International Journal of Multimedia and Ubiquitous Engineering
Vol.12, No.9 (2017), pp.27-40
http://dx.doi.org/10.14257/ijmue.2017.12.9.03

A Stackelberg Game Spectrum Sensing Scheme with Malicious Users in Cooperative Cognitive Radio Networks

Shuyan Xiao, Shuqi Liu and Yang Yu

School of Electrical and Information Engineering, JiangSu University of Technology
xiaosy@jsut.edu.cn, dxlsq@jsut.edu.cn, dxyy@jsut.edu.cn

Abstract

Aiming at solving the problem of the spectrum sensing data falsification attack in cognitive radio networks, a novel spectrum sensing scheme with malicious users that reports the presence of primary user with certain probability, in which Stackelberg game is adopted to improve the sensing performance. Considered as leaders, users with acceptable reliability will share their sensing observations with the ones experiencing malicious and fading channel conditions. According to the reliability difference between the malicious users and other users, the proposed scheme can indentify malicious users easily. The performance of the Stackelberg game scheme is investigated and compared with schemes which don't employ Stackelberg game. It proves the benefits of the proposed scheme.

Keywords: *spectrum sensing; energy detector; Stackelberg game; malicious users*

1. Introduction

With the ever-increasing demand on high date rate communications and wider bandwidth, the frequency spectrum becomes more and more scarce. Cognitive Radio (CR) [1] technology proposed by Mitola has been considered as a potential technology to improve spectrum utilization by sharing the dynamic spectrum band. Spectrum sensing has been considered as the key element of CR. Through sensing spectrum of the primary user's, secondary user (SU) can utilize the spectrum when it is idle without interfering in the transmissions of licensed user, also known as primary user (PU).

Several detection algorithms [2] are proposed to sense the PU signal such as energy detection [3], matched filter detection [2], and cyclostationary detection [2]. Nevertheless, these detection algorithms are susceptible to the impact of hidden terminal due to the path loss, receiver uncertainty and shadowing. This problem brings up collaboration spectrum sensing (CSS) [4-7] studied extensively which is a very effective detection scheme and can greatly improve detection performance at a certain cost.

But these schemes assume that all SUs are honest and all cognitive users' local sensing results are treated equally. When a malicious user (MU) appears in the cognitive radio network (CRN), it may counterfeit the local sensing information [8] and send false sensing results to the central fusion center (FC), which will damage the spectrum sensing performance greatly. This phenomenon is called spectrum sensing data falsification (SSDF) attack [8]. SSDF attack can result in serious problems because false sensing result may reduce the detection performance of CSS [9] while many schemes are vulnerable to MUs. For the reason that MUs are adaptive, unpredictable, simple prevention is not enough and robust and MU detection schemes are required. In relevant literatures [9]-[13], there are various schemes proposed to identify MUs. For example, pre-filtering of sensing results with MU detection is developed in [9]. MU's observations are sensing

Received (December 22, 2016), Review Result (August 25, 2017), Accepted (September 1, 2017)

ISSN: 1975-0080 IJMUE

results which different from the rest of the results. In [10] the proposed MU detection algorithm calculates the trust and consistency values of SUs based on their past reports. If the consistency value and the trust value fall below certain thresholds, the SU is characterized as an outlier and its reports are not considered for the final decision. However, only one MU has been considered and needs some PU's relevant prior knowledge in this paper. The authors in [11] use a reputation metric to detect and isolate MUs from legitimate SUs. Through the computation of this metric, the output of each SU is compared with the decision made by the FC. If the reputation metric of a user exceeds a predefined threshold, its decisions are isolated and thus not used by the FC. But in this work, the reputation metric of a user depends solely on the difference between the observations this user reports and the decision finally made by FC, which is very complicated to implement and has bad robustness. The MU detection scheme proposed in [12], which is based on Anderson-Darling (AD) statistics, tests whether the empirical distribution of each SU fits the expected distribution of a MU. Moreover, the detected MUs are cutting off from the sensing data combined with the rest at the FC and the authors assume that the MU is 'always yes' user in this context.

With the schemes for detecting MUs attack being mature, more hidden problems destructive to CR system is produced by MUs. For example, MU would send the message that there is primary signal present with a certain probability, which is called probability malicious user ('PMU') in this paper that will be discussed in detail in Section 2.1 of this paper. 'PMU' is difficult to be identified. To address this problem, a Stackelerg game [14] is developed for spectrum sensing scheme with malicious users which works as follows: Based on reliability of SU, a SU is considered as a MU ('always yes' user, 'always no' user or 'PMU') or a non-malicious user. A SU can be considered as a leader or a follower while a MU must be considered as a follower. Because of the good PU signal reception, leading SUs have higher reliability and they can broadcast their sensing observations to other SUs. On the other hand, following SUs only look for announced sensing results broadcasted by leading SUs to discover whether a primary signal is present. The contributions of the proposed scheme can be summarized as follows:

1) 'PMU' is identified utilizing the proposed scheme, which has not been studied temporarily in the previous literatures. This is an intelligent attacker which is hidden and difficult to be identified.

2) Based on the reliability of SU, FC determines each SU as a leader or a follower by adopting Stackelberg game theory to enhance the sensing performance of the CRN. Stackelberg game theory is usually applied in spectrum and power allocation in CRN but it is seldom used in spectrum sensing.

