Malicious User Suppression Based on Kullback-Leibler Divergence for Cognitive Radio

Hiep-Vu Van and Insoo Koo
School of Electrical Engineering, University of Ulsan
680-749 San 29, Muger 2-dong, Ulsan, Republic of Korea
[e-mail: vvhiep@gmail.com and iskoo@ulsan.ac.kr]
*Corresponding author: Insoo Koo

Received March 18, 2011; revised May 19, 2011; accepted June 8, 2011;
published June 28, 2011

Abstract

Cognitive radio (CR) is considered one of the most promising next-generation communication systems; it has the ability to sense and make use of vacant channels that are unused by licensed users. Reliable detection of the licensed users' signals is an essential element for a CR network. Cooperative spectrum sensing (CSS) is able to offer better sensing performance as compared to individual sensing. The presence of malicious users who falsify sensing data can severely degrade the sensing performance of the CSS scheme. In this paper, we investigate a secure CSS scheme, based on the Kullback-Leibler Divergence (KL-divergence) theory, in order to identify malicious users and mitigate their harmful effect on the sensing performance of CSS in a CR network. The simulation results prove the effectiveness of the proposed scheme.

Keywords: Cognitive radio, spectrum sensing, malicious suppression, KL-divergence.

This work was supported by KRF funded by MEST (Mid-Carrier Researcher Program 2010-0009661).

DOI: 10.3837/tiis.2011.06.003

1. Introduction

In recent years, additional bandwidth and higher bitrates have been required to meet usage demands due to the large development in wireless communication technologies. As a result, frequency bands have become a scarce resource. However, according to the recent study conducted by the Federal Communications Commission [1], most of the assigned radio frequency bands are not being efficiently utilized by licensed users. Cognitive Radio (CR) technology [2] has been proposed to solve the spectrum band utilization problem; the spectrum band's inadequacy can be relieved by allowing some CR users to opportunistically access the spectrum assigned to the Primary User (PU) whenever the channel is free. At the same time, CR users must vacate their frequency when the presence of a PU is detected. Therefore, high reliability detection of the PU signal is crucial for CR networks.

In order to ascertain the presence of a PU, CR users can use one of several common detection methods, such as matched filter, feature, and energy detection [2][3]. Energy detection is the optimal method if the CR user has limited information about a PU signal (e.g., only the local noise power is known) [3]. With energy detection, the frequency energy in the sensing channel is received in a fixed bandwidth, *W*, over an observation time window, *T*, in order to compare with the energy threshold and determine whether or not the channel is being utilized. However, the received signal power may severely fluctuate due to multipath fading and shadowing effects; therefore, it is difficult to obtain reliable detection with only one CR user. Fortunately, improved usage detection can be obtained by allowing some CR users to perform Cooperative Spectrum Sensing (CSS) [4].

In the CSS scheme, the variability of the signal strengths at various CR user locations can be used to improve the sensing performance of a network with a large number of CR users [4]. The research presented in Reference [5] determined that the presence of a few malicious users sending false sensing data can severely reduce the performance of a CSS scheme. Algorithms used to identify the malicious users have been proposed in the studies of References [6] and [7]. In previous research [7], a malicious user detection scheme was proposed based on a robust outlier-detection technique; in the study, only the always YES malicious users are considered, which reduces the throughput of the CR system by giving false high energy values when the PU signal is not present. In addition, the technique in Reference [7] is unable to protect the CSS in the event of a large number of malicious users in the network.

In this paper, we propose a robust malicious user detection scheme based on KL-divergence to protect a CSS against an attack from malicious users, and focus on evaluating the effects of four types of malicious users on spectrum sensing: 1) always *YES* users, who are the users that always give a high energy value; 2) always *NO* users, who are the users that always give a low energy value; 3) *Opposite* malicious users, who are the users that give a false high energy value when the absence of a PU signal is detected or give a false low energy value when the presence of a PU signal is detected; 4) *Random opposite* malicious users who will act like an *opposite* malicious users with probability *r* and act like a normal CR user with the probability*1-r*. The proposed scheme is based on the difference between the signal power distribution obtained from legitimate CR users and malicious users, in order to identify the malicious users. The KL-divergence is a helpful tool for measuring the (dis) similarity between the two distributions. Subsequently, it is suitable to adopt KL-divergence as a criterion for the detection of malicious users.

