy is named as tp() in Procedure 1.

- **Random Priority**

Initially, FC chooses an SU randomly to use the pop vacant band when several SUs have the same competitive coefficient at time h. But such choice is restricted by another index r which is the number of the SU who has been chosen randomly in the Random Priority strategy. For SUi, ri =0 if he has never been chosen and ri will be added by 1 when he is chosen. Then, FC can compare the r values for different SUs to decide who will pop up. Of course, it is possible that there are more than two SUs with the same low r value. In this case, FC should chooses an SU randomly from them again. This strategy is named as rp() in Procedure 1.

Let S={SU1, …, SUi,…, SU n} denotes the set of several SUs who send requests to ask a pop vacant band at time h, U is the set filtered from S and |U| resprents the amount of elements in U.

Procedure 1 Winpop(U)

Input: S

Output: U

Initialize $U=U_1=U_2=U_3=\varnothing$
for each C_i or C_k **do**
 if ($C_i \neq C_k$) **then**
  U={SU$_i$} with the highest competitive coefficient in S
 else
  U_1 = S filtered by *gbp*()
  if($|U_1|==1$) **then**
   $U=U_1$
  end if
  if($|U_1|>1$) **then**
   U_2 =U_1 filtered by *tp*()
   if ($|U_2|==1$) **then**
    $U=U_2$
   end if
   if($|U_2|>1$) **then**
    U_3 =U_2 filtered by *rp*()
    if($|U_3|==1$) **then**
     $U=U_3$
    end if
    if($|U_3|>1$) **then**
     Continue to perform *rp*() until $|U_3|==1$
     $U=U_3$
    end if
   end if
  end if
 end if
end for

4.2 Competitive Coefficient Maintain for Mobility Environment

We have known that the process of CSS is in the charge of FC which is usually a base station. However, the management area of FC is local and the sensing distance of an SU is limited. Take **Fig. 2** as an example, local areas compose the cognitive radio network. In order to facilitate the depiction of this figure, we draw a PU in each local area. In practice, there are a FC and several PUs coexiting with SUs in a local area. If PUs are fixed devices, they will not move. If not, they may move from a local area to another one.

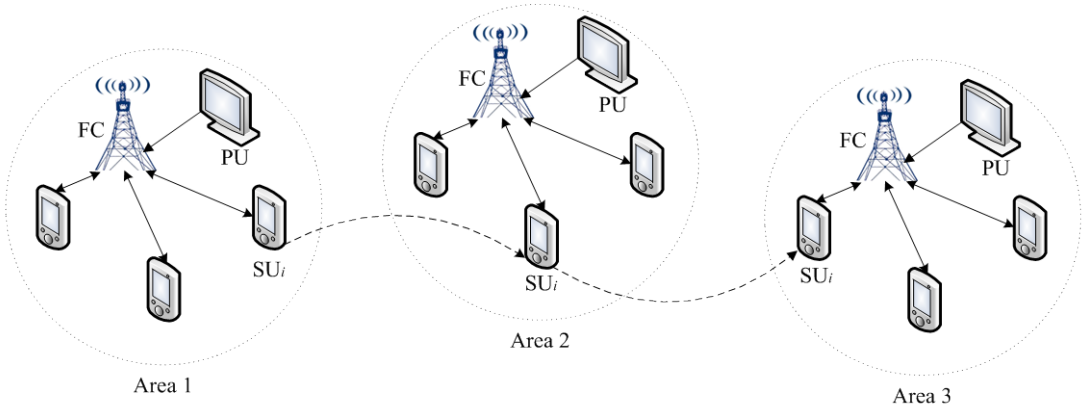

Fig.2. Example of local areas in cognitive radio network.

