International Journal of Future Generation Communication and Networking
Vol. 8, No. 3 (2015), pp. 1-14

A Trust Game Model and Algorithm for Cooperative Spectrum Sensing in Cognitive Radio Networks

Wang Zhendong[1], Wang Huiqiang[2] and Zhu Qiang[2]

[1] *Faculty of Information Engineering, Jiangxi University of Science and Technology*
[2] *College of Computer Science and Technology, Harbin Engineering University*
Wangzhendong1982@yeah.net

Abstract

The existence of malicious secondary users will bring damage to the performance of cooperative spectrum sensing and spectrum access in cognitive radio networks, so effectively curbing malicious behavior of secondary users become the key to success for cooperative spectrum sensing mechanism. Inspired by economics of repeated game theory, a trust game model and algorithm of distributed cooperative spectrum sensing oriented to malicious secondary users named FRTrust is proposed. In FRTrust, the reputation status is used to describe the performance of a secondary user in cooperative spectrum sensing process. It encourages secondary users to choose positive and honest behavior strategies for greater and long term benefits. Simultaneously, a 'differentiation' punishment mechanism is presented to respond malicious behaviors of secondary users. By this way, the 'first offender' secondary users and the 'recidivist' secondary users can be distinguished effectively. If a secondary user departs from the normal times in its life period, it will be punished superimposed. Simulation results show that the FRTrust algorithm can encourage secondary users to participate in spectrum sensing in a cooperative attitude, improve the transaction success ratio of cooperative spectrum sensing, and guarantee the fairness and spectrum access performance for cognitive radio networks.

Keywords: *Cognitive radio networks, Cooperative spectrum sensing, Game theory, Reputation*

1. Introduction

As the foundation and premise for cognitive radio networks from theoretical research towards actual deployment, spectrum sensing technology plays an important role in cognitive radio networks technology system [1]. Cooperative spectrum sensing technology can overcome network environments that exist shadowing, multi-path fading and other unfavorable factors, improve the accuracy of the spectrum sensing in complex network environments, thus become the mainstream of development for spectrum sensing. In cooperative spectrum sensing process, secondary users are mainly divided into two types: honest secondary users (honest users) and selfish secondary users (selfish users). Honest users are consciously involved in the process of spectrum sensing across the spectrum sensing lifecycle, and transmit real sensory data to fusion center. However, spectrum sensing operation will consume the limited energy for secondary users, selfish users may choose to refuse to participate in spectrum sensing, and turned to overhear other user's sensing data. Currently, the cooperative spectrum sensing technology research focuses on honest users and selfish users on mixed cooperative spectrum sensing, and proposes a variety of cooperative spectrum sensing method such as bargaining [2], evolutionary game[3] and coalition game[4] to meet different

ISSN: 2233-7857 IJFGCN

requirements for behavioral constraints on selfishness under different limited conditions. However, out of self-interest, there may exist other different secondary users called malicious cognitive users [5] that benefit from prejudice the interests of other secondary users. In the sensing phase, malicious users obtain the on-off state of licensed spectrums through sensing or overhearing, but deliberately transmit false data to fusion center or other secondary users in collaboration stage. For example, a malicious user found no primary users existence on a specific spectrum, but to report the spectrum is occupied to fusion center or other secondary users, thereby preventing other cognitive users access to the spectrum and exclusive some spectrum holes. The presence of malicious users may cause cognitive radio network system showing DoS features to honest users, and do serious harm to cognitive radio network fairness and performance of spectrum access[6,7].

In response to the presence of malicious users, a series of methods such as forward consecutive mean excision(FCME)[8], Bayesian belief propagation[9], goodness of fit[10], conditional frequency check(CFC)[11] and combinatorial optimization identification[12] are proposed, these methods have good effect for detecting the presence of malicious users, but lack of concrete measures to deal with the situation. Duan [13] developed two novel attack-prevention mechanisms with direct and indirect punishments to prevent attacks with *attack–and-run* and *stay–with-attacks* by malicious users. Direct punishment mechanism can prevent all attacks in both *attack-and-run* and *stay-with-attacks* scenarios, but once found attack on the imposition of penalties for all secondary users undermines the fairness of cognitive radio networks. Furthermore, the overhead and complexity of the method are high, and the deployment in practical network is difficult. Indirect attack-prevention mechanism mainly used to deal with *stay-with-attacks*, the key idea is to terminate collaborative sensing upon detection of an attack, which forces malicious users to rely on their own sensing results in the future, and results in an increase in missed detection probability for attackers, reduce the attackers' incentives to attack. However, this method leads to cooperative spectrum sensing downgraded to single-user spectrum sensing, and has a greater impact on performance of spectrum sensing for cognitive radio networks.

