KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 6 (2020) 3–6

www.elsevier.com/locate/icte

Order statistics and recursive updating with aging factor for cooperative cognitive radio networks under SSDF attacks☆

Seungwon Lee[a], Yalei Zhang[a], Seokho Yoon[b], Iickho Song[a,c,*]

[a] School of Electrical Engineering, Korea Advanced Institute of Science and Technology, 291 Daehag Ro, Yuseong Gu, Daejeon 34141, Republic of Korea
[b] College of Information and Communication Engineering, Sungkyunkwan University, 2066 Seobu Ro, Jangan Gu, Suwon 16419, Republic of Korea
[c] Liangjiang International College, Chongqing University of Technology, 459 Pufu Avenue, Longxing Town, Yubei District, Chongqing 401135, China

Received 12 March 2019; accepted 15 April 2019
Available online 15 May 2019

Abstract

For detecting the presence of the primary user under malicious attacks in cooperative cognitive radio networks, we propose a detection scheme based on the order statistics and recursive updating algorithm with aging factor. The aging factor not only makes the detector sensitive to the change in the behavior of secondary users but also allows reduction in the storage space. The order statistics help select secondary users with higher degree of reputation for cooperation, and consequently, reduce the influence of malicious users. Computer simulations show the proposed scheme can defend the network against malicious attacks more effectively than the conventional scheme.

Keywords: Aging factor; Cooperative spectrum sensing; Order statistics; Recursive updating algorithm

1. Introduction

By sharing a number of sensing results to make a decision, the cooperative spectrum sensing alleviates the performance degradation in cognitive radio systems. Due to its openness, on the other hand, the cooperative spectrum sensing is vulnerable to security attacks which may cause serious degradation in the accuracy of the spectrum sensing process. Among the various types of attacks, spectrum sensing data falsification (SSDF) attacks [1] control some sensors and manipulate the sensing results simultaneously for their own purpose, leading to a wrong final decision at the fusion center.

In the meantime, two hidden Markov models, one each for honest and malicious users, are adopted in [2] to characterize the sensing behaviors of the users, and detection of malicious users is achieved via detecting the difference in the parameters of the hidden Markov models. In [3], by allocating a reputation measure to each SU, the fusion center identifies the attackers and removes their inputs from the data fusion process.

In most cooperative spectrum sensing schemes proposed to defend against SSDF attacks, it is normally assumed that SSDF attackers do not change their behavior over the time, which may be not a practical assumption. In this paper, we propose a scheme which puts a relatively higher weight to more recent sensing time period by introducing an aging factor into the Bayesian reputation model. Unlike the scheme considered in [4], where local observations instead of local decisions are sent to the fusion center, each cooperative SU first makes a decision of one binary bit and then sends it to the fusion center in the proposed scheme. Obviously, the one bit decisions require a control channel of narrower bandwidth compared with the local observation.

The contributions of this paper are mainly two-fold: (1) An aging factor is introduced into the recursive updating algorithm to alleviate the influence of the behavior change of the SSDF attacks. (2) The order statistics are employed to select the SUs with high probability of being honest SUs.

☆ This study was supported by the National Research Foundation (NRF) of Korea under Grant NRF-2018R1A2A1A05023192, for which the authors wish to express their thanks.

* Corresponding author at: School of Electrical Engineering, Korea Advanced Institute of Science and Technology, 291 Daehag Ro, Yuseong Gu, Daejeon 34141, Republic of Korea.
E-mail addresses: kkori21@gmail.com (S. Lee), 1223727152@qq.com (Y. Zhang), syoon@skku.edu (S. Yoon), i.song@ieee.org (I. Song).

Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2019.04.003

2. Proposed architecture

2.1. System model

Consider a centralized cooperative cognitive radio network composed of one primary user (PU), one fusion center, and N SUs: Among the N SUs, we assume N_m are malicious users. Each SU reports one bit sensing result, 1 and 0 standing for the presence and absence of the PU, respectively, to the fusion center via a perfect control channel.

