Towards Addressing Group Selfishness of Cluster-Based Collaborative Spectrum Sensing in Cognitive Radio Networks

Yiyong Sun, Zhaoyu Gao, Suguo Du, Shuai Li, Haojin Zhu
Shanghai Jiao Tong University, Shanghai, China
{syy, oversky710, sgdu, shuailee, zhu-hj}@sjtu.edu.cn,

Xiaodong Lin
University of Ontario Institute of Technology, Canada
xiaodong.lin@uoit.ca

***Abstract*—Collaborative spectrum sensing has been recognized as a promising way to ameliorate the sensing performance in cognitive radio networks. Unfortunately, it also introduces some system overhead to users, and as a result some selfish secondary users might be unwilling to contribute to collaborative spectrum sensing. In this paper, we propose a new selfishness model in cluster-based collaborative spectrum sensing, which is referred to Overclaim Selfishness (OS). An OS group may gain benefit by sharing nominally equal but actually much less sensing reports than it declares. To deal with this problem, we propose an Overclaim Selfishness Detection Scheme (OSDS) to detect the potential OS groups. We find that a single secondary user tends to have one special type of sensing reports correlated with his physical location, thus the cluster number estimated by OSDS should be no much less than the number of users the group contains. Further, we adopt an incentive scheme to stimulate rational groups to behave honestly. Finally, a real world experiment is adopted to demonstrate the effectiveness of our proposed scheme OSDS.**

Keywords – **Cluster-Based Collaborative Spectrum Sensing, Overclaim Selfishness, Selfishness Detection, Incentive Scheme**

I. INTRODUCTION

The dramatic increase of wireless applications has highlighted the scarcity of available spectrum resource and motivated the concept of cognitive radio, which is proposed to improve the efficiency of current spectrum utilization [1]. By applying the technique of cognitive radio, secondary users (SUs) are allowed to have dynamic spectrum access to licensed channels when primary users (PUs) are absent, which is very different from the traditional fixed allocation paradigm.

In a Cognitive Radio Network(CRN), one of the major challenges for SUs is how to conduct precise spectrum sensing. The performance of generally used schemes for primary transmitter detection (energy detection, feature detection etc. [2]) degrades severely when wireless channel experiences fading or shadowing. Recent research shows that collaborative spectrum sensing could significantly improve the sensing performance by exploiting the spatial diversity [3]. Cluster-based collaborative sensing is regarded as one typical way. As shown in [4], a typical clustered-based collaborative spectrum sensing could be described as follows: the SUs will interact to form collaborating clusters, and, the sensing reports within and among different clusters could be propagated via peer-to-peer manner until they converge to a unified decision on the presence or absence of PUs by iterations. In practice, these clusters may be operated by different WhiteFi Access Points [5] or Wireless Service Providers [6].

Most of the existing works assume that all SUs are ready to contribute to collaborative spectrum sensing. This assumption, however, might be easily violated in the presence of rational users, who may choose to save their precious resources (e.g. energy, transmission time, or even energy detectors), but, at the same time, will still enjoy the sensing results from others. Such kind of selfish behavior may seriously degrade the performance of collaborative spectrum sensing, thereby attracting some researchers to explore incentive schemes from the perspective of game theory to stimulate SUs to cooperate with each other in a good manner.

In [7], the incentive issue for cooperative spectrum sensing has been firstly studied. Song *et al.* model collaborative sensing as an N-player horizonal infinite game, and apply two strategies in the scenarios of ignoring and considering uncertain collisions in wireless channels respectively. In [8], an evolutionary game has been adopted to develop the best cooperation strategy for SUs. Wang *et al.* analyze behavior dynamics of SUs, and then prove that the behaviors of SUs will finally converge to an evolutionary stable strategy. Both of these two works assume that selfish behaviors could be detected immediately by their neighbors.