3) The proposed algorithm has low implementation complexity and good robustness, for the reason that we compute the reliability of SUs based on their own reporting energy and signal to noise ratios (SNR) in the proposed scheme.

4) The identified MUs aren't removed from the cooperative sensing process but follow the leading SU's movement, thus improve the sensing performance of the CSS in this paper.

Game theory is a mathematical tool which analyzes the strategic interaction among multiple decision makers. In recent years, the application of game theory in CRN has obtained great attention from resource allocation, power control, routing and communications. Literature [14] gives an overall summary of the application of game theory in CR system. Stackelberg game is a strategic game considering two types of players: leaders and followers. Always the leader moves first and the follower moves sequentially. Knowing of the leader's move, the follower can make a move to optimize its own objective function. For example, this game is applied in literature [15] for the goal of power allocation in CRN.

The rest of this paper is organized as follows: Section II represents the system model while Section III represents the proposed Stackelberg game scheme with malicious users. Then the simulation results and conclusions are given in Section IV and V respectively.

2. System Model and Formulation

Consider that a CRN consists of one primary transmitter and N SUs which are denoted by $\mathrm{SU}_i, i = 1..., N$. Figure 1 illustrates a scenario where SU_3 is a MU and SU_6 is sheltered from some obstacle in PU-SU_6 path. Furthermore, it is assumed that there is a signaling channel among SUs so that they can communicate with each other.

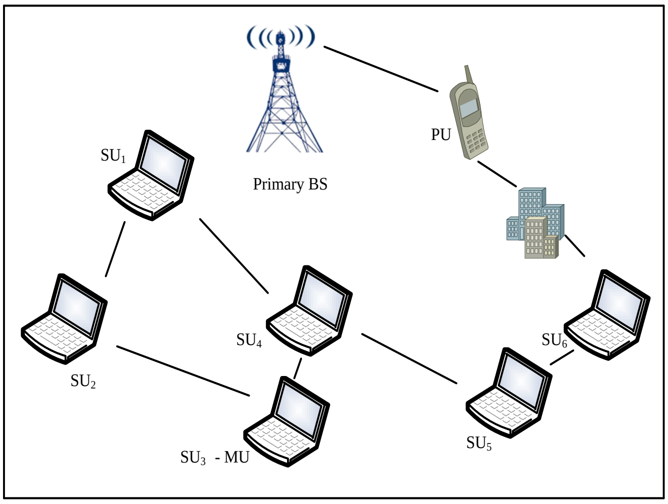


Figure 1. System Model of Proposed Spectrum Sensing Scheme with Mus

Assume all the SUs are using energy detector with the same parameters in this paper. The detection problem for local sensing at SUs can be stated in terms of a binary hypothesis test, with the hypothesis H_0 indentifying the absence of the PU signal, and alternative hypothesis H_1 denoting that PU is active, as

$$\begin{cases} H_0 & y_i(t) = n_i(t) \\ H_1 & y_i(t) = h_i(t) \otimes s(t) + n_i(t) \end{cases} \tag{1}$$

Here y_i represents received signal at SU with $s(t)$ being the primary signal, $n_i(t)$ being the additive white Gaussian noise while $h_i(t)$ represents the fading coefficient. $s(t) \sim N(0, \sigma_s^2), n_i(t) \sim N(0, \sigma_n^2)$.

In energy detection, Y is compared with the threshold λ to make a decision out of two hypotheses: H_0, H_1. If Y is equal to or greater than λ, the PU is identified to be present, otherwise absent.

$$\begin{cases} Y \geq \lambda & H_1 \\ Y < \lambda & H_0 \end{cases} \tag{2}$$

The output of the integrator Y received by a single SU is

$$Y = \sum_{i=1}^{2TW} \left| x_i \right|^2 \tag{3}$$

Here x_i is the $i-th$ sample of received signal at SU from PU, and TW is the time-bandwidth product. When $TW > 125$, Y can be approximated as a Gaussian random variable under both hypotheses H_0 and H_1, with mean μ_0, μ_1 and variance σ_0, σ_1 respectively [11].

$$\begin{cases} \mu_0 = 2TW \qquad , \sigma_0^2 = 4TW \\ \mu_1 = 2TW\left(\bar{\gamma}+1\right), \sigma_1^2 = 4TW\left(2\bar{\gamma}+1\right) \end{cases} \tag{4}$$

Here $\bar{\gamma}$ is the signal to noise ratio of the PU transmitting signal at the SU.

If the PU is active and the sensing result is H_1, this scenario is known as perfect detection, and the corresponding probability is referred to the probability of detection, which is denoted by P_d. If the PU is inactive and the sensing result is H_1, this scenario is known as false alarm, which is denoted by P_f . When energy detection is used, P_d and P_f are given by:

$$P_d = P\left\{Y > \lambda \mid H_1\right\} = \frac{1}{2} erfc\left[\frac{\lambda - 2TW - 2TW\gamma}{2\sqrt{2}\sqrt{TW\left(1+2\gamma\right)}}\right] \tag{5}$$

$$P_f = P\left\{Y > \lambda \mid H_0\right\} = \frac{1}{2} erfc\left[\frac{\lambda - 2TW}{2\sqrt{2}\sqrt{TW}}\right] \tag{6}$$

$$erfc(z) = \left(\frac{2}{\sqrt{\pi}}\right)\int_z^{\infty} \exp\left(-x^2\right)dx \tag{7}$$

2.1. Impact of Malicious Users

MUs can degrade the performance of spectrum sensing in CRN. The behaviors of MUs may be unintentional or intentional however which will significantly affect the detection of PU signals. There are three kinds of MUs: ‘always yes’ users, ‘always no’ users and ‘PMU’. The following are the detail interpretations of the three kinds of MUs.