The spectrum sensing problem in the subband of the nth SU can be formulated as a statistical hypothesis testing problem of choosing between the null hypothesis 'H_0: The subband is currently not being used' and the alternative hypothesis 'H_1: The subband is currently being used'. Equivalently, we have '$H_0: \ y_n(i) = w_n(i)$' and '$H_1: \ y_n(i) = h_n x_n(i) + w_n(i)$' for $i = 1, 2, \ \ldots, I_n$. Here, I_n is the number of samples over one sensing interval, $y_n(i)$ denotes the ith sample of the received signal, h_n denotes the channel response, $x_n(i)$ is the ith sample of the signal transmitted by the PU, and $w_n(i)$ is the zero-mean additive white Gaussian noise with variance σ_n^2.

After some manipulations, we have the detection probability

$$P_{D,n} = Q_{\delta_n}\left(\sqrt{\theta_1}, \sqrt{2\theta_2}\right) \tag{1}$$

and false-alarm probability

$$P_{FA,n} = \frac{\Gamma(\delta_n, \theta_2)}{\Gamma(\delta_n)} \tag{2}$$

as shown in [5]. Here, $\theta_1 = \frac{\gamma_n}{\sigma_n^2}$, $\theta_2 = \frac{\lambda_n}{2\sigma_n^2}$, $\delta_n = \frac{I_n}{2}$, λ_n is the detection threshold, $\gamma_n = \frac{h_n^2}{\sigma_n^2}\sum_{i=1}^{I_n}|x_n(i)|^2$, $\Gamma(a, x) = \int_x^\infty t^{a-1}e^{-t}dt$ is the incomplete gamma function with $\Gamma(a) = \Gamma(a, 0)$ the gamma function,

$$Q_u(a, x) = \int_x^\infty \frac{t^u \mathbb{B}_{u-1}(at)}{a^{u-1}} \exp\left(-\frac{t^2 + a^2}{2}\right) dt \tag{3}$$

is the generalized Marcum Q-function, and

$$\mathbb{B}_\nu(x) = \left(\frac{x}{2}\right)^\nu \sum_{j=0}^{\infty} \frac{x^{2j}}{4^j j!\Gamma(\nu + j + 1)} \tag{4}$$

is the νth order modified Bessel function of the first kind [6]. With the energy detector, the local binary spectrum sensing decision of the nth SU is obtained as $L_n = 1$ if $Y_n > \lambda_n$ and $L_n = 0$ if $Y_n < \lambda_n$, where $Y_n = \sum_{i=1}^{I_n}|y_n(i)|^2$. The threshold λ_n is set to satisfy the target false alarm probability α_n, called the significance level, and can be determined as $\lambda_n = \left\{Q^{-1}(\alpha_n)\sqrt{2I_n} + I_n\right\}\sigma_n^2$ with $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{t^2}{2}}dt$ the Gaussian tail probability. Only the one-bit decisions $\{L_n\}_{n=1}^N$ are sent to the fusion center to minimize the overhead.

2.2. Fusion center

At the fusion center, the final (global) decision can be made, for example via 'K out of N rule' [7], based on the one-bit local decisions $\{L_n\}_{n=1}^N$. Let us define the set of all N-dimensional binary vectors $B_N = \{(0, 0, \ \ldots, 0), (0, 0, \ \ldots, 0, 1), \ \ldots, (1, 1, \ \ldots, 1)\}$ and $B_{N,k} = \{\boldsymbol{b}_i : \boldsymbol{b}_i \in B_N, \|\boldsymbol{b}_i\| = k\}$, where $\|\cdot\|$ denotes the number of 1's in a vector and $\boldsymbol{b}_i = \left[b_{i,1}, b_{i,2}, \ \ldots, b_{i,N}\right]$. When the K out of N rule is adopted, the probabilities of detection and false-alarm of the fusion center can be expressed as

$$\begin{aligned} P_D &= \sum_{i=K}^{N}\sum_{\boldsymbol{b}_i \in B_{N,i}}\prod_{n=1}^{N} P_{D,n}^{b_{i,n}}\left(1 - P_{D,n}\right)^{1-b_{i,n}} \\ &= \sum_{n=K}^{N}\binom{N}{n}P_{D,S}^n\left(1 - P_{D,S}\right)^{N-n} \end{aligned} \tag{5}$$

and

$$\begin{aligned} P_{FA} &= \sum_{i=K}^{N}\sum_{\boldsymbol{b}_i \in B_{N,i}}\prod_{n=1}^{N} P_{FA,n}^{b_{i,n}}\left(1 - P_{FA,n}\right)^{1-b_{i,n}} \\ &= \sum_{n=K}^{N}\binom{N}{n}P_{FA,S}^n\left(1 - P_{FA,S}\right)^{N-n}, \end{aligned} \tag{6}$$

respectively, assuming that the SUs experience the same signal-to-noise-ratio (SNR) and thus $P_{D,n} = P_{D,S}$ and $P_{FA,n} = P_{FA,S}$ for $n = 1, 2, \ \ldots, N$.