Taking into account the shortcomings of existing research, this paper presents a flexible trust model for distributed cooperative spectrum sensing against malicious users. The key idea is to utilize reputation status parameters to quantify and describe the behavioral characteristics of malicious users, then adjusts the reputation value of malicious users according to sensing strategy selection in interactive process. The model encourages secondary users to choose positive and honest behavior strategies for greater and long term benefits. Existing trust model such as RGTrust [14]considered users' historical behavior as discrete events, failed to recognize the importance of continuing to provide real services, therefore it is unfair to such secondary users that continues to provide honest services. In addition, these models are difficult to suppress the secondary users' malicious behaviors effectively because of lack of good punishment mechanism. Accordingly, this paper develops a flexible trust model referred to as FRTrust, it puts the continuity of user behavior as an important factor for users reputation evaluation, and establishes a differentiation punishment mechanism to respond malicious behaviors of secondary users. FRTrust has different punishments for 'first offender' secondary users and the 'recidivist' secondary users, incentives malicious users to repent, improves the transaction success ratio among secondary users participated in spectrum sensing, and then safeguards the fairness of cognitive wireless networks and spectrum access performance.

2. Hypotheses

Hypothesis 1 Secondary users participate in cooperative spectrum sensing in a distributed manner, i.e., no fusion center exist to make centralized decision, secondary users make decisions by themselves using specific fusion rules(such as AND-OR rules) according to spectrum sensing data obtained by interaction among other secondary users.

Hypothesis 2 A honest user participates in spectrum sensing, and sends real sensing data to other secondary users. A malicious user gets spectrum data by overhearing, and releases false data to others.

*Hypothesis*3 The behavior of a malicious user is completely independent and rational, the purpose is to obtain the maximum benefit during its lifetime. Therefore, when uncooperative strategy selection benefits outweigh benefits from cooperative strategy, honest users may choose uncooperative strategy to become malicious users. Meanwhile, malicious users will translate into honest users in the opposite conditions.

3. Cooperative Spectrum Sensing Game

In this section, we build a cooperative spectrum sensing game among secondary users. Through behavior analysis of secondary users in cognitive radio networks, we can establish a collaborative spectrum sensing game scenario. Then, we analyze behavioral characteristics using *prisoner's dilemma* model in cooperative spectrum sensing.

3.1 Cooperative Spectrum Sensing Scenario

In cognitive radio networks, the behavior of secondary users is independent. During the lifetime, secondary users abide by the rule ‘secondary users can access spectrum holes freely without interfering with the primary users’ made by federal communications commission [15]. However, the rule does not explain and restrain spectrum sensing, that results in the autonomy of secondary users too large, makes secondary users may refuse to share spectrum information even send false information to other users out of their own purposes and interests in information interaction stage.

Thus, the scenario of cooperative spectrum sensing coincides with the thoughts of game theory. It mainly reflects in two aspects, first is secondary users have selfish characteristics, and second is cooperative spectrum sensing procedure has the characteristic of incomplete information. In cooperative spectrum sensing, information of profit and loss for secondary users with different strategy does not open to other secondary users, causes secondary users participating in cooperative spectrum sensing can not obtain all the information during cooperative spectrum sensing procedure. This information inequality may lead to uncooperative relationship between secondary users. Therefore, game theory can be used for modeling the scenario with malicious behavior and characteristics with incomplete information, and through the analysis of the equilibrium of the model, we can develop distributed cooperative spectrum sensing strategy fit for cognitive radio networks against malicious secondary uses.

When we apply game theory to study cooperative spectrum sensing, the game can be described as follows. *n* secondary users participated in cooperative spectrum sensing are players in the game, the benefits of individuals can be quantified as spectrum usage time denoted as T. Secondary users detect the existence of the

primary users on licensed spectrum, if there is a primary user, secondary users send binary digits '1' to others, otherwise send '0'. The actions of secondary users are strategies in strategy space. The benefit of a secondary user obtained depends on its strategy, in addition, the benefit also depends on other secondary users' strategies. Therefore, only when the strategies all secondary users adopted make spectrum sensing game reach a Nash equilibrium, all the secondary users can get maximum benefits. When the game is in Nash equilibrium, a single secondary user can not obtain greater benefit with changing its strategy.

3.2 Cooperative Spectrum Sensing Game and its Analysis

We express cooperative spectrum sensing behaviors of secondary users as non-cooperative game denoted as $G=[N, \{S_i\},\{P_i\}]$. The game is infinitely repeated game and discount factor is denoted as η $(0<\eta<1)$. N is the number of secondary uses participated in cooperative spectrum sensing. S_i are sensing strategies for secondary users and $S_i=\{co, no\}$. *co* denotes the strategy that a secondary user participates in spectrum sensing and sends real sensing data, *no* denotes the strategy that a secondary users overhears others and sends false sensing data to other secondary users. P_i is payoff function that is used to describe the gain secondary users obtained under their strategies.