1) ‘Always yes’ users always send high energy values regardless of the primary signal being present or not, which will increase P_f and decrease the throughput of CR system.

2) ‘Always no’ users always send low energy values no matter the primary signal is present or absent, which will decrease the P_d and cause interference to the PU system.

3) ‘PMU’ sometimes sends high energy values while sometimes low energy values. In other words, it sends the message there being primary signal present with a certain probability P_t. The intentions of ‘PMU’ are divided into two aspects. On one hand, ‘PMU’ may try to disrupt the sensing results of CSS in order to provide more spectrum opportunities for themselves and introduce interference to PU severely. On the other hand, ‘PMU’ may don’t sense the CR environment but just send an intentional results to cope with the FC, in order to save energy consumption, thereby selfishly transmitting their own signals on the free channel.

Thus, MUs detection schemes should be efficient in identifying MUs who send the false sensing results to the FC and detecting a non-malicious user having a good channel condition. Since the MUs detection schemes cannot judge whether a PU is present or not, identifying MUs in sensing spectrum of CR system is very difficult and important.

2.2. Identifying Malicious Users

P_d and P_f of 'always yes' users are '1' as the P_d and P_f of 'always no' users are '0'. Because the pattern of 'always yes' and 'always no' users' parameters is easy to identify and these kinds of users do not have to know any spectrum status information, so these kinds of attacks are easy to realize. MU detection and the security of the CSS with 'PMU' have not been studied temporarily. In this section we will give the characteristics of 'PMU' firstly, and then investigate how to differentiate this hidden MU to ensure the performance of CSS.

Assume that 'PMU' sends the message that there is primary signal present with a certain probability P_t . P_d of 'PMU' can be written as:

$$P_d = P\left\{H_{1t} \mid H_1\right\} \tag{8}$$

Here H_{1t} denotes 'PMU' announcing the presence of primary signal and H_1 represents the primary signal being present in actual performance. Since MUs obtain their sensing reports based on their own but not the detection of primary signal, there is no relation to the presence of primary signal. Hence, equation (8) can be rewritten as:

$$P_d = P\left\{H_{1t} \mid H_1\right\} = \frac{P\left\{H_{1t} H_1\right\}}{P\left(H_1\right)} = \frac{P_t \cdot P\left(H_1\right)}{P\left(H_1\right)} = P_t \tag{9}$$

Here $P\left(H_1\right)$ is the priori probability that PU is active.

Meanwhile, the P_f can be written as:

$$P_f = P\left\{H_{1t} \mid H_0\right\} \tag{10}$$

MUs' detection results of the presence of primary signal have no relation to the presence of primary signal as P_d. Hence, equation (10) can be rewritten as:

$$P_f = P\left\{H_{1t} \mid H_0\right\} = \frac{P\left(H_{1t} H_0\right)}{P\left(H_0\right)} = \frac{P_t \cdot P\left(H_0\right)}{P\left(H_0\right)} = P_t \tag{11}$$

From what has been discussed above we can know equation (9) and (11) are decided by P_t . P_d of MU is equal to P_f of MU.

$erfc(.)$ is a monotone decreasing function. In order to prove equation (5) is greater than equation (6), only the following equation (12) needs to be proved:

$$\frac{\lambda - 2TW\left(\gamma + 1\right)}{\sqrt{2\gamma + 1}} < \lambda - 2TW \tag{12}$$

For $\gamma > 0$, there is $\frac{\lambda - 2TW\left(\gamma + 1\right)}{\sqrt{2\gamma + 1}} < \lambda - 2TW$. So it can be obtained that $P_d \geq P_f$ for non-malicious users in energy detection.

In this paper, we defined the reliability of each SU R as follows:

$$R = {}^{P_d}\!/\!_{P_f} \tag{13}$$

From the above mentioned, we can obtain the reliability R of MU is ‘1’ while the non-malicious user’s reliability R is greater than 1. Furthermore, the greater R is the better channel condition is.

In order to categorize SUs into non-malicious users and MUs each SU needs to evaluate its reliability R. Table 1 shows the value range of R. An SU with $R=1$ is considered as a MU and also a follower, otherwise as a non-malicious user. If $R \geq \alpha(\alpha > 1)$, the SU is considered as a leader. Furthermore, $R<1$ and $1<R<\alpha$ identifies SU having a weak channel, so it should be considered as a follower too.