From **Fig. 2** we can find a question that competitive coefficient is usually utilized in a local area. Can SU_i's competitive coefficient in area 1 be used in area 2 when he moves from area 1 to area 2? To address this question, E3C is introduced to maintain competitive coefficient for SUs in different local areas. E3C records the indexes $\{(pos_{i1}, neg_{i1}), (pos_{i2}, neg_{i2}), (pos_{i1}, neg_{i2})\ \tau_i, r_i\}$ for SU_i. To make E3C work better, four characteristics should be abided by E3C.

- E3C cannot be modified by anyone except for the FC of local areas in which only dose the FC have the right to read and update E3C in terms of an SU's behaviors. Procedure 2 is performed to update E3C.
- E3C is hold by each SU and cannot be deleted by anyone except an SU wants to give up his mobile device. With a new device, he can get a new E3C.
- Without E3C, an SU cannot be accepted by the FC in any local area to get vacant bands. An SU with E3C can participate in a competition to win a pop vacant band by evaluating its competitive coefficient in E3C.
- For a newcomer who hasn't come into any local areas, his E3C is initialized as {(0, 0), (0, 0), (0, 0), 0, 0}. When he comes into a local area, his E3C will be updated. The indexes $\{(pos_{i1}, neg_{i1}), (pos_{i2}, neg_{i2}), (pos_{i1}, neg_{i2})\ \tau_i, r_i\}$ are accumulated when he moves from a local area to another local area, rather than a certain local area.

Assuming SU_i, SU_j denote cooperating SU and initiator SU in Procedure 2. As shown in **Fig. 1**, d_i is the individual sensing data from SU_i and d is the cooperative decision from FC. To ensure E3C update effectively, detection method of the CSS threats {FS, SS, LO} by FC should be considered in Procedure 2.

- **Detect FS threat**: Two cases should be considered in the detection of FS threat. 1) SU_j interferes with PU. 2) SU_j does not interfere with PU. Such interference is caused by d when SU_j adopts it. Of course, such interference will not happen while PU is absent. In the first case, SU_i can be detected to lanuch SS threat for d=1&&d_i=1. In the second case,

SU_i can be detected to lanuch SS threat for d=0&&d_i=1.

- **Detect SS threat**: Although the location of SU_i is convenient for sensing PU, he does still refuse to the CSS query of FC. In this case, SU_i is detected to lanuch SS threat.
- **Detect LO threat**: When PU comes back, SU_j still continues to occupy the PU band, not to get out. To protect his rights, this PU would send a complaint to FC. In this case, SU_j is detected to lanuch LO threat. To avoid false complaint, SU_j is asked to send a departure response when he leaves the PU band. If PU sends a complaint before the departure time (i.e. the time of receiving departure response by FC), this complaint is real. If after the departure time, this complaint is false. But if SU_j does not send a departure response, the complaint from PU will default to real as soon as it is received. Specially, it is impossible for some PUs to collaborate with each other to send false complaints. Such collaborative attacks can be detected by two reasons, 1) they may send complains after the departure time regarding on their bands, 2) FC only accepts the complaints of the PUs that SU_j has utilized their bands.
-

Procedure 2 Updating E3C

Input: $E3C_i$, $E3C_j$, U
Output: $E3C_i$, $E3C_j$

Initialize $U=\varnothing$
if(SU_i launches SS threat at time h) **then**
  neg_{i2}++
else
  pos_{i2}++
  if($U=\{C_j\}$ while performing $rp()$) **then**
    r_j ++
  else if
  if(SU_j interferes with PU) **then**
    if(d=0) **then**
      neg_{j3}++
    else
      pos_{j3}++
      if($d=d_i$) **then**
        neg_{i1}++
      else
        pos_{i1}++
      end if
    end if
else
    pos_{j3}++
    if($d=d_i$) **then**
      pos_{i1}++
    else
      neg_{i1}++
    end if
  end if
end if

5. Simulation Analysis

We would perform five simulations to validate the BW scheme and show its effectiveness.

5.1 Simulation Setup

The simulations are performed based on the energy detection, in which the primary signal is a baseband QPSK modulated signal under the AWGN (additive white Gaussian noise) environment. The general simulation setup is shown in **Table 1**.