Profits secondary users obtained under different strategies are described as follows. U_h and U_d denote the profits obtained when secondary users adopt *co* and *no* strategy respectively. C_s is the cost that secondary users participate in spectrum sensing. C_r denotes the overhead that secondary user transmits sensing information, and the overhead has nothing to do with the type secondary users send. Then, we have the payoff matrix for cooperative spectrum sensing of secondary users as follows.

Table 1. Payoff Matrix for Cooperative Spectrum Sensing of Secondary Users

Strategy	*co*（*cooperation*）	*no*（*non-cooperation*）
co（cooperation）	U_h-C_r-C_s, U_h-C_r-C_s	-C_s-C_r, U_d -C_r
no（non-cooperation）	U_d -C_r, -C_s-C_r	-C_r, -C_r

From Table 1 we know that the spending is C_s+C_r when secondary users adopt *co* strategy. The comprehensive benefit is U_d -C_r when secondary users adopt *no* strategy. The profit is U_h-C_r-C_s when players are cooperative, and the loss is C_r when players are uncooperative. Obviously, we know that U_d -C_r > U_h-C_r-C_s >0.

Any secondary user participated in cooperative spectrum sensing will fall into *Prisoner's Dilemma* that individual rationality and collective rationality in contradiction when they select spectrum sensing strategies. In cognitive radio networks, secondary users always have a tendency to use non-cooperation strategy in order to obtain more benefits. The aim of cooperative spectrum sensing is to have more accuracy spectrum occupation data. Uncooperative behavior among secondary users will make the cooperative spectrum sensing accuracy lowered, reduce each cognitive user's own benefits. In fact, *Prisoner's Dilemma* among secondary users appearance is due to consider their benefits only in a single stage. In the actual environment, the lifetime of secondary users participated in cooperative spectrum sensing is long-term, therefore, long-term benefits should be considered when we establish payoff functions for secondary users. We can develop a reasonable constraint mechanism allows users to get rid of *prisoner's dilemma* of a single game,

and establish a friendly cooperative spectrum sensing mode to achieve long-term win-win.

4. Distributed Cooperative Spectrum Sensing Trust Model

The objective to establish the distributed cooperative spectrum sensing trust model includes three aspects. The first is to encourage honest users send real spectrum sensing information to others continuously. Secondly, to inhibit malicious user send false information to other secondary users. Finally, the model should prompt malicious users to adopt cooperative strategies in cooperative spectrum sensing.

4.1 Definitions and Descriptions of Secondary Users' Reputation Features

Definition 1 Local reputation of secondary users denoted as $LoRep_{i,j}$, that means the evaluation of secondary users j (SU_j) to SU_i according to the spectrum sensing information SU_i send to SU_j. $LoRep_{i,j} \in [0,1]$. When the value of $LoRep_{i,j}$ close to 1, it means the probability of real information that SU_i send to SU_j is higher. If the value of $LoRep_{i,j}$ close to 0, the probability of false information that SU_i send to SU_j is higher.

In order to highlight the historical behavior in the role of reputation evaluation, we introduce historical local reputation variable denoted as $hLoRep_{i,j}$ to describe the evaluation of SU_j to SU_i in the history of interaction. For example, for the l^{th} interaction of SU_i and SU_j, the evaluation is denoted as $loRep_{i,j}^{l}$. When SU_j consider the information may be true SU_i send, $loRep_{i,j}^{l} \in (0,1]$, otherwise, $loRep_{i,j}^{l} = 0$. Then, we update $hLoRep_{i,j}^{l}$ as follows

$$hLoRep_{i,j}^{l} = \begin{cases} 0, & loRep_{i,j}^{l} = 0 \\ \alpha hLoRep_{i,j}^{l} + (1-\alpha) loRep_{i,j}^{l}, & loRep_{i,j}^{l} \in (0,1] \end{cases} \quad (1)$$

Where α is a historical factor, it represents the proportion of historical reputation when calculating the local historical reputation, $\alpha \in [0,1]$. α close to 1 indicates historical reputation plays a major role in local reputation calculation, and α close to 0 means that the last evaluation plays a major role.

Definition 2 Global reputation of secondary users denoted as $GoRep_{i,j}$ which means the evaluation obtained by SU_j that integrated the local reputation gave by $SU_k (k \neq j)$ interacted with SU_i.

From definition 2, it is easy to know that local reputation reflects only one secondary uses' evaluation to other secondary users, so it has some limitations and subjectivity. Global reputation combines evaluation of multiple secondary users interacted with the specific secondary user, that can reflect the real reputation features and behaviors of secondary users objectively.