2. System Description

We consider a CR network composed of N CR users and one PU. There is one PU occupying the observed band with a specific probability. All of the CR users use energy detectors to detect the presence of the PU signal. In addition, there are P ($P < N$) malicious users in the network, and they can be one of four types: always *YES*, always *NO*, *opposite* or *random opposite*. In order to perform CSS, all CR users will send their sensing data to the Fusion Center (FC) through a control channel, which is assumed to be perfect. Based on the sensing data obtained from the CR users, the FC makes a global decision concerning the presence or absence of the PU signal using a data fusion scheme.

Each CR user performs individual spectrum sensing at a specific spectrum band in order to decide between the following two binary hypotheses:

$$\begin{cases} H_0 : x_j(k) = n_j(k) \\ H_1 : x_j(k) = h_j s(k) + n_j(k) \end{cases} \tag{1}$$

where H_0 and H_1 correspond to the hypothesis of the absence and presence, respectively, of the PU signal, $x_j(k)$ represents the signal received by the CR user, h_j denotes the amplitude gain of the channel, $s(k)$ is the signal transmitted from the PU, and $n_j(k)$ is the additive white Gaussian noise.

At the i^{th} sensing interval for the j^{th} CR user, the received signal power, $E_j(i)$, is given as

$$E_j(i) = \begin{cases} \sum_{k=k_i}^{k_i+M-1} \left|n_j(k)\right|^2, & H_0 \\ \sum_{k=k_i}^{k_i+M-1} \left|h_j x(k) + n_j(k)\right|^2, & H_1 \end{cases} \tag{2}$$

where M is the number of samples over one sensing interval, and k_i is the time slot at which the i^{th} sensing interval begins.

When M is relatively large (often no less than *10* [8]), E_j can be closely approximated as a Gaussian random variable under both hypotheses as follows [8][9]:

$$E_j \sim \begin{cases} \mathrm{N}\left(\mu_0 = M, \sigma_0^2 = 2M\right), & H_0 \\ \mathrm{N}\left(\mu_1 = M\left(\gamma_j + 1\right), \sigma_1^2 = 2M\left(2\gamma_j + 1\right)\right), & H_1 \end{cases} \tag{3}$$

where $\{\mu_0, \mu_1\}$ and $\{\sigma_0^2, \sigma_1^2\}$ are means and variances respectively and γ_j is the SNR of the channel between the PU and the j^{th} CR user.

The received signal power of each of the CR user in each sensing interval is reported to the FC, and the equal gain combination (EGC) rule will be used to combine all of them, such that

$$Z(i) = \frac{1}{N} \sum_{j=1}^{N} E_j(i) \tag{4}$$

Finally, the global decision *B(i)* is determined by comparing *Z(i)* with the global energy threshold, λ, such that

$$B(i) = \begin{cases} H_1, \ if \ Z(i) \geq \lambda \\ H_0, \ otherwise \end{cases} \tag{5}$$

3. Secure Cooperative Spectrum Sensing Base on Kullback-Leibler Divergence

3.1 Kullback-Leibler Divergence

The KL-divergence [10] is also known as the relative entropy between two probability density functions, *f(x)* and *g(x)*, such that

$$D(f \| g) = \int f(x) \log\left[\frac{f(x)}{g(x)}\right] dx \tag{6}$$

It is obvious that the KL-divergence is always non-negative. Also, it is zero if and only if the two distributions coincide. KL-divergence is often used as a measure of the (dis) similarity between two distributions.

The KL-divergence between two normal distributions with means and variance as $f \sim (\mu_f, \sigma_f^2)$ and $g \sim (\mu_g, \sigma_g^2)$ respectively, can be obtained such that [11]

$$\begin{aligned} D(f \| g) &= D(\mu_f, \mu_g, \sigma_f^2, \sigma_g^2) \\ &= \frac{1}{2}\left[\log\left(\frac{\sigma_g^2}{\sigma_f^2}\right) - 1 + \frac{\sigma_f^2}{\sigma_g^2} + \frac{(\mu_f - \mu_g)^2}{\sigma_g^2}\right] \end{aligned} \tag{7}$$