However, selfishness detection remains to be one of the major challenges for thwarting selfish behaviors in CRN. Different from traditional ad hoc networks, in which the selfish behaviors such as packet-dropping could be easily observed and detected by neighbor nodes, a selfish user in CRN could pretend to be a *good* one by sharing a dummy or slightly modified sensing report based on real sensing reports forwarded from others. This problem will be more challenging in a clustered CRN if the SUs collude to form a selfish cluster, within which some SUs could pretend to be *good* users with the help of other normal ones. Thus the colluding cluster will generate more sensing reports including both fake and real ones and claim all of them are authentic. Such kind of selfishness will decrease other clusters' sensing performance and therefore violates the stipulate equivalent exchange in

978-1-4673-0921-9/12/$31.00 ©2012 IEEE

cluster-based collaborative spectrum sensing. We coin such kind of new selfish behavior as *Overclaim Selfishness* (OS). The existing works on filtering malicious sensing reports [9] [10] may not work well for OS since users who conduct OS do not seek to change the aggregating results but only to disguise their behaviors of free-riding.

To address this problem, we propose an Overclaim Selfishness Detection Scheme (OSDS). OSDS is motivated by an observation that, from the classification point of view, the SU at a certain location will have one "type" of sensing reports, which forms one data cluster correlated with his physical space [5] [9] [11]. Since the sensing reports of each "type" follow a certain Gaussian distribution, thus we utilize the Gaussian Mixture Model (GMM) [12] to classify the sensing reports and get the number of data clusters. To avoid confusion of the concept between the user cluster and the data cluster classified by GMM, we will call "user cluster" as *group* in the remaining of this paper. The attacker whose data cluster number is much smaller than it claims will be regarded as a selfish group. Since punishing a selfish group without affecting others is impossible in distributed CRN [7], we also introduce an incentive game to stimulate rational groups to behave honestly.

The contribution of this paper is summarized as follows.

1) To the best of our knowledge, this is the first work discussing group selfishness of cluster-based collaborative spectrum sensing in CRN.
2) Different from former works indicate [7] [8], this new kind of selfishness is hard to detect. Thus we propose a novel selfishness detection method based on GMM. Also, we introduce an incentive scheme in the new scenario to stimulate rational groups to contribute to the cluster-based collaborative spectrum sensing.

The paper is organized as follows: we model our system in Section II. Both OSDS and an incentive scheme are proposed in Section III. Experimental results of OSDS are shown in Section IV. We conclude this paper in Section V.

II. System Model and Preliminaries

In this section, we would briefly introduce our system model as well as some preliminaries about cluster-based collaborative spectrum sensing and Gaussian Mixture Model.

A. Cluster-Based Collaborative Spectrum Sensing

In this paper, we consider a distributed CRN in which each SU is equipped with an energy detector. As existing works mentioned [9] [11], the PUs considered here are TV towers whose ON/OFF status are independent with each other. The accuracy of judging an incumbent's presentence or absence is guaranteed by the collaborative spectrum sensing among SUs. We adopt soft decision which requires SUs to report the sensed RSS values of targeted spectrum in each time slot, i.e. 2s [2]. In a distributed CRN, the SUs in a close proximity will join together as a group.

However, the number of SUs in a single group may not be enough to make a precise decision of PU's status. Furthermore, shadowing and fading in a particular region may degrade the performance of spectrum sensing significantly. As shown in Fig.1, the proximity of Group 1 is shadowed by the obstruction, therefore all the SUs in Group 1 will get wrong sensing results which may lead to a severe interference with the PU unintentionally. Therefore, cluster-based collaborative sensing is proposed in [2] and [4]. The groups first exchange their collected sensing reports with each other, then combine those collected sensing results to determine the spectrum availability, which is shown in Fig.1.

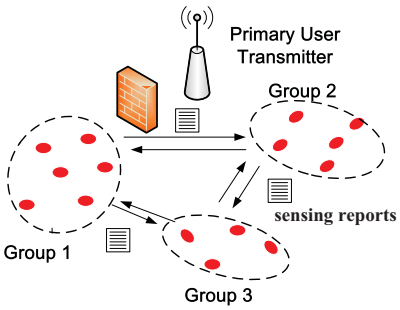


Fig. 1. the Cluster-based Collaborative Spectrum Sensing Architecture

B. Threat Model

Cluster-based cooperation could overcome the problem of shadowing and fading in a particular region, but it also introduces a new threat which has not been considered by other researchers. Normal SUs and free-riders in a group who share some common interests could cheat other honest groups' sensing reports as conspirators, which is different from the individual free-rider [7]. In particular, an SU who performs spectrum sensing could forward his sensing report to free-riders, then the free-riders pretend to be normal SUs by submitting the forwarded sensing reports. By doing this, a selfish group contributes much less than it should do to collaborative sensing. If there is no proper method thwarting such misbehavior, the popularity of OS groups would largely degrade the cooperative sensing performance.