For a more detailed description of honesty and malicious behavior for secondary users, encouraging secondary users to send real sensing information to other secondary users continuously, while suppressing the intentional and swing (false - real - false) types of malicious behaviors, we define four parameters such as *Latest Continuous Release Times for Honest Sensing* (*LCRTHS*), *Latest Continuous Release Times for Dishonest Sensing* (*LCRTDS*), *Dishonest Continuous Rank* (*DCR*) and *Honest Continuous Factor* (*HCF*).

Definition 3 *LCRTHS* represents the times to send real sensing information continuously in the latest phase. *LCRTHS* reflects the honesty index of secondary users in the most recent period.

To explain *LCRTHS* in detail, we give an example as follows. If the evaluation is {0.1, 0.4, 0.3, 0, 0.5, 0.8} for a secondary user after interaction with another secondary user in the latest phase, then, its *LCRTHS* value is 2. If the secondary user obtains a negative evaluation in the latest interaction, i.e., $loRep_{i,j}^{k}=0$, the its *LCRTHS* value will reduce to 0, otherwise, *LCTHRS*=2+1=3.

Definition 4 *LCRTDS* denotes the times that continues to send false information before sending real sensing data. This parameter is used to judge the malicious behavior of secondary users is occasional or intentional.

We explain *LCRTDS* as follows. If the evaluation is {0.6, 0.1, 0.4, 0, 0.2, 0.3} for a secondary user after interaction with another secondary user in the latest phase, the value of *LCRTDS* is 1, we can consider the malicious behavior is occasional. If the evaluation is {0.1, 0, 0, 0, 0, 0.2}, the value of *LCRTDS* is 4, we consider the malicious behavior is intentional.

Definition 5 *DCR* denotes the times that secondary users send false sensing information discontinuously in the most recent period. So *DCR* is the rank of *LCRTDS*. This parameter reflects a secondary user whether to take swing type policies.

For example, if the evaluation is {0.1, 0.4, 0, 0.2, 0, 0.3, 0, 0, 0.4} for a secondary user after interaction with another secondary user in the most recent period, the value of *DCR* is 3, we can consider the secondary user take swing type policy.

Definition 6 *HCF* is a modulus that represents the relationship with *LCRTHS*, $HCF \in [0,1]$. The relationship between *HCF* and *LCRTHS* can be denoted as

$$HCF = f(LCRTHS) = \frac{a\tan(LCRTHS - \beta) + a\tan(\beta)}{\pi / 2 + a\tan(\beta)} \tag{2}$$

Where β is the parameter that controls the increase speed of *HCF*.

After obtaining the HCF_i for SU_i, local reputation of SU_i can be calculated as follows

$$LoTrust_{i,j}^{l} = hLoTrust_{i,j}^{l} * HCF_i \tag{3}$$

Suppose secondary users set that interacts with SU_i is Ω_i, then, for SU_j, the global reputation of SU_i is gave as follows

$$GoTrust_{i,j}^{l} = (1-\gamma)LoTrust_{i,j}^{l} + \gamma \frac{\sum_{SU_k \in \Omega_i} LoTrust_{i,k}^{l} * LoTrust_{k,j}^{l}}{\|\Omega_i\| - 1} \tag{4}$$

Where $0 \le \gamma \le 1$, $\|\Omega_i\|$ denotes number of secondary users that interact with SU_i. When γ tends to 1, that denotes the relationship of SU_i to SU_j will not be considered, and if γ tends to 0, that denotes we only consider the relationship of SU_i to SU_j. When calculating the global reputation, the local reputation of SU_k is considered as recommended coefficient, which can prevent exaggerated or defamation for SU_k to SU_i.

The process of global reputation obtained can be described as

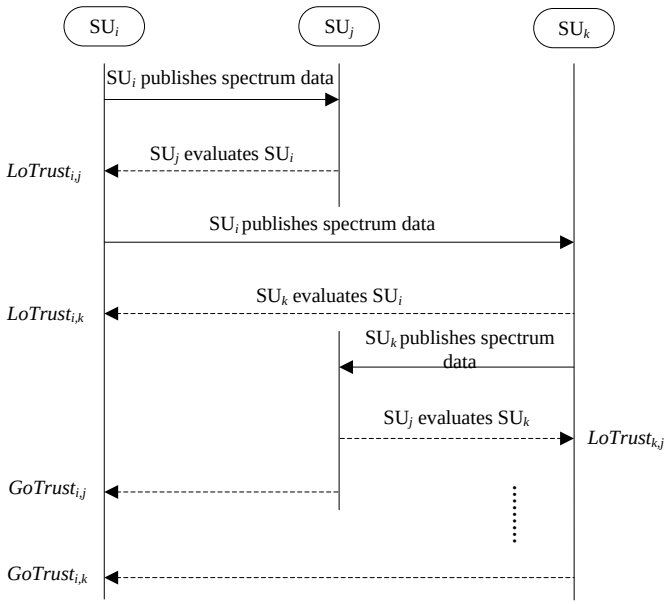


Figure 1. Global Reputation Value Acquisition Process for Secondary Users

4.2 Punishment Mechanism based on Reputation

Definition 7 Punishment modulus T^P is used to depict punishment for secondary users that sends false data in cooperative spectrum sensing. The value of punishment modulus relates to global reputation and historical behavior. Lifetime of secondary users can be divided to several phase, and each phase includes at least one data dissemination. Then, T^P can be denoted as