Table 1. The Value Range of Reliability

R	$R \geq \alpha$	$1<R<\alpha$	$R=1$	$R<1$
MU or Non-MU	Non-MU	Non-MU	MU	Non-MU
Leader or Follower	Leader	Follower	Follower	Follower

3. Stackelberg Spectrum Sensing Scheme with Malicious Users

3.1. Stackelberg Game Formulation

In this section, Stackelberg game is applied to design spectrum sensing schemes with MUs. Since SU is considered either as a leader or a follower based on its reliability, the sensing process can be described as a Stackelberg game [14]. Hence, the leaders but not the MUs determine the sensing decision regarding the presence or absence of a primary signal as the followers take actions by leaders. Therefore, the final decision of network is dominated by leaders who are more reliable. Moreover, the leaders can benefit SUs with low reliability. As a result P_d of the whole system will increase since it is dominated by leaders having acceptable reception of the PU. On the assumption that SUs are sharing their sensing observations, the collaborative P_d would be the average over the $P_{d,i}$ per SU as follows:

$$Q_d = \frac{\sum_{i=1}^{n} H_{k,i} P_{d,i}}{\sum_{i=1}^{n} H_{k,i}} \tag{14}$$

Where $H_{k,i} = H_{0,i}$ *or* $H_{1,i}$ represents the sensing bit and also the action of the $i-th$ SU, while n denotes the number of SUs. From equation (14) we can see only in the case $H_{k,i} = H_{1,i}$ will the detection performance be affected.

3.2. The Proposed Scheme for Sensing Process

In the proposed algorithm SUs are divided into two types: leaders or followers based on the reliability R of the SU and MUs which must be followers. Moreover, this paper considers the scene that there is a communication channel among SUs so that the sensing reports can be exchanged between the SUs. Then, the spectrum sensing is carried out according to the Figure 2.

Sensing Process:

Process 1: Each SU employs energy detector to sense local information;

Process 2: After local spectrum sensing is finished, SUs transmit the local sensing results to FC and then FC calculates the reliability of SUs;

Process 3: A judgment will be made by FC. SU would be considered as a follower if $R<1$, else the FC will continue to judge whether $R=1$. If $R=1$, the SU should be considered as a malicious user, otherwise R will be compared with α. If $R \geq \alpha$, the SU is considered as a leading SU, else as a follower.

Process 4: If a SU is considered as a leader, it will broadcast its sensing results to the SUs.

Process 5: If a SU is a MU, it should be considered as a follower but not a leading SU.

Process 6: If a SU is a follower, it requires searching the leaders' sensing observations. If anything found, the follower stops the search and takes the found leader's decision as its decision and the SU catch the sensing results of leaders based on nearly receiving principle.

Process 7: Make judgment whether the Stackelberg game reaches equilibrium. If does the process is end, otherwise go on with process 6. The Stackelberg game reaching equilibrium means that each follower should be paired with only one leader while each leader can have more than one follower.

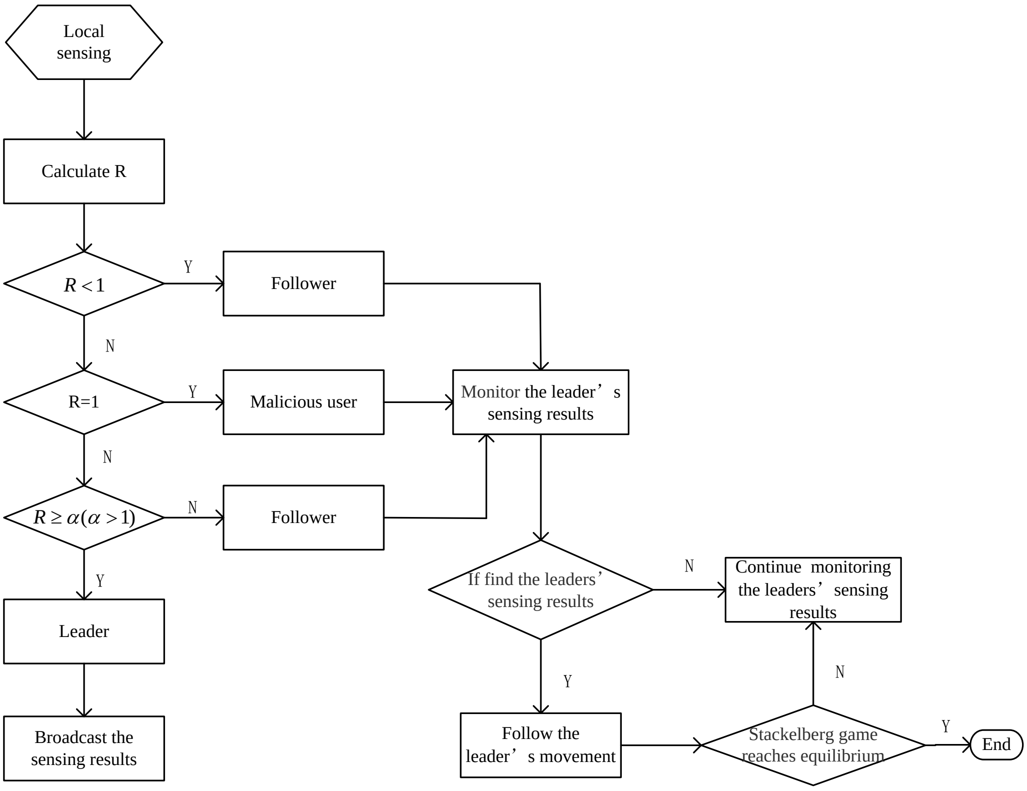

Local sensing
Calculate R
$R<1$
Y
Follower
N
R=1
Y
Malicious user
Monitor the leader's sensing results
N
$R\geq\alpha(\alpha>1)$
N
Follower
Y
Leader
Broadcast the sensing results
If find the leaders' sensing results
N
Continue monitoring the leaders' sensing results
Y
N
Follow the leader's movement
Stackelberg game reaches equilibrium
Y
End