Table 1. Description of simulation elements

	Description	Default
Environment Setting	Number of PUs in the network	5
	Number of SUs in the network	100
	Percentage of attackers	40%
	Sampling frequency	1KHz
	SNR	-8dB
	Time-bandwidth product	50
	Threshold of competitive coefficients	0.5

In the simulations, the SUs are split into two types: malicious SUs and honest SUs. The percentage of malicious SUs is set to 40%. The behavior pattern for them is to launch three threats in CSS, while honest SUs always behave well.

All simulations are executed by cycle-based fashion. At each cycle, all SUs are selected to perform CSS actions with each other randomly. After a few cycles, a competitive network topology is gradually formed by the BW scheme. FC then uses this scheme to perform CSS actions at each cycle, and update the competitive coefficients on the corresponding SUs.

5.2 Simulation Results

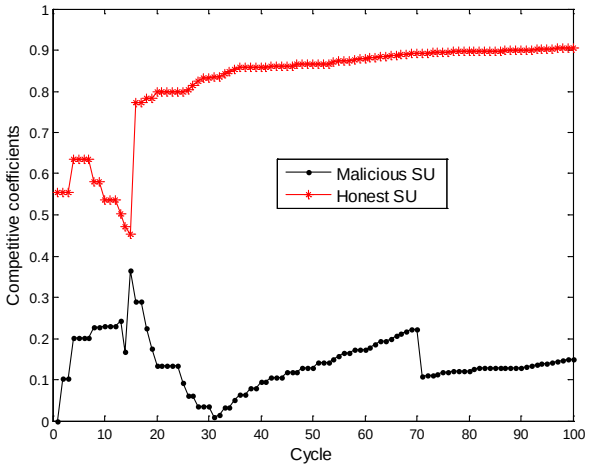

Fig. 3. Updating process of competitive coefficients.

In the first simulation, we choose a malicious and honest SU randomly to observe the updating process of their competitive coefficient. An SU's competitive coefficient is associated with his past sensing behaviors. As shown in **Fig. 3**, an honest SU's competitive coefficient is greater than δ and tends to 0.9 after 20 cycles, since he always behaves well in CSS.

Conversely, a malicious SU's competitive coefficient is rarely larger than δ. We can also find that BW makes the malicious SU's competitive coefficient fluctuates with the increase of cycles. This is because the *common* and *zero* scenarios can suppress the boost of competitive coefficient against threats. With a lower competitive coefficient, a malicious SU is difficult to win a vacant band.

We then perform three simulations to validate the robust of BW in terms of its suppressing three threats.

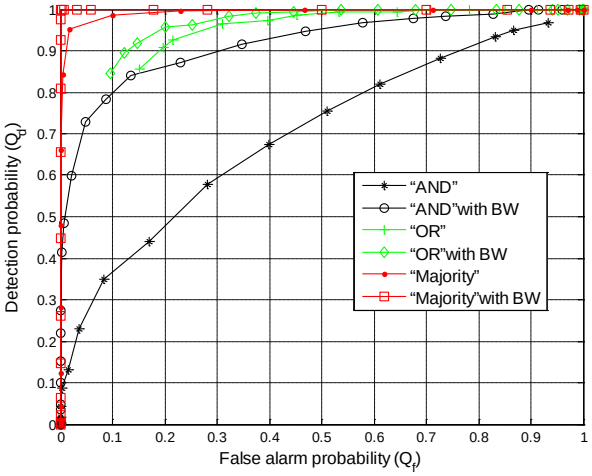

Fig. 4. ROC curves under the FS threat.

In the second simulation, we analyze the receiver operating characteristic (ROC) curves, the relationship between the probabilities of detection (Qd) and false alarms (Qf), which is usually to validate the sensing performance of CSS. As shown in **Fig. 4**, we can see that the ROC curves of the "AND" and "Majority" rule with BW are better than traditional rules without protection, which indicates that the BW scheme under the FS threat can enhance the performance of the two fusion rules significantly after filtering out malicious SUs. When one SU reports "1" in the "OR" rule, the PU signal is considered to be present. It also can be seen that malicious SUs have a little influence on the "OR" rule by analyzing the ROC curves.