In this paper, we assume our considered group consists of η SUs, and only γ of them really perform the spectrum sensing, where $\gamma \leq \eta$, so the other $\eta - \gamma$ SUs are free-riders. And we define this threat as Overclaim Selfishness (OS) attack which could be launched in two ways:

- *Sensing Report Duplication (SRD) Attack:* In each time slot, a free-rider duplicates the sensing report from another SU and adds a Gaussian white noise $\mathcal{N}(0, \delta_0^2)$ in each channel to generate a *new* sensing result[1]. We denote this attack as (γ, η) SRD attack.
- *Sensing Report Modification (SRM) Attack:* In each time slot, a free-rider duplicates a sensing report generated in SRD attack, then modifies $100\sigma\%$ channels with each channel i substituted by a random variable from a Gaussian distribution $\mathcal{N}(\mu_i', \delta_i'^2)$, where μ_i' should be

[1]To avoid being detected, a smart free-rider cannot duplicate the exact sensing data forwarded by others

in a reasonable range. The probability σ is fixed and the channels to be modified are predetermined. We denote this attack as (γ,η,σ) SRM attack.

Furthermore, we don't consider malicious behaviors which have already been solved by other works [9] [10], and the OS attack is different from the malicious attack in two ways:

1) A malicious user seeks to change the aggregating result, while a selfish user seeks to enjoy free sensing results.
2) A malicious user will modify his sensing reports to a large extent while a selfish user just duplicates or slightly modifies others' forwarded sensing reports.

C. Gaussian Mixture Model

The sensing reports of a certain SU follow a Gaussian distribution, thus we utilize Gaussian Mixture Model to classify the sensing reports in our proposed detection scheme. A Gaussian Mixture Model [12] is a weighted sum of M component Gaussian densities as given by the equation:

$$p(\vec{x}|\lambda) = \sum_{k=1}^{M} w_k \mathcal{N}(\vec{x}|\mu_k, \Sigma_k) \tag{1}$$

where $\vec{x}$ is a multi-dimensional vector; w_k is the mixture weight, and $\sum_{k=1}^{M} w_k = 1$; $\mathcal{N}(\vec{x}|\mu_k, \Sigma_k)$ is the component Gaussian density (multivariate Gaussian function) with mean vector μ_k and covariance matrix Σ_k. In order to analyze these components, we should estimate the parameter λ of this model: $\lambda = \{w_k, \mu_k, \Sigma_k\}, k = 1, 2, \cdots, M$.

Generally, the algorithm of Expectation Maximization (EM) is a popular way to obtain the parameter of GMM. The EM algorithm is basically a kind of maximum likelihood estimation method, which could maximize the estimation likelihood of GMM [12]:

$$\ln p(X|\lambda) = \sum_{n=1}^{N} \ln \{\sum_{k=1}^{M} w_k \mathcal{N}(\vec{x}|\mu_k, \Sigma_k)\} \tag{2}$$

where X is a sequence of N vectors $X = \{\vec{x}_1, \cdots, \vec{x}_N\}$. By executing EM algorithm iteratively, the estimated parameter $\hat{\lambda}$ will tends to make the training data more likely to happen in the prediction of GMM [12].

III. Proposed Scheme

In this section, we first discuss the basics of our scheme, then propose our Overclaim Selfishness Detection Scheme which aims to detect the selfishness in cluster-based collaborative spectrum sensing, and finally adopt an incentive scheme to stimulate rational groups to behave honestly.

A. Basics

The spectrum sensing result of a channel can be described as [13]:

$$r_k^i \sim \begin{cases} \mathcal{N}(N_0, \frac{N_0^2}{M}) & \mathcal{H}_0 \\ \mathcal{N}(P_k^i + N_0, \frac{(P_k^i + N_0)^2}{M}) & \mathcal{H}_1 \end{cases} \tag{3}$$

where r_k^i is an SU u_i's RSS value over the kth channel. $\mathcal{H}_0$ denotes the channel is idle, and $\mathcal{H}_1$ denotes the channel is busy. P_k^i is u_i's received signal power for spectrum k, and M is the signal sample number. N_0 is the noise power. Thus no matter a channel k is idle or not, for each SU, the RSS value of this channel will always follow a normal distribution which could also be denoted as $r_k \sim \mathcal{N}(\mu_k, \delta_k^2)$, where μ_k is the mean value and δ_k is the standard variance. According to the property of normal distribution, we could get following lemma:

Lemma 1 An SU's sensing report $\mathcal{R} = \{r_1, r_2, \cdots, r_n\}$ follows a multi-dimensional normal distribution $\mathcal{N}(\vec{\mu}, \Sigma)$, where $\vec{\mu} = (\mu_1, \mu_2, \cdots, \mu_n)$, and Σ is a diagonal matrix $diag(\delta_1^2, \delta_2^2, \cdots, \delta_n^2)$.

Proof: See Appendix A.

According to Lemma 1 and equation (1), the sensing reports submitted by all η SUs of a group should follow a Gaussian Mixture Model. But the sensing reports slightly modified and submitted by free-riders can still pretend to be real and legitimate, according to the following lemma:

Lemma 2 The *new* sensing report generated from SRD attack follows a multi-dimensional normal distribution $\mathcal{N}(\vec{\mu}, \Sigma + \delta_0^2 I)$, where $\vec{\mu}$ and Σ are the same with Lemma 1, I is a n-dimensional unit matrix $diag(1, 1, \cdots, 1)$ and δ_0 is the variance of the added Gaussian white noise. The correlation between the *new* sensing report and the original sensing report is $(\frac{\delta_1}{\sqrt{\delta_1^2+\delta_0^2}}, \cdots, \frac{\delta_n}{\sqrt{\delta_n^2+\delta_0^2}})$.

Proof: See Appendix B.

Lemma 2 implies that a *new* sensing report generated from SRD attack still follows a multi-dimensional Gaussian distribution, and it is the similar with the SRM attack. If a free-rider bounds the maximal correlation $max\{\frac{\delta_i}{\sqrt{\delta_0^2+\delta_i^2}}\}(i = 1, \cdots, n)$ smaller than a predetermined boundary, the modified sensing reports will not be distinguished effectively by a malicious behavior detection method.

B. Overclaim Selfishness Detection Scheme

Overclaim Selfishness Detection Scheme (OSDS) is proposed to detect the selfishness in cluster-based collaborative spectrum sensing. The basic idea of OSDS is based on the fact that a classification method could aggregate the sensing reports which share a high shadowing correlation, i.e. higher than 0.3 [2], and it is also inspired by the observation that the spatial diversity exists in the sensing data [5], which means the SUs in different locations, even though within a close proximity, will have different sensing results with shadowing correlation small enough to be distinguished. This observation has been proved by both [5] and [11]. OSDS is based on GMM which could be solved by EM algorithm.

According to Lemma 1, if we assume, the shadowing correlation [2] between any two locations is small enough, an ideal result of GMM classification should divide the sensing reports into different Gaussian distributions. Since each SU submits his sensing report in every time slot, the quantity of each SU's sensing reports should be the same. Thus the mixture weight $w_j (j = 1, 2, \cdots, m)$ of GMM should be close to $\frac{1}{m}$. But if the sensing reports include free-riders' SRD or

SRM attack reports, the classification result will reveal the selfishness, because the mixture weight of some data clusters will be close to zero, and some will be much larger than $\frac{1}{m}$. Thus, when we count the total number of all the data clusters, we will dismiss the data cluster with quite a small weight.

Further, since the estimation likelihood of GMM is super-linear shown as equation (2) and the approximate algorithm EM may not predict the exact result of a GMM, which may lead to extremely high false positive and false negative rate, we will combine the data clusters whose centers are close to each other to exclude the false positive/negative incurred by EM algorithm. If μ_i and μ_j of two data clusters are close enough, which means $\|\mu_i - \mu_j\| \leq \epsilon$, where ϵ is a predetermined threshold for the components, these two data clusters will be determined belonging to a same data cluster. Thus if the classification result includes η Gaussian distributions as same as a group claims, the group is judged as honest, or the classification result will have less than η Gaussian distributions, then it will be judged as a selfish group.