Figure 2. Flow Chart of Stackelberg Game Spectrum Sensing Scheme with Malicious User

We take Figure1 as an example to explain the process of the propose scheme. Figure 1 illustrates a scenario where SU_3 is a MU and SU_6 is shadowed over PU-SU_6 path, so SU_3 and SU_6 should be seen as a follower while the other SUs as leaders. In this case, SU_1 SU_2 SU_4 SU_5 will broadcast their sensing observations but SU_3 and SU_6 will do nothing but look for the observations of others. Then SU_3 will probably catch the sensing observations sent by SU_4 while SU_6 will probably catch the sensing results sent by SU_5 based on nearby receiving principle. Therefore, SU_3 and SU_6 will have a good reception of the PU signal although they are in malicious and weak channel condition.

4. Simulation Results

In simulation, it is presumed that there are N SUs placed around a PU randomly with the parameters being set as follows: $T=0.001$, $W=5*10\text{^}4$, $\alpha=3$. 100000 Monte

Carlo experiments are implemented in the simulation at different SNR levels between -28 dB and -4 dB.

Figure 3 shows the value range of R under different SNR. Here, parameter α is set to be 3 and the average SNR for leading SUs can be acquired as -11.7 dB.

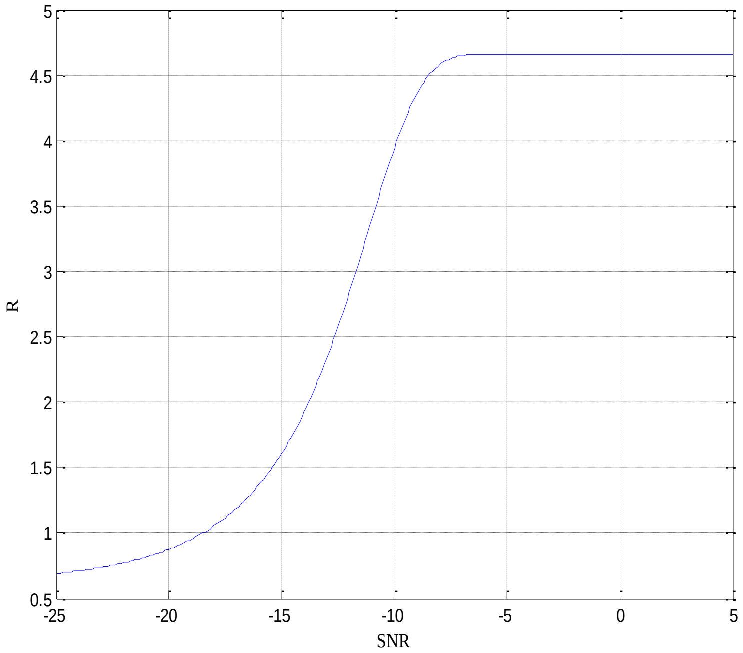


Figure 3. The Value Range of R Under Different SNR

13 cases are simulated in this paper. Case 1 is for the proposed scheme adopting Stackelberg game. Cases 2-13 don't adopt Stackelberg game. In cases 2-5, N is set to be 5 with only one MU ($SNR = -10.0$ dB). Case 2 is for the MU being and 'always no' user. Case 3 is for the MU being an 'always yes' user. Case 4 and 5 are for the MU being a 'PUM' with $P_t = 0.8$ and $P_t = 0.2$ respectively. In case 6-9 N is set to be 6 and there is a MU and a weak user. Case 6 is for the MU being an 'always no' user. Case 7 is for the MU being an 'always yes' user. Case 8 and 9 are for the MU being a 'PUM' with $P_t = 0.8$ and $P_t = 0.2$ respectively. In case 10 there is only one 'PMU' while in case 11 there are two 'PMUs' and case 12 is for three 'PMUs'. In case 13 there is only one weak user (SNR=-15 dB) suffering from deep shadowing.