$$T_i^P = \left\lceil \log_\theta \frac{\mathrm{K}}{\sum_{k=1}^{\mathrm{K}} \left[\min_{SU_j \in \Omega_i, l \in k} GoTrust_{i,j}^l \times \left(\max_{l \in k} LCRTDS_i^l \times \max_{l \in k} DCR_i^l \right)^{-1} \right]} \right\rceil \tag{5}$$

Where θ （θ >0）is a punishment factor. It easily to see that T^P is proportional with *LCRTDS* and *DCR* to some extent. It means the more times and the bigger rank of publishing false sensing data, the more severe punishment for secondary users.

Assuming all secondary users involved in the initial spectrum sensing published real information, at this point the value of *GoTrust* for all secondary users is set to 1. Once the secondary user to publish false data, it will be placed in punitive state immediately. In order to suppress the secondary users continue publishing false information in the punishment period, set T^P can be adjusted. T^P will be prolonged if malicious users still publish false data In the punishment period, and enter a new round of punishment. The number of remaining stages SU$_i$ end of the punishment period after executing *m* stages are as follows

$$R_i^{m+1} = \begin{cases} T_i^{P'}, & \mathrm{SU}_i \ \textit{publishes false data} \\ T_i^P - m - 1, & \mathrm{SU}_i \ \textit{publishes real data} \end{cases} \tag{6}$$

$T_i^{P'}$ is new punishment modulus when SU$_i$ send false information in the punishment period.

4.3 FRTrust Algorithm

In this section, we give FRTrust algorithm according to above analysis as follows

Algorithm 1 FRTrust algorithm

Initializing *LoTrust* and *GoTrust* for all SUs.
Start reputation calculation process
Calculating *LoTrust* for each SU
for each SU_i **do**
  for each SU_j（$j \neq i$）**do**
    Calculating $hLoTrust_{i,j}^{l}$ according to Eq.(1)
    Calculating $LoTrust_{i,j}$ according to Eq.(3)
  end for
end for
Calculating $GoTrust_{i,j}$
for each SU_k （$k \neq i, k \neq j$）**do**
  Extracting $LoTrust_{i,k}$ and $LoTrust_{k,j}$
  Calculating $GoTrust_{i,j}$ according to Eq.(4)
end for
Start reputation punishment process
for each SU_i **do**
  while punishment period is not end
    Calculating punishment modulus according to Eq.(5)
  Executing punishment to SU_i
    Updating punishment modulus according to Eq.(6)
  end while
end for

From the description of FRTrust we can see complexity of the algorithm is mainly concerned with the number of secondary users. In the local reputation computing phase, the algorithm calculates historical reputation value of SU_i to SU_j for the k^{th} phase, and the computational complexity of the algorithm is $O(1)$, then the algorithm needs $O(N)$ operations to obtain local trust value of SU_i for other secondary users. It can be seen the algorithm needs $O(N^2)$ operations to get local trust value of all secondary users. In the global reputation computing phase, it also needs $O(N^2)$ operations to calculate the global reputation value for $SU_{i..}$ Therefore, the complexity of FRTrust in reputation calculation phase is $O(N^2)$. In the reputation punishment phase, calculating punishment modulus needs $(N\text{-}1)\times(N\text{-}1)\times$ K operations, so in the reputation punishment phase, the complexity of FRTrust is $O(N^2)$. Finally, we know the complexity of FRTrust is $O(N^2)$.

4.4 Nash Equilibrium Analysis

Cooperative spectrum sensing among secondary users can be denoted as a non cooperative game G=[N, $\{S_i\}$, $\{P_i\}$]. In order to analyze the Nash equilibrium of G, the following lemma is introduced.

Lemma 1 In the game G=[N, $\{S_i\}$, $\{P_i\}$], for every SU_i ($i \in N$), s_i^* is a optimal response strategy for $(s_1^*, s_2^*, ..., s_{i-1}^*, s_{i+1}^*, ..., s_N^*)$, that is for $\forall s_i' \in S_i$, $P(s_1^*, s_2^*, ..., s_i^*, ..., s_N^*) \geq P(s_1^*, s_2^*, ..., s_i', ..., s_N^*)$, then Nash equilibrium exist.

Theorem 1 Sub-game perfect Nash equilibrium exists in G based on FRTrust.