This is the ideal result of a simple classification approach, but our experiment result doesn't support this conjecture. The reason is that the inherent shadowing correlation in a close proximity and the spatial diversity in a relative large range are bounded if the correlation threshold has been given. For example, we predetermine a shadowing correlation threshold which is 0.3 [2], and the shadowing correlation is $c = e^{-\alpha d}$. The minimal distance d_{min} could be estimated based on the predetermined shadowing correlation threshold [2]. Then the maximal possible classification number N_c could be roughly estimated (the estimation method is shown in our full paper due to the page limitation). Thus we need to estimate N_c of a group in a proximity first, then if the number of data clusters in the classification result is larger or equal to N_c, the group is determined to be honest, otherwise, it is a selfish group.

The OSDS algorithm is shown in Algorithm 1.

Algorithm 1: OSDS

```
Execute EM algorithm to get μ_i, i = 1, 2 ··· η of GMM
for each data cluster with μ_i do
  for any other data cluster with μ_j do
    if ‖μ_i − μ_j‖ < ε then
      combine these two data clusters as one
    end if
  end for
end for
count the total number of all the combined data clusters m̂.
estimate the threshold N_c
if m̂ < N_c then
  It is a selfish group.
else
  It is an honest group.
end if
```

Based on OSDS, we further propose an incentive scheme to rule out the selfishness by bounding the benefit of the cluster-based collaborative spectrum sensing.

C. Incentive Scheme

In distributed CRN, even if most of OS attacks could be detected by OSDS, it is impossible to punish the OS attacker directly because punishment will also affect other honest groups [7]. For the sake of maintaining a good cooperation, in this section, we propose an adaptive incentive scheme to stimulate rational groups to behave honestly.

In the cooperation, the collaborator could choose to be an honest group, or an OS attacker. And we assume every group is able to launch OSDS scheme to detect potential selfish groups. For the simplicity of derivation, here we model the problem as 2-player infinitely repeated game, (multi-players' gaming result could be obtained similarly)which is shown as follows:

Definition 1: *The Collaborative Spectrum Sensing Game is the game:*

$$G = \langle N, \{a_{i,t}\}, \{u_{i,t}\} \rangle$$

- $N = 1, 2$ is the set of players
- $a_{i,t} \in \{0, 1\}$, is the action of player i in round t. 0 means the player launches OS attack, and 1 means the player behaves honestly.
- $u_{i,t}$ is the utility of player i in round t.

Without a proper strategy, the game will end up with no honest groups, because the Nash Equilibrium of the game is that every group chooses to violate an honest cooperation. In addition, a simple tit for tat strategy does not fit our game for the possibility of false detection by applying OSDS. Once a group is wrongly detected to be a selfish one by the other, the cooperation will end forever. As a result, we deploy a *Carrot-and-Stick* strategy [7], which is a self-adaptive one and could be defined as follows:

Definition 2: *In a Carrot-and-Stick strategy, player i has the following actions:*

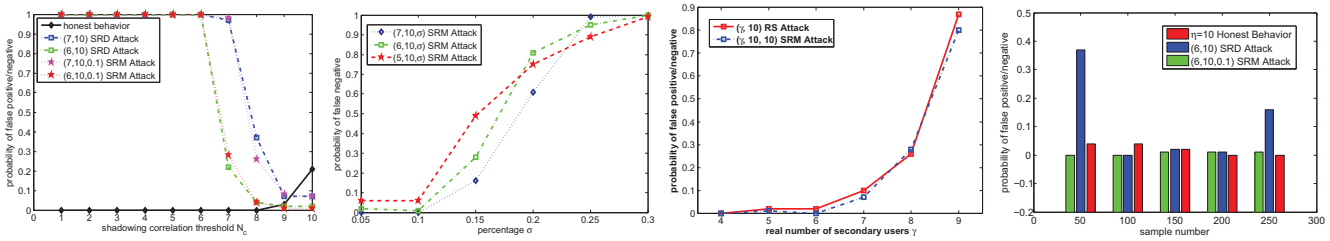
- $a_{i,1} = 1$
- $a_{i,t+1} = 0$ if $a_{i,t} = 1$ and $a_{-i,t} = 0$
- $a_{i,t+1} = 1$ if $a_{i,t} = 0$ and $a_{-i,t} = 0$

Cooperation stops if there is any violation and continues if they both deviate. And it is adaptive to the occurrence of incorrectly identifying an honest group as a selfish one (or called false positive) due to its ability of recovery.