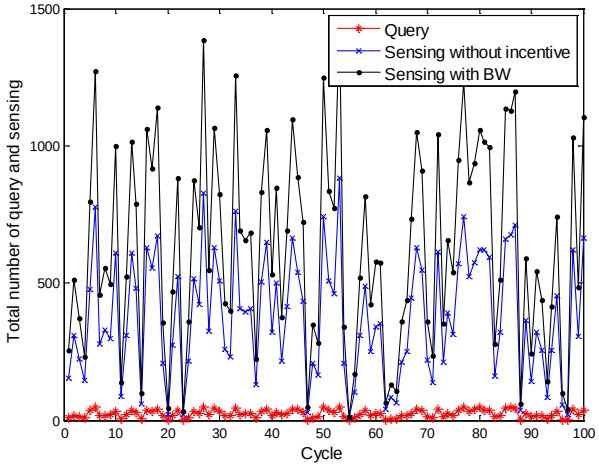

Fig. 5. Total number of query and respond at each cycle under the SS threat.

To analyze the effectiveness of BW under the SS threat, we observe the total number of query and sensing at each cycle in the third simulation. As shown in **Fig. 5**, BW can increase the total number of sensing to a certain extent under the SS threat. In the BW scheme, if an SU (such as SUi) provides nothing in CSS for a long time, the growing number of negi2 will decay his competitive coefficient. To main a high competitive coefficient, BW can inspire SUs to provide sensing data.

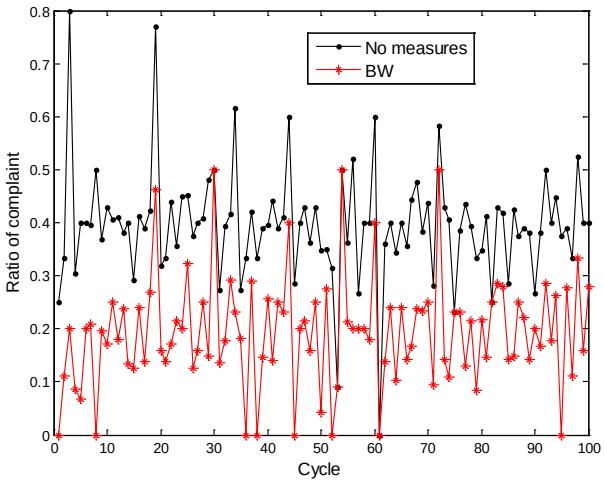

Fig. 6. Suppressing ratio of complaint at each cycle under the LO threat.

In the fourth simulation, we analyze the effectiveness of BW under the LO threat. BW makes some SUs scruple that lots of complaint will cause the decrease of their competitive coefficient. Therefore, BW can suppress the ratio of complaint at each cycle under the LO threat, as shown in **Fig. 6**.

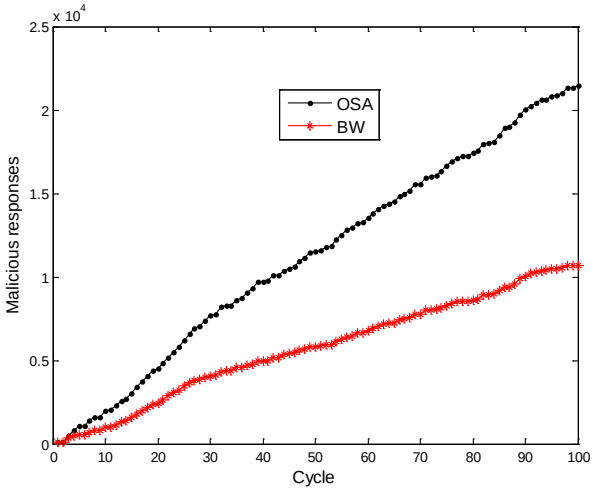

Fig. 7. Suppressing malicious responses.