Proof When SU_j use FRTrust, we analyze different benefits that SU_i sticks FRTrust and transmits false data at some stage, we denote the gains as $P_{FRTrust}=\sum_{i=1}^{\infty}\eta^{i-1}p_i$ and P_d. If $P_{FRTrust}>P_d$, SU_i will chose FRTrust for maximize benefits. Assume $\sum_{i=1}^{\infty}\eta^{i-1}p_i$ is the account, we know

$$\begin{aligned}\frac{U_h-C_r-C_s}{1-\eta} > \frac{1}{1-\eta}\left[(U_h-C_r-C_s)(1-\eta^k)+(U_d-C_r)\eta^k(1-\eta)\right] \\ -\frac{1}{1-\eta}\left[(C_r+C_s)\eta^{k+1}(1-\eta^n)-(U_h-C_r-C_s)\eta^{k+n+1}\right]\end{aligned} \tag{7}$$

Solving the above inequality, we get

$$\eta > \sqrt[n]{\frac{U_d+C_s}{(n+1)U_h}} \tag{8}$$

That is if this condition met, when SU_j insisted FRTrust and publishing false information without first choice, SU_i would not choose to publish false data. When SU_j first select publish false data, if SU_i insisted FRTrust in the ensuing period punishment strategy, the maximize benefits in each stage is U_d -C_r, so SU_i will adhere FRTrust strategy. After the penalty period, SU_i will continue to adhere FRTrust Policy because of its benefits obtained. It can be seen, FRTrust strategy is the optimal response strategy for both sides of the game, so as to constitute a Nash equilibrium. Since the G is an infinitely repeated game, that is sub game are consistent with the original game at any stage, so we know the original Nash equilibrium also constitute a Nash equilibrium on each sub game.

5. Experimental Results Analysis

To verify the performance of FRTrust in cooperative spectrum sensing, we design simulation experiments for FRTrust on Simulink platform, and use RGTrust for comparison. During the simulation, secondary users enter cognitive radio networks is random, and when to leave is unknown. All the secondary users are rational and the relationship among secondary users is peer to peer. Simulation parameters are set up as follows. The number of licensed spectrum in cognitive radio networks is 6, spectrum are mutually independent. The number of primary users is 10, and the arrival of primary users obeys Poisson distribution. The number of secondary users is 20. Each phase includes 5 time-slot. α is set to 0.6, β is set to 5, γ is set to 0.3 and θ is set to 1.25. We compare the performance of FRTrust in reputation status change and transaction success ratio.

5.1 Comparison of Reputation Status for Secondary Users

p is used to denote the probability the secondary users send false information. Fig.2 compares the change of reputation status for secondary users under p=0.3. It is easy to see that RGTrust can distinguish behavior deviation during punishment period and form "ladder" credibility state curves. It makes cognitive radio networks can not distinguish honest secondary users and malicious secondary users, making it difficult to deal with malicious user to use the ‘swing’ type data distribution strategy. For FRTrust algorithm, once the secondary users to take a publishing false data strategy, and its value will be difficult to restore reputation to the punishment of the previous level, to achieve a effective defense for malicious user ‘swing’ type data dissemination strategy.

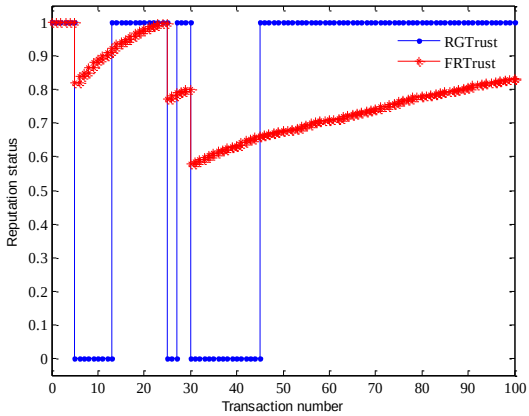


Figure 2. Influence of Reputation Status with SUs' Different Behavior Departure Probability

5.2 Comparison of Average Gain for Secondary Users

Assuming there are three sorts of secondary users in cognitive radio networks, such as honest secondary user, secondary user with malicious behavior occasionally and secondary user with continuous malicious behavior. We compare the average gain for secondary users above under FRTrust and RGTrust. In Fig.3, it can be seen the average income rose after first falling trend, but the overall average gain maintain at a higher level for honest cognitive users, this is due to the malicious behavior of part of secondary users affect accuracy of spectrum sensing for other secondary users. From Fig.4, it is easy to see although a small amount of malicious behavior can sometimes enhance the average revenue for malicious users, but the long term revenue is still low. However, due to take an active cooperation strategy in the punishment phase and subsequent phases, the average income is still showing an upward trend. Fig.5 shows average income has been maintained at a low level under the continuing unfriendly policies, it can be understood as paying for their 'intransigence' of malicious behavior.