Before discussing how Carrot-and-Stick strategy influences our game, we would firstly define a few parameters we will use. First, we normalize the benefit from cooperation as 0 when the other group launches OS attack, and we assume the benefit from fully cooperation is b. The corresponding cost for the honest group is c, and for the selfish group is d, where $d < c$. The probability of false positive(defined above) is supposed to be p_f, while the probability of false negative (mistaking a selfish group to be an honest one) is p_m. And finally we have

Lemma 3: With 2 player Carrot-and-Stick strategy for cluster-based collaborative spectrum sensing, robust cooperation could be achieved when

$$b > \frac{(1+p_f)(1-p_m)X \times c - (1-p_m\sigma)Y \times d}{(1-p_m)X - (1-p_m\sigma)Y} \quad (4)$$



(a) False positive/negative rate varies with correlation threshold N_c (b) False negative rate varies with σ (c) False negative rate varies with γ (d) False positive/negative rate varies with the number of data sample M

Fig. 2. The experimental results of OSDS under different parameters.

$$X = (1 + \sigma - p_m\sigma), Y = (p_f\sigma + p_f\sigma^2 + 1)$$

Proof: See Appendix C.

Lemma 3 implies when the benefit from fully cooperation satisfies the condition of Lemma 3, an effective incentive scheme will be achieved among rational groups.

IV. Experimental Results

In this section, the experimental results are shown to demonstrate the effectiveness of OSDS.

A. Experiments Setup

Our experiment is set up at the Building of Electronic Information and Electrical Engineering School located in Shanghai Jiao Tong University, Minhang Campus. We use Universal Software Radio Peripheral (USRP) with a TVRX daughterboard (50 MHz to 860 MHz Receiver) and a wide band antenna (70 MHz to 1000 MHz) to detect TV broadcasts (channels of $662-670$MHz,$750-758$MHz and $798-806$MHz) of 10 sampled regions at the building. The sensing reports in each sampled location follows a Gaussian distribution statistically, and differs from other locations which verifies the experiment result of [9] and [11].

B. Simulation Results

Utilizing the sensing data obtained in the real world experiment, we simulate a series of SRD and SRM attacks with different parameters to demonstrate how well our proposed OSDS could filtering OS attacks, and to analyze how these parameters will affect the performance of OSDS.

Firstly we estimate the shadowing correlation threshold N_c of the three channels we scanned, and N_c is 9 in this $150m \times 150m$ region. Given the threshold N_c and the claimed number η, we could get the false positive and false negative rate of OSDS as shown in Fig. 2.(a). The curve of the honest behavior reflects the false positive rate, and the others show the false negative rate. As we will see when $N_c = 9$, both false positive and false negative rate are lower than 10%, which is the best tradeoff of OSDS. This verifies the estimation result and substantiates OSDS could achieve a good selfishness detection performance.

In SRM Attack, the percentage of chosen modified channels will affect the false negative rate. In Fig.2.(b), we could see false negative rate of the three curves respectively holding $\gamma = 5, 6, 7$ remain low when σ is restricted within 0.1. With a higher rate of modified channels a SU will be detected as a malicious user, which is not considered in this paper. So we can define the boundary between selfishness and maliciousness as $\sigma = 0.1$.

Fig.2.(c) shows the relationship between γ and the false negative rate. It means that when a claiming number of SUs $\eta = 10$, the less the number γ of reals sensing reports there are, the better performance the OSDS will achieve. We could see that when $\gamma \leq 7$, the OSDS could achieve almost 100% selfishness detection rate. Please notice that under the circumstance when $\gamma = 9$, a sufficient location diversity has already been achieved for the correlation threshold is estimated to be N_c, even though the selfish group containing 1 free-rider is not detected. OSDS could tolerate this slightly selfish behavior which will not decrease the performance of collaborative spectrum sensing.

Fig.2 (d) implies that the number of data sample used in OSDS affects little on the performance of OSDS when $M \geq 100$ for the false positive and false negative rate fluctuate slightly. Therefore a data sample with the number of $M = 100$ is recommended to launch OSDS, and if the time slot $t = 2s$, 200s is needed for clusters to launch OSDS every time.