In addition, some opportunistic spectrum access (OSA) [20-21] technologies also involve the issue to coordinate SUs to utilize a pop vacant band to aviod their collision. Nevertheless, they neglect that the security would affect the fairness of allocating a pop vacant band. That is,

some SUs launch threats to maximize their benefit, but no punitive measures are adopted to prevent them from utilizing vacant bands. In fact, the actions that malicious SUs launch threats in CSS will generate a large number of malicious responses which is mainly caused by the FS, SS and LO threat in CSS. If not suppressed, the number of malicious responses would become more and more terrible with the increase of cycles. So, the best method to compare BW with OSA is to test how they can suppress malicious responses. The fifth simulation is performed to observe this comparison. As shown in **Fig. 7**, BW can suppress the growth of malicious responses significantly compared with OSA with the increase of cycles. In the BW scheme, the SUs who launch threats are punished in the competition of vacant bands. To increase their opportunities for vacant bands, some malicious SUs would become to behave well.

6. Conclusion

In this paper, we have proposed a competition scheme called BW to enhance a healthy competition among SUs. The key idea of our scheme is that an SU who always behaves well will win a pop vacant band more easily. Inspired by this, we analyze the main threats against CSS, and thus introduce the competitive coefficient which is associated with each SU's past sensing behaviors in CSS. A higher competitive coefficient can contribute significantly to winning a pop vacant band for an SU. The implementation strategies of BW are also described in detail. Simulation results show that BW can make malicious SUs obtain a low competitive coefficient and improve the robust of CSS.

References

[1] Federal Communications Commission, "Spectrum Policy Task Force," Rep. ET Docket no. 02-135, Nov. 2002. http://www.fcc.gov/sptf/files/SEWGFinalReport_1.pdf

[2] J. Mitola, "Cognitive radio: An integrated agent architecture for software defined radio," *Royal Instutute of Technology*, 2000. Article (CrossRef Link)

[3] I. F. Akyildiz, B. F. Lo and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communication*, vol. 4, no. 1, pp. 40-62, 2011. Article (CrossRef Link)

[4] P. Kaligineedi and M. Khabbazian, "Malicious User Detection in a Cognitive Radio Cooperative Sensing System," *IEEE Transactions on Wirelss Communications*, vol. 9, no. 8, pp. 2488-2497, 2010. Article (CrossRef Link)

[5] A.W Min, K.G Shin and X. Hu, "Secure Cooperative Sensing in IEEE 802.22 WRANs Using Shadow Fading Correlation," *IEEE Transactions on Mobile Computing*, vol. 10, no. 10, pp. 1434-1447, 2011. Article (CrossRef Link)

[6] E. Soltanmohammadi and M. Naraghi-Pour, "Fast Detection of Malicious Behavior in Cooperative Spectrum Sensing," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 3, pp. 377-386, 2014. Article (CrossRef Link)

[7] G. Noh, S. Lim, S. Lee, et al, "Goodness-of-Fit-based Malicious User Detection in Cooperative Spectrum Sensing," in *Proc. of 2012 IEEE Vechicular Technology Conference*, pp. 1-5, 2012. Article (CrossRef Link)

[8] H.F Chen, X. Jin and L. Xie, "Reputation-based Collaborative Spectrum Sensing Algorithm in Cognitive Radio Networks," in *Proc. of 20th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 582-587, 2009. Article (CrossRef Link)

[9] J.Y Feng, Y.Q Zhang, G.Y Lu, et al, "Securing Cooperative Spectrum Sensing against Rational SSDF Attack in Cognitive Radio Networks," *KSII Transactions on Internet and Information Systems*, vol.8, no.1, pp.1-17, 2014. Article (CrossRef Link)