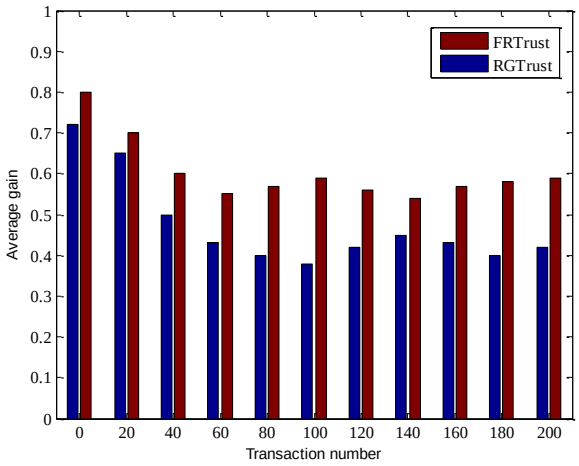


Figure 3 .Honest Secondary User

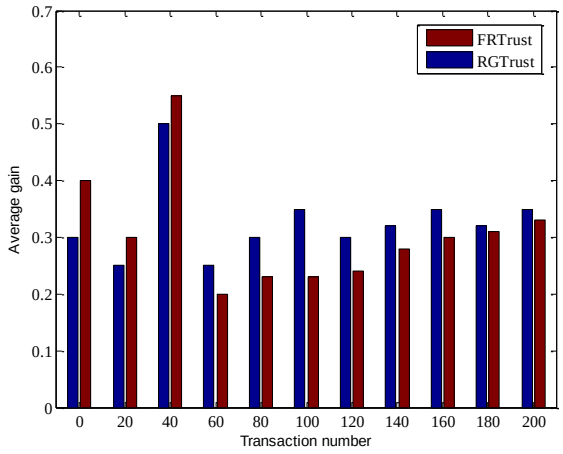


Figure 4. Secondary User with Malicious Behavior Occasionally

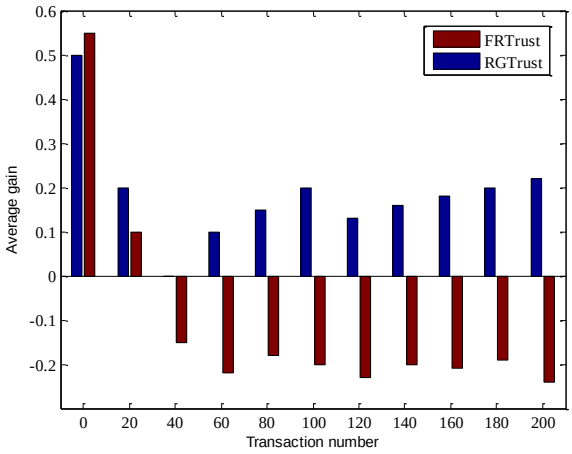


Figure 5. Secondary User with Continuous Malicious Behavior

5.3 Transaction Success Ratio for Secondary Users

The transaction success ratio of secondary users is used to describe incentive effect the spectrum sensing of cognitive users to publish truthful information. In this experiment, the secondary users in accordance with the honesty of honest users: malicious users (p = 0.3) = 0.6:0.4 of mixing, and compare the transaction success ratio under the two algorithms. From Fig.6, we can see secondary user interaction success ratio all has a greater fluctuation under the two algorithms in initial phase, it indicates that malicious behavior has a big impact on transaction success ratio. In the subsequent stabilization phase, each secondary user constitutes a Nash equilibrium strategy choice, then any one of the participants to change their strategy will lead to decline in revenue. Compared with RGTrust algorithm, FRTrust algorithm has a higher success rate and equilibrium (steady state), it mainly due to FRTrust algorithm for secondary user stiffer penalties for malicious behavior, can be more effectively promote the malicious user ‘repented’ and adopt a cooperative strategy.