V. Conclusion

In this paper, we identify a new selfish model in cluster-based collaborative spectrum sensing between cooperating groups, which is named as Overclaim Selfishness. To address OS attack, we propose an Overclaim Selfishness Detection Scheme to detect the potential selfish groups. Further, in order to stimulate rational groups to behave honestly, we propose an incentive game. The effectiveness and the efficiency of OSDS are also demonstrated by our experiment. And our future works will focus on a single user's selfish behavior detection in collaborative spectrum sensing.

ACKNOWLEDGEMENT

This research is supported by National Natural Science Foundation of China (Grant No.61003218, 70971086, 61161140320, 61033014), Doctoral Fund of Ministry of Education of China (Grant No.20100073120065).

REFERENCES

[1] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications (JSAC)*, Vol. 23, No. 2, pp. 201- 220, Feb. 2005

[2] H. Kim, and K.G. Shin, "In-band Spectrum Sensing in Cognitive Radio Networks: Energy Detection or Feature Detection?," in *Proc. of MOBICOM*, 2008.

[3] I.F. Akyildiz, B.F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communication (Elsevier) Journal*, Vol. 4, No. 1, pp. 40-62, Mar. 2011

[4] T. Chen, H. Zhang, G.M. Maggio, and I. Chlamtac, "CogMesh: A Cluster-based Cognitive Radio Network," in *Proc. of IEEE DySPAN*, pp. 168 - 178, Apr. 2007.

[5] P. Bahl, R. Chandra, T. Moscibroda, R. Murty, and M. Welsh, "White Space Networking with Wi-Fi like Connectivity" in *Proc. of SIGCOMM*, 2009.

[6] H. Kim, J. Choi, and K.G. Shin, "Wi-Fi 2.0: Price and quality competitions of duopoly cognitive radio wireless service providers with time-varying spectrum availability," in *Proc. of INFOCOM*, 2011.

[7] C. Song and Q. Zhang, "Achieving Cooperative Spectrum Sensing in Wireless Cognitive Radio Networks," in *ACM MC2R, Special Issue on Cognitive Radio Technologies and Systems*, Vol. 13, Issue 2, Apr. 2009.

[8] B. Wang, K.J.R. Liu, and T.C. Clancy, "Evolutionary Cooperative Spectrum Sensing Game:How to Collaborate?," *IEEE Transactions on Communications*, Vol. 58, No. 3, pp. 890 - 900, Mar. 2010.

[9] O. Fatemieh, A. Farhadi, R. Chandra, and C.A. Gunter, "Using Classification to Protect the Integrity of Spectrum Measurements in White Space Networks," in *Proc. of NDSS*, 2011.

[10] S. Li, H. Zhu, B. Yang, C. Chen, X. Guan, "Believe Yourself: A User-Centric Misbehavior Detection Scheme for Secure Collaborative Spectrum Sensing" in *Proc. of ICC*, 2011.

[11] S. Li, H. Zhu, Z. Gao, X. Guan, and S. Shen, "Location Privacy Preservation in Collaborative Spectrum Sensing," in *Proc. of INFOCOM*, 2012.

[12] C.M. Bishop, "Pattern Recognition and Machine Learning," Springer, 2006.

[13] A. Min, K. Shin, X. Hu, "Secure Cooperative Sensing in IEEE 802.22 WRANs Using Shadow Fading Correlation," *IEEE Trans. on Mobile Computing*, Vol. 10, pp. 1434 - 1447.

[14] H.H. Andersen, M. Hojbjerre, D. Sorensen, and P.S. Eriksen, "Linear and Graphical Models: For the Multivariate Complex Normal Distribution," (1995) lecture notes in statistics 101, New York: Springer-Verlag, ISBN 0-387-94521-0.

APPENDIX

A. Proof of Lemma 1

The PU we considered in this paper are presumed to be independent with each other, so for each $r_k \sim \mathcal{N}(\mu_k, \delta_k^2)$ must be independent with $r_j, j \neq k$. The characteristic function of a sensing report $\mathcal{R}$ is:

$$\varphi_{\mathcal{R}=(r_1,r_2,\ldots,r_n)}(\vec{u}) = \Pi_{k=1}^{n} \varphi_{r_k}(u_k)$$
$$= \Pi_{k=1}^{n} \exp\left(i\mu_k u_k - \frac{1}{2}\delta_k^2 u_k^2\right)$$