2.3. Analysis of attack

Assuming independent SSDF attack, let C_H and C_M denote the numbers of honest and malicious users, respectively, who have detected the channel state correctly. For the sake of simplicity, we assume that all SUs have the same probability of detection and that attackers have the same attack level $\mu = 1$: Here, the attack level μ, the probability that a user will flip its local inference, is a quantification of the level of attacks of malicious users. Then, C_H follows a binomial distribution with parameters $N - N_m$ and $P_{D,B}$, the probability of detection of SUs before being attacked (for example, it is (5) depending on the fusion rule). Similarly, C_M follows a binomial distribution with parameters N_m and $P_{D,A}$, the probability of detection of SUs after being attacked and determined by $P_{D,B}$ and the type and method of attacks [7]. When the fusion center makes a final decision based on the K out of N rule for example, the probability of detection under SSDF attacks can be expressed as

$$\begin{aligned} \bar{P}_D = \sum_{i=0}^{N_m}\Bigg\{&\binom{N_m}{i}P_{D,A}^i\left(1 - P_{D,A}\right)^{N_m - i}\sum_{j=K-i}^{N-N_m} \\ &\binom{N - N_m}{j}P_{D,B}^j\left(1 - P_{D,B}\right)^{N-N_m-j}\Bigg\}. \end{aligned} \tag{7}$$

2.4. Reputation updating

We next consider the recursive updating algorithm for binomial Bayesian reputation systems [8] with two levels (*e.g.*, Good or Bad). The service quality of the nth SU at the tth sensing interval can be represented by a rating vector $\boldsymbol{r}_{n,t} = \left[a_{n,t} \ b_{n,t}\right]$, where $\left(a_{n,t}, b_{n,t}\right) \in \{(0, 1), (1, 0)\}$ with $a_{n,t} = 1$ $\left(b_{n,t} = 1\right)$ denoting the positive (negative) contribution made by the nth SU in the tth sensing interval.

In the proposed scheme, to take not only the reputation of SUs but also the history of reputation into account, we adopt the accumulated rating vector

$$\boldsymbol{e}_{n,t+1} = \kappa \boldsymbol{e}_{n,t} + \boldsymbol{r}_{n,t+1} \tag{8}$$

after time period $t+1$ for $t = 0, 1, \ldots$, where $\boldsymbol{e}_{n,t} = \left[g_{n,t}\ s_{n,t}\right]$ with $g_{n,t}$ and $s_{n,t}$ representing the positive (Good) and negative (Bad) services, respectively, by the nth SU until the tth time period. Unlike the rating vector $\boldsymbol{r}_{n,t}$, the accumulated rating vector $\boldsymbol{e}_{n,t+1}$ contains the information on the history of reputation. The aging factor $\kappa \in [0, 1]$ introduced in (8) controls the rapidity with which old ratings are aged and discounted as a function of time: As the attackers may change their behavior over time, it is desirable to put relatively higher weight to more recent ratings than to old ones.

2.5. Order statistics

To represent the sensing reliability of SUs, we employ the reputation degree

$$d_{n,t} = \frac{g_{n,t}}{g_{n,t} + s_{n,t}} \tag{9}$$

of the nth SU after the tth sensing time interval. The reputation degree $d_{n,t}$ is the ratio of the number of Good services to the total number of services, and therefore represents the empirical probability that the next local decision will be equal to the global decision.