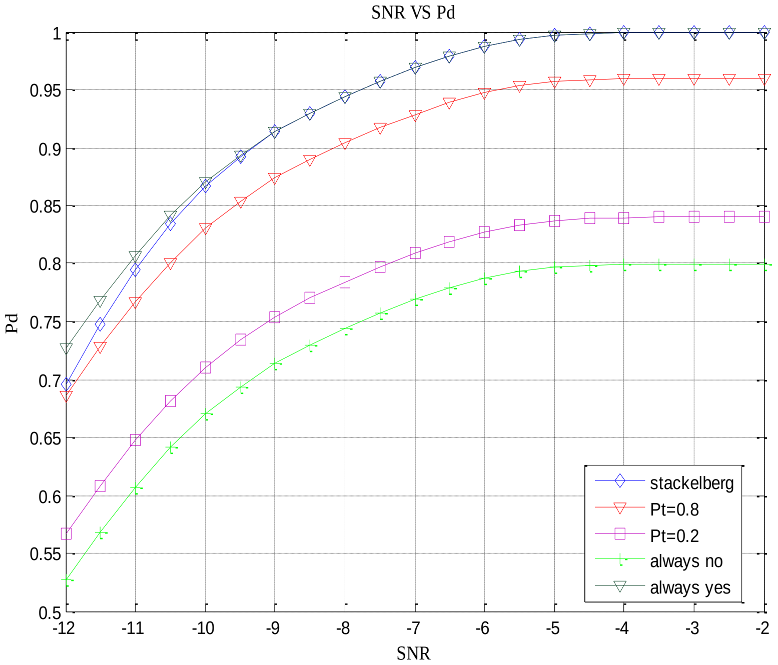


Figure 4. Relationship of P_d and SNR when there is Only One Malicious User

Figure 4 illustrates the relationship of detection probability Pd and the average SNR for cases 1-5. In this case, N is set to be 5 with one MU being a follower and the remaining four being leaders. From Figure 4, it’s seen that the detection performance of Stackelberg scheme is between ‘always yes’ and $P_t = 0.8$. This is because when the SNR>-11.7 dB, P_d of the SU is greater than 0.8. It is obvious in the simulation result that the detection performance of the scheme proposed in this paper is better than the other four schemes when the SNR changes.

Figure 5 consider a more practical scenario, N is set to be 6 with one malicious user and one weak user suffering from deep shadowing. Figure 5 shows the relationship of P_d and the average SNR for case 1 compared with cases 6-9 which don’t employ Stackelberg game. In the proposed scheme, the malicious user (SNR=-10dB) and the weak user (SNR=-25dB) being followers while the remaining four being leaders. The experimental result of the proposed scheme is compared with the ones of other four cases which don’t use the Stackelberg game.

From Figure 5 we can see the detection performance of Stackelberg scheme is better than the other four cases because the appearance of the weak user affects the detection performance of the other four cases. Seen from the simulation result, the proposed scheme increases P_d by 14.17%, 17.88%, 29.04%, and 32.77% at SNR=-12dB compared to ‘always yes’, $P_t = 0.8$, $P_t = 0.2$, and ‘always no’ case respectively. It is obvious that the detection performance of the scheme proposed here is better than the other four schemes when the SNR changes. Compared to Figure 4, proposed scheme achieves the significant improvement in Figure 5. This interesting result can be explained by the fact that in Figure 4 only one MU follows the leading SU’s movement, however, in Figure 5 there are two SUs (one MU and one weak user) following the decisions of leaders. As a result, the more following SUs follow the leaders’ movements, the better the detection performance is.

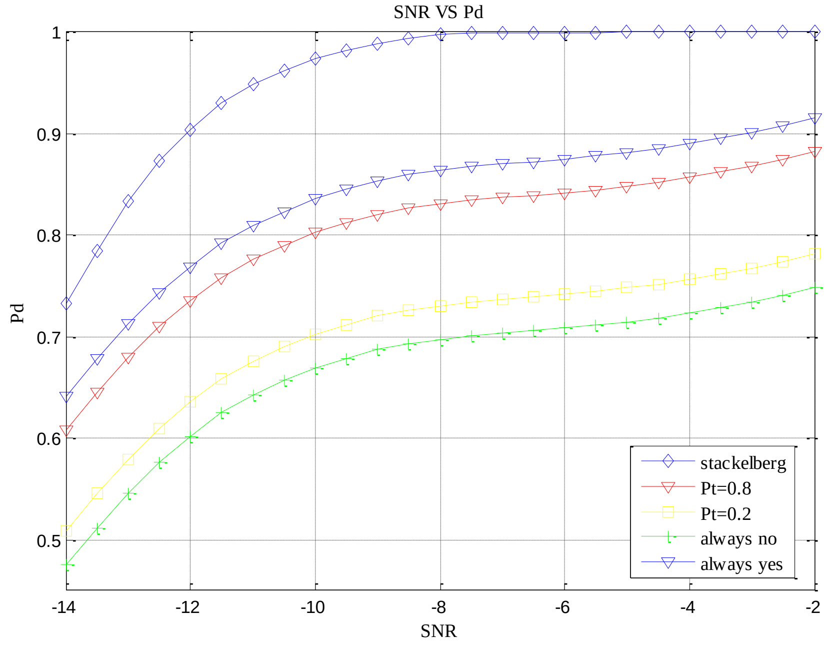


Figure 5. Relationship of P_d and SNR when there is One Malicious User and One User Suffering from Shadowing

Figure 6 shows the ROC curves for case 1, case 4 and case 13. It is obviously obtained from Figure 6 that the performance of the detection performance degrades greatly even when there is only one MU or one weak user. In addition, it can be clearly seen from Figure 5 and Figure 6 that the proposed scheme adopting Stackelberg game can not only improve the detection performance when there is MU but also the weak user appearing in CRN.