It is the characteristic function of multi-dimensional Gaussian distribution $\mathcal{N}(\vec{\mu}, \Sigma)$, where $\vec{\mu} = (\mu_1, \mu_2, \cdots, \mu_n)$ and Σ is a diagonal matrix $diag(\delta_1^2, \delta_2^2, \cdots, \delta_n^2)$. According to the bijection property of characteristic function [14] that $F_{X_1} = F_{X_2} \Leftrightarrow \varphi_{X_1} = \varphi_{X_2}$, where F_X is the distribution function of the random variable X. Therefore $\mathcal{R} \sim \mathcal{N}(\vec{\mu}, \Sigma)$

B. Proof of Lemma 2

Without loss of generality, we consider a single channel i of the sensing report which follows a Gaussian distribution $\mathcal{N}(\mu_i, \delta_i^2)$. Since the noise n of sensing report added by free-rider follows another Gaussian distribution $\mathcal{N}(0, \delta_0^2)$ in SRD attack. Thus the *new* sensing report of a channel i follows $\mathcal{N}(\mu_i, \delta_i^2 + \delta_0^2)$. Then similar with the proof of Lemma 1, the *new* sensing report still follows a multi-dimensional Gaussian distribution $\mathcal{N}(\vec{\mu}, \Sigma + \delta_0^2 I)$.

The correlation a single channel i between the *new* sensing report r_i' and the original sensing report r_i is:

$$corr = \frac{Cov(r_i', r_i)}{\sqrt{D(r_i')D(r_i)}} = \frac{Cov(r_i + n, r_i)}{\delta_i \sqrt{\delta_i^2 + \delta_0^2}}$$

n is the Gaussian noise added by free-riders, according to the property of covariance,

$$corr = \frac{Cov(r_i, r_i) + Cov(n, r_i)}{\delta_i \sqrt{\delta_i^2 + \delta_0^2}} = \frac{\delta_i}{\sqrt{\delta_i^2 + \delta_0^2}}$$

here $Cov(n, r_i)$ is 0 because we assume the added noise n is independent with the sensing result r_i. Thus the correlation between the *new* sensing report and the original sensing report is $(\frac{\delta_1}{\sqrt{\delta_1^2+\delta_0^2}}, \cdots, \frac{\delta_n}{\sqrt{\delta_n^2+\delta_0^2}})$.

C. Proof of Lemma 3

Firstly we adopt the *average discounted payoff* of an infinitely repeated game as $U_i = (1-\sigma)\sum_{t=1}^{\infty} \sigma^{t-1} u_{i,t}$, where $\sigma \in (0, 1)$ is the discount factor. Then we assume the average discounted payoff of group i as U_i when cooperates while $\hat{U}_i$ when it deviates.

Thus in the 1st stage, if group i chooses to behave honestly, it might be detected to be the attacker. Then, the game results could be shown as in TABLE.I.

t	a_{it}	a_{-it}	u_{it}
1	1	1	b-c
2	1	0	-c
3	0	0	0
⋮	⋮	⋮	⋮

TABLE I

We could obtain the overall payoff matrix in this case as $U_i^* = (1-\sigma)(b-c-\sigma\times c+0+\sigma^3 \times \frac{U_i}{1-\sigma})$. In the complementary case, that is to say, this group is detected to be honest, the payoff is $U_i^{**} = (1-\sigma)(b-c+\sigma \times \frac{U_i}{1-\sigma})$. Therefore, the expected overall payoff could be shown as $U_i = p_f \times U_i^* + (1-p_f) \times U_i^{**}$. By solving the above equation, we have

$$U_i = \frac{b - (1+\sigma p_f)c}{1 + \sigma p_f (1+\sigma)}$$

On the other hand, the game result is given when the group chooses to launch OS. We assume the misbehavior is detected in the kth stage of the game. Because the probability of first detection of the misbehavior in kth stage is $p_m^{k-1}(1-p_m)$, the average discounted payoff could be obtained similarly:

$$\hat{U}_i = (1-p_m)((1-\sigma)(b-d)\sum_{k=1}^{\infty} p_m^{k-1} k + U_i \sum_{k=1}^{\infty} p_m^{k-1} \sigma^{k+1})$$

The game achieves full cooperation if and only if $\hat{U}_i < U_i$. We could get the result in Lemma 3 by solving this inequality.