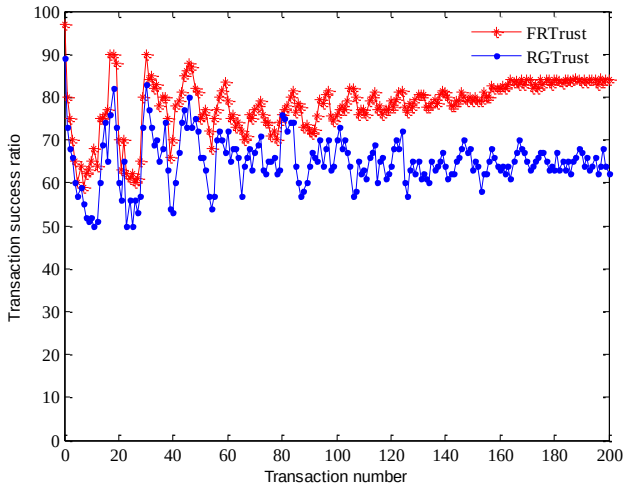


Figure 6. Comparison of Transaction Success Ratio for SUs

6. Conclusions

Since cognitive radio networks proposed, the researchers have a lot of research on cooperative spectrum sensing technology. Based on the existing cooperative spectrum sensing technology shortcomings, this paper proposes a malicious user-oriented distributed cooperative spectrum sensing trust game model and algorithm FRTrust. In FRTrust, the reputation status is used to describe the performance of a secondary user in cooperative spectrum sensing process. It encourages secondary users to choose positive and honest behavior strategies for greater and long term benefits. Simulation results show that the FRTrust algorithm can encourage secondary users to participate in spectrum sensing in a cooperative attitude, improve the transaction success ratio of cooperative spectrum sensing, and guarantee the fairness and spectrum access performance for cognitive radio networks.

Acknowledgements

This work is supported by the Doctoral Scientific Research Fund of Jiangxi University of Science and Technology (jxxjbs14007).

References

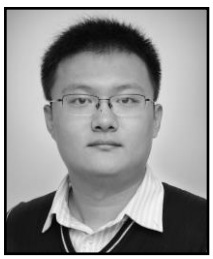
[1] B. Wang and K. J. R Liu, J Sel Area Comm, vol.1, no.5, **(2011)**.
[2] M. Pan and Y. Fang, "Bargaining based pairwise cooperative spectrum sensing for cognitive radio networks", Proceedings of 2008 IEEE Military Communications Conference, **(2008)**; San Diego, USA.
[3] X. Hao, M. H. Cheung and V. W. S. Wong, IEEE T Wirel Commun, **(2012)**.
[4] B. Wang, K. J. R Liu and T. C. Clancy, IEEE T Commu, **(2010)**.
[5] A. G. Fragkiadakis, E. Z. Tragos and I. G. Askoxylakis, IEEE T Commun, **(2013)**.
[6] W. Wang, H. Li, and Y. L. Sun, "Attack-proof collaborative spectrum sensing in **cognitive** radio networks", Proceedings of the 43rd Annual Conference on Information Sciences and Systems, **(2009)**; Baltimore, USA.
[7] A. S. Rawat, P. Anand, and H. Chen, "Countering byzantine attacks in cognitive radio networks", Proceedings of 2010 IEEE International Conference on Acoustics Speech and Signal Processing, **(2010)**; Dallas, USA.
[8] J. Vartiainen, "Always one/zero malicious user detection incooperative sensing using the FCME method", Proceedings of the 7th International ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications, **(2012)**; Cannes, France.
[9] F. Penna, Y. Sun and L. Dolecek, IEEE T Signal Proces, **(2012)**.
[10] G. Noh, L. Sungmook and L. Seokwon, "Goodness-of-Fit-Based malicious user detection in cooperative spectrum sensing", Proceedings of 2012 IEEE Vehicular Technology Conference, **(2012)**; Quebec City, Canada.

[11] X. He, H. Dai and P. Ning, IEEE T Wirel Commun, **(2013)**.
[12] Z. Qin, Q. Li and H. George, IEEE T Wirel Commun, **(2013)**.
[13] L. Duan, A. W. Min and J. Huang, J Sel Area Comm, vol.9, no.30, **(2012)**.
[14] Y. Liu, P. Yang and J Comp Res Dev, **(2006)**.
[15] Y. Xing, R. Chandramouli and S. Mangold, J Sel Area Comm, vol. 3, no. 24, **(2006)**.

Authors

Wang Zhendong, he received his B.S. and M.S. degrees in Information & Computing Sciences and Technology of Computer Application from Changchun University of Science and Technology and Harbin University of Science and Technology in 2006 and 2009 respectively. He is recently working towards his Ph.D. degrees at Harbin Engineering University (HEU), Harbin, China. His research interests span the broad area of cognitive radio networks spectrum sensing and access. Recently, he focuses on the investigation of spectrum migration in cognitive radio networks.

Wang Huiqiang, he received the B.S. degree in computer science and technology from Harbin Institute of Technology (HIT) in 1982, received M.S. and Ph.D. degrees in Technology of Computer Application from HEU in 1985 and 2005 respectively. From 2001 to 2002, he was at Queen's University, Ontario, Canada, as a senior visiting scholar. Since then, he has been engaged in teaching and researching at computer networks and communications. Now, he is a full professor and doctoral advisor at HEU. Up to now, he holds ten Chinese patents. His research interests include network security, cognitive network, dependability, autonomic computing.



Zhu Qiang, he was born in TsingTao, China. He received the B.S. and M.S. degree in computer science and technology from the HEU in 2009 and 2011. His current research interests include resource allocation and resource discovery in network virtualization environment.