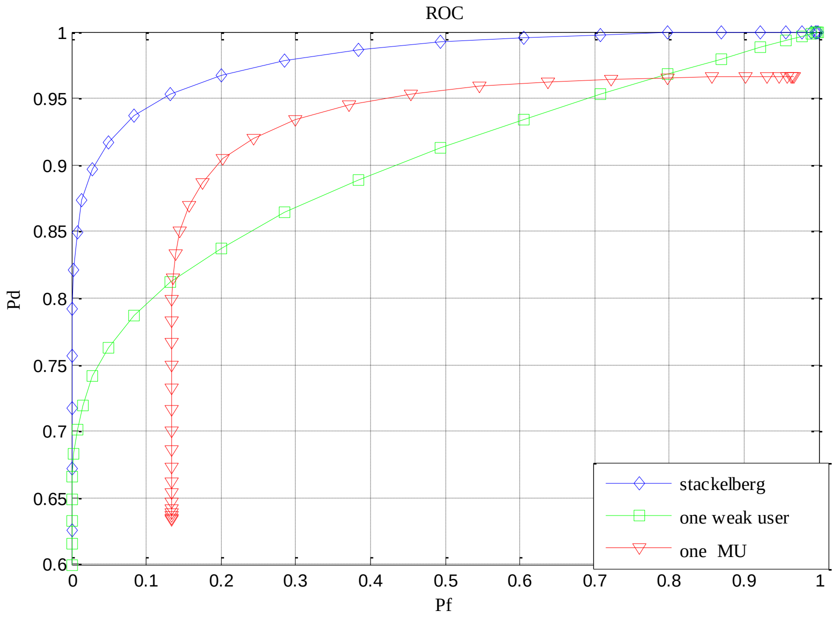


Figure 6. ROC Curves for Different Schemes when there is a Weak User and MU

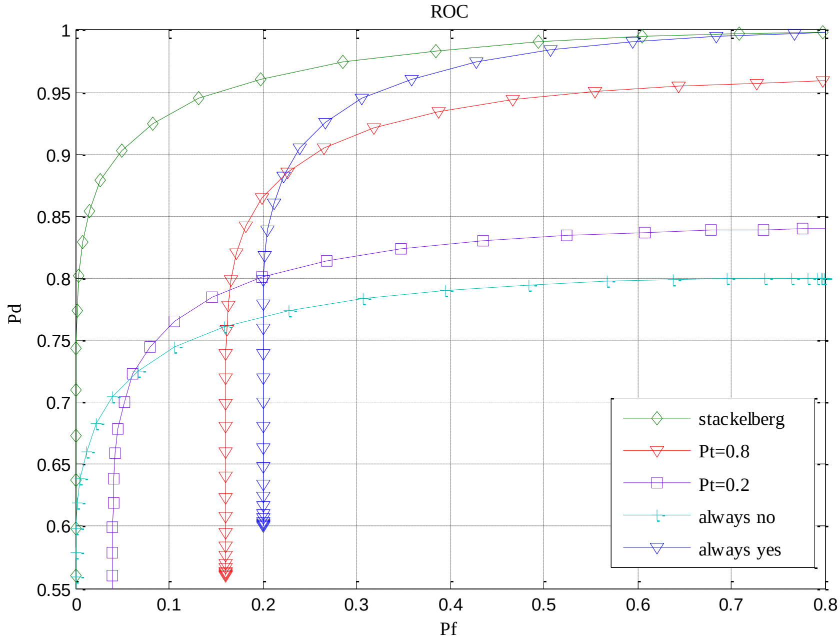


Figure 7. ROC Curves for Different Schemes when there is Only One MU

Figure 7 compares the ROC curves for the proposed Stackelberg game with cases 1-4. From Figure 7, it is seen that, the proposed scheme can identify ‘PMU’, ‘always yes’ user and ‘always no’ user easily and the performance improves with the Stackelberg game. Comprehensive Figure 7 and Figure 4, we can seen ever there is only one MU the detection performance degrades in CSS, in addition, the detection performance of the proposed scheme is better than case 1-4 that don’t adopt Stackelberg game. This result can be explained by the fact that the identified MU follows the decision of leading SU.

Figure 8 considers a more practical scene that there are more than one MU in CRN. In the proposed scheme, all of the MUs should be followers but not the leaders. Figure 8 shows the ROC curves for case 1 and case 10-12. It is also seen from Figure 8, the proposed scheme can identify not only one PMU.

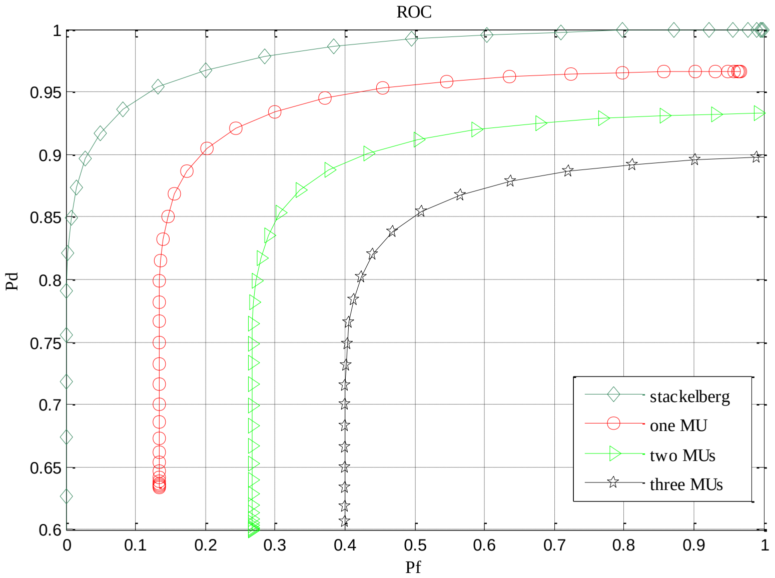


Figure 8. ROC Curves for Different Schemes when there are Different Number of MUs

5. Conclusions

A Stackelberg game spectrum sensing scheme which can identify not only common MUs but also 'PMU' is proposed in this paper. In the scheme, we define P_d / P_f as the reliability (R) of SUs. The greater R is, the better reception of the primary signal is and we identify malicious users through analyzing R of SUs where In addition, based on Stackelberg game SUs are considered as leaders or followers while MUs must be as followers. SUs are considered as leaders or followers while malicious users as followers. The simulation results show that this scheme can obtain a significant performance when SUs are suffering from malicious and weak channel conditions. Finally, in our future research we plan to extend this work for multiple PUs in CRN.