[10] Q. Q Pei, B. B Yuan, L. Li and H. N Li, "A sensing and etiquette reputation-based trust management for centralized cognitive radio networks," *Neurocomputing*, vol. 101, no. 4, pp. 129-138, 2013. Article (CrossRef Link)
[11] K. Zeng, P. Pawełczak and D. Cabri, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Communications Letters*, vol. 14, no. 3, pp. 26-228, 2010. Article (CrossRef Link)
[12] J.Y Feng, G.Y Lu, X.C Min, "Social Incentives for Cooperative Spectrum Sensing in Distributed Cognitive Radio Networks," *KSII Transactions on Internet and Information Systems*, vol.8, no.2, pp.355-369, 2014. Article (CrossRef Link)
[13] H. Li, X. Cheng, K. Li, X. Xing and T. Jing, "Utility-based cooperative spectrum sensing scheduling in cognitive radio networks," in *Proc. of the 32nd IEEE INFOCOM Conference*, Apr. 14-19, pp. 165-169, 2013. Article (CrossRef Link)
[14] Y. Chen and K. J. R. Liu, "Indirect reciprocity game modelling for cooperation stimulation in cognitive networks," *IEEE Transactions on Communications*, vol. 59, no. 1, pp. 159-168, 2011. Article (CrossRef Link)
[15] C.H Jiang, Y. Chen, Y. Gao, et al, "Joint Spectrum Sensing and Access Evolutionary Game in Cognitive Radio Networks," *IEEE Transactions on Wireless Communications*, vol.12, no.5, pp. 2470–2483, 2013. Article (CrossRef Link)
[16] R. Chen, J. M. Park and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. of 27th IEEE INFOCOM Conference*, pp. 1876–1884, 2008. Article (CrossRef Link)
[17] E. Peh, Y. C Liang, Y. L Guan and Y. G Zeng, "Optimization of Cooperative Sensing in Cognitive Radio Networks: A Sensing-Throughput TradeoView," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 9, pp. 5294-5299, 2009. Article (CrossRef Link)
[18] A. Jøsang and R. Ismail, "The beta reputation system," in *Proc. the 15th Bled Electronic Commence Conference*, pp. 1-14, 2002. Article (CrossRef Link)
[19] Gamma function. http://en.wikipedia.org/wiki/Gamma_function
[20] C. Y Peng, H. T Zheng, B.Y Zhao, "Utilization and fairness in spectrum assignment for opportunistic spectrum access," *Mobile Networks and Applications*, vol. 11, no. 4, pp. 555-576, 2006. Article (CrossRef Link)
[21] H. Fang, L. Xu, C. Huang, "Dynamic Opportunistic Spectrum Access of Multi-channel Multi-radio Based on Game Theory in Wireless Cognitive Network," in *Proc. the IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks*, pp. 127-132, 2013. Article (CrossRef Link)

Jingyu Feng received his B.S. degree in electrical information science and technology from Lanzhou University of Technology, China, in 2006. He received his Ph.D. degree from Xidian University, China, in 2011. He is currently a lecturer in Department of Communication Engineering, Xi'an University of Posts & Telecommunications, China. He is also a Postdoctor of University of Chinese Academy of Sciences, China. His main research interests include wireless security, trust management and cooperative spectrum sensing.

Guangyue Lu is a professor in Department of Communication Engineering, Xi'an University of Posts & Telecommunications. He received his B.S. and M.S. degree from Yangtze University, China, in 1992 and 1995 respectively. He received his Ph.D. degree from Xidian University in 1999. His research interests include wireless communication, cognitive radio and cooperative spectrum sensing.

Hong Chang received her B.S. degree in Electronic and Information Engineering from Zhongbei University, China, in 2003. She received her Ph.D. degree from Xidian University, China, in 2011. She is currently a lecturer in Department of Communication Engineering, Xi'an University of Posts & Telecommunications, China. Her main research interests include information countermeasure, communication signal processing and spectrum sensing.