Obviously, the SUs with high reputation degree should be chosen to make the global decision in the fusion center to improve the performance of the cooperative spectrum sensing. Taking only the local decisions with the J_t highest reputation degrees into account, the global decision of the fusion center can be expressed as

$$\sum_{n=1}^{J_t} L_{(N-n+1),t} \underset{H_0}{\overset{H_1}{\gtrless}} \lambda_{FC,t}, \tag{10}$$

where the order statistics [9] $\left\{L_{(1),t}, L_{(2),t}, \cdots, L_{(N),t}\right\}$ of local decisions are associated with the order statistics $\left\{d_{(1),t}, d_{(2),t}, \ldots, d_{(N),t}\right\}$ of reputation degrees with $d_{(1),t} \leq d_{(2),t} \leq \cdots \leq d_{(N),t}$, and the threshold $\lambda_{FC,t}$ is determined by the fusion rule and required level of significance.

As the fusion center would remove the SUs with lower reputation degree when making the final decision, it is anticipated that the detection performance of the proposed scheme will be improved.

3. Performance comparison

We resort to simulations for discussing the performance of the proposed scheme since explicit analysis is not plausible due to the nature of order statistics. In the first stage of making local decision, the average SNR of each SU is set to be -10 and -5 dB with the noise power $\sigma_n^2 = 1$ and the number of samples $I_n = 100$. In the fusion center, the final decision is made based on the K out of N rule, where the value K is set to $\left\lceil \frac{J_t}{2} \right\rceil$. The simulation results are obtained from Monte Carlo simulation of 10^4 runs with $N = 20$, $\kappa = 0.9$, and after 10 sensing time periods.

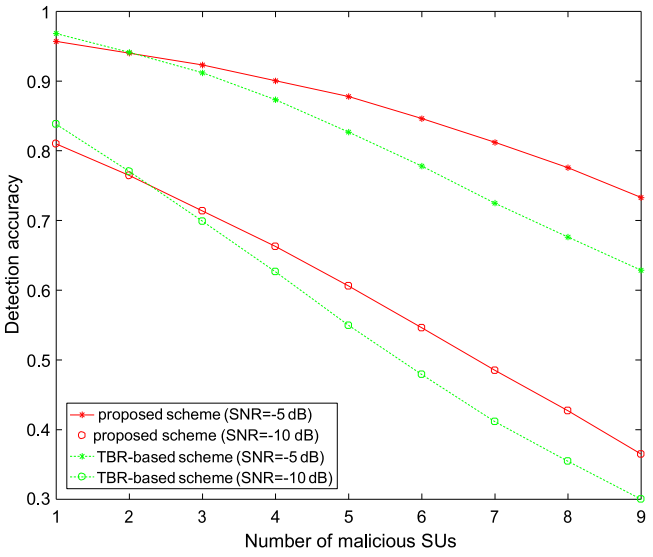

Fig. 1. Detection accuracy versus the number of malicious SUs.

From preliminary experiments with $N_m = 3$ malicious SUs, $\kappa = 0.1$, 0.7, and 0.9, and attack level $\mu = 0.8$ and 1, we have observed/confirmed that the convergence rate of the reputation degree of malicious users gets higher as the aging factor decreases. It is also observed that the reputation degree of the normal and malicious SUs increases and decreases, respectively, with the sensing period.

Next, to choose the number J_t, we have conducted some experiments at the average SNR 5 dB of an SU, target probability 0.2 of false alarm, and attack level $\mu = 1$. It is observed that, as the number of malicious users increases, no matter what the number J_t is, the detection accuracy decreases. In addition, when the deleted number of SUs is approximately equal to the number of malicious users, the detection accuracy is larger than that with other number of deleted SUs. Based on these observations we have concluded that a number between 9 and 13 is a reasonable choice as the number J_t of selected SUs when the number of SUs is 20. These observations are confirmed also by the receiver operating characteristics of the proposed scheme.

Next we compared the performance of the proposed scheme with the traditional Bayesian reputation based scheme [4], denoted as the TBR-based scheme. We assumed $\kappa = 0.9$, $\mu = 1$, $K = \left\lceil \frac{J_t}{2} \right\rceil = \left\lceil \frac{13}{2} \right\rceil = 7$, and target false-alarm probability 0.2. Fig. 1 compares the detection accuracy as a function of the number of malicious SUs. It is observed that the detection accuracy of the proposed scheme is higher than that of the TBR-based scheme when the number of malicious SUs is larger than 2. It is also observed that the detection accuracy of both schemes decreases as the number of malicious SUs increases, with slower rate of decrease for the proposed scheme. Fig. 2 shows the receiver operating characteristics of the proposed and TBR-based schemes when