Acknowledgments

This research was supported by the Natural Science Foundation of China (Grant No.61701202), National Science Foundation of Jiangsu Province (Grant No. BK20160294) and National Natural Science Foundation of Jiangsu University of Technology (Grant No. KYY15006).

References

[1] J. Mitola and G. Q.Maguire, "Cognitive radio:Making software radios more personal", IEEE Personal Communication, vol. 6, no. 2, **(1999)**, pp. 13-18.

[2] D. Cabric, S. M. Mishr and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios", The Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, **(1995)**, pp. 72-776.

[3] F. F. Digham, M. S. Alouini and M. K. Simon, "On the energy detection of unknown signals over fading channels", IEEE International Conference on Communications (ICC), Anchorage, AK, **(2003)**, pp. 3575-3579.

[4] Y. Wang, W. Lin and Y. Huang, "Optimization of Cluster-Based Cooperative Spectrum Sensing Scheme in Cognitive Radio Networks with Soft Data Fusion", Wireless Personal Communications, vol. 77, no. 4, **(2014)**, pp. 1-18.

[5] P. Kaligineedi, M. Khabbazian and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system", IEEE Transaction on Wireless Communications, vol. 9, no. 8, **(2010)**, pp. 2488-2497.

[6] S. O. Jaewoo and W. Sung, "Group-based Multi-bit Cooperative Spectrum Sensing for Cognitive Radio Networks", IEEE Transactions on Vehicular Technology, vol. 65, no. 12, **(2016)**, pp. 10193-10198.

[7] I. Joe, Y. Jiao and P. Yin, "A Novel Clustering Scheme for Cooperative Spectrum Sensing in Cognitive Radio Networks", IET Communications, vol. 10, no. 13, **(2016)**, pp. 1590-1595.

[8] A. S. Rawat, P. Anand, H. Chen and P. K. Varshney, "Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks", IEEE Transactions on Signal Processing, vol. 59, no. 2, **(2011)**, pp. 774-786.

[9] P. Kaligineedi, M. Khabbazian and V. K. Bhargava, "Secure Cooperative Sensing Techniques for Cognitive Radio Systems", IEEE International Conference on Communications(ICC), Beijing, China, **(2003)**, pp. 3406-3410.

[10] W. Wang, H. Li and Y. Sun, "Attack-proof collaborative spectrum sensing in cognitive radio networks", Conference on Information Sciences and Systems, Baltimore, Md, Usa, **(2009)**.

[11] K. Zeng, P. Przemysaw and C. Danijela, "Reputation-based cooperative spectrum sensing with trusted nodes assistance", IEEE Communications Letters, vol. 14, no. 3, **(2010)**, pp. 226-228.

[12] N. G. Oh, S. Lim and S. Lee, "Goodness-of-Fit-Based Malicious User Detection in Cooperative Spectrum Sensing", Vehicular Technology Conference (VTC), Quebec City, Canada, **(2012)**, pp. 1-5.

[13] M. J. Saber and S. M. Sajad Sadough, "Multiband Cooperative Spectrum Sensing for Cognitive Radio in the Presence of Malicious Users, IEEE Communications Letters, vol. 20, no. 2, **(2016)**, pp. 404-407.

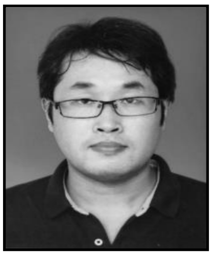
[14] B. Wang, Y. Wu, and R. Liu, "Game theory for cognitive radio networks: An overview", Computer networks, vol. 5, no. 4**, (2010)**, pp. 2537-2561.

[15] A. Sharma, V. Hastir and D. S.Saini, "Transmit power optimization in Cognitive Radio Networks using game theoretic approach", International Conference on Signal Propagation and Computer Technology. **(2014)**, pp. 312-316.

Authors

Shuyan Xiao, received the Ph.D. degree information and communication engineering of China University of Mining and Technology, Xuzhou, P.R. China, in 2015, and now she is a lecture in the Department of Electric Information Engineering, Jiangsu University of Technology, China. Since 2010, her main research interests are wireless communications and cognitive radio.

Shuqi Liu, received her B.S. degree in School of Information Engineering from Zhengzhou University, in 2002, and M.S. degree and Ph.D degree from Soochow University in 2005 and 2016, respectively. Now she is an associate professor at School of Electrical and Information Engineering, Jiangsu University of Technology. Her research interests include adaptive signal processing, cross-layer design and routing design for cognitive radio networks.



Yang Yu, received the Dr. Eng. degree from Shinshu University, Japan in 2013. Since 2013, he is a lecture in the Department of Electric Information Engineering, Jiangsu University of Technology, China. His current research interests include sensor networks, coding and modulation for mobile communication systems.