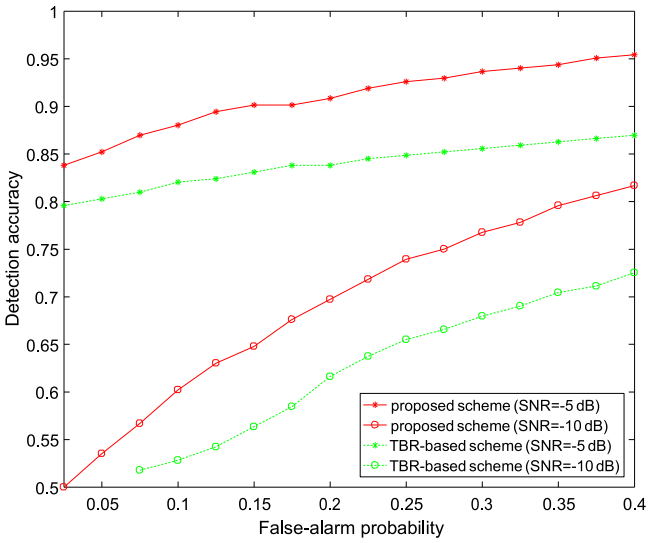

Fig. 2. The receiver operating characteristics of the proposed and TBR-based schemes.

the number of malicious SUs is 6. The proposed scheme is again clearly observed to provide better performance than the TBR-based scheme.

4. Conclusions

A detection scheme, based on order statistics and a recursive updating algorithm with aging factor, is analyzed. As an effect of the aging factor, the fusion center can avoid the use of trust values established far back in time. In addition, the recursive updating algorithm provides reduced storage space compared with the algorithm using all data collected during the observation time. To eliminate the influence of malicious users, a test based on order statistics is applied at the fusion center in selecting SUs with higher reputation degree.

The detection performance of the proposed scheme is discussed via Monte-Carlo simulations. It is observed that the proposed scheme is capable of detecting the malicious users effectively and provides better detection performance than the conventional scheme.

Acknowledgments

The authors would like to thank the Editor and two anonymous reviewers for their constructive suggestions and helpful comments.

Declaration of competing interest

The authors declare that there is no conflict of interest in this paper.

References

[1] L. Zhang, G. Ding, Q. Wu, Byzantine attack and defense in cognitive radio networks: A survey, IEEE Commun. Surveys, Tuts. 17 (3) (2015) 1342–1363.

[2] X. He, H. Dai, P. Ning, HMM-Based malicious user detection for robust collaborative spectrum sensing, IEEE J. Sel. Areas Commun. 31 (11) (2013) 2196–2208.

[3] A.S. Rawat, P. Anand, H. Chen, Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks, IEEE Trans. Signal Process. 59 (2) (2011) 774–786.

[4] M. Zhou, J. Shen, H. Chen, A cooperative spectrum sensing scheme based on the Bayesian reputation model in cognitive radio networks, in: Proc. IEEE Wireless Commun. Netw. Conf. 614-619, Shanghai, China, Apr. 2013.

[5] Y. Zhang, A Recursive Updating Algorithm with Aging Factor and Order Statistics for Cognitive Radio Networks under SSDF Attacks (MSE Thesis), Korea Advanced Institute of Science and Technology, Daejeon, 2017.

[6] I.S. Gradshteyn, I.M. Ryzhik, Table of Integrals, Series, and Products, sixth ed., Academic, San Diego, CA, 2000.

[7] C.S. Hyder, B. Grebur, L. Xiao, M. Ellison, ARC: Adaptive reputation based clustering against spectrum sensing data falsification attacks, IEEE Trans. Mob. Comput. 13 (8) (2014) 1707–1719.

[8] A. Jøsang, W. Quattrociocchi, Advanced features in Bayesian reputation systems, in: Proc. Int. Conf. Trust Privacy, Security Digit. Bus., Linz, Austria, Sep. 2009, pp. 105–114.

[9] I. Song, C.H. Park, K.S. Kim, S.R. Park, Random Variables and Stochastic Processes, Freedom Academy, Paju, Korea, 2014 (in Korean).