3.2 Detection of Malicious Users Based on KL-Divergence

The presence of malicious users can significantly reduce the sensing performance of a CSS in a CR network [5]. In the paper, we consider four types of malicious users (i.e., always *YES*, always *NO*, *opposite* and *random opposite* malicious users), each of which has different effects on the cooperative sensing system. Firstly, the always *YES* malicious user always sends high energy values, thus increasing the false alarm probability and decreasing the available bandwidth for the CR system. Secondly, the always *NO* malicious user always sends low energy values, thus increasing both the missed detection probability and the interference for the PU. The thirdly, the *opposite* malicious user, which is the most harmful user, may send a high energy value when no PU signal is present, or may send a low energy value when the PU signal is present; hence it can increase both the false alarm and the missed detection probability, as well as reduce the available bandwidth while increasing the interference to the PU. Lastly, we consider the *opposite* malicious users with the random manner (denoted as *random opposite* malicious user) who will act like an *opposite* malicious users with probability *r* and act like a normal CR user with the probability*1-r*.

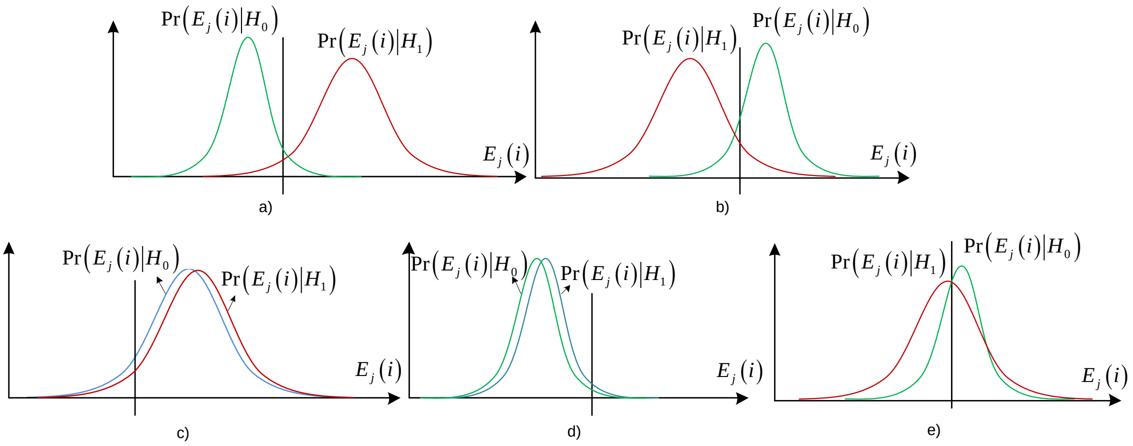

Fig. 1. PDF of the energy distribution reported from the CR users under the absence or presence hypothesis of the PU signal: **a)** normal user, **b)** *opposite* malicious user, **c)** always *YES* malicious user, **d)** always *NO* malicious user and e) *random opposite* malicious user with *r=0.6*.

The probability density function (PDF) of the energy value distribution that is given by the type of CR users under the hypothesis of the absence or presence of the PU signal can be illustrated as shown in **Fig. 1**.

There is no doubt that the energy distribution given by the four types of malicious users is very different as compared to the one of a normal CR user. Therefore, it is feasible to detect malicious users based on the "distance" between their energy distribution and a normal CR user's. Consequently, in this section we present a new secure CSS scheme based on the (dis) similarity measurement tool between the two distributions, called *the KL-divergence*. The proposed scheme is conducted in three successive steps: local sensing, identification, and global combining.

Step 1: Local sensing

All of the CR users detect the signal from the PU in order to measure received signal power $E_j(i)$, where *j* is the index of the CR user and *i* is the index of the sensing interval. The signal power received by all of the CR users at each sensing interval will be reported to the FC. Here, we assume that the FC has a similar function as the N^{th} CR user, that is, it also detects the signal from the PU in obtaining its own received signal power $E_N(i)$. Because the FC performs the role of the control center of a CR network and provides the final decision concerning the absence or presence of a PU, it is reasonable to assume that the sensing result of the FC is legitimate.

Step 2: Identification

In this step, the KL-divergence will be used as the criterion to identify which of the CR users are malicious. KL-divergences are defined below.

$$\begin{aligned} d_{11}(j) &= D\left(\Pr\left(Z(i)|H_1\right)\middle\|\Pr\left(E_j(i)|H_1\right)\right) \\ d_{10}(j) &= D\left(\Pr\left(Z(i)|H_1\right)\middle\|\Pr\left(E_j(i)|H_0\right)\right) \\ d_{01}(j) &= D\left(\Pr\left(Z(i)|H_0\right)\middle\|\Pr\left(E_j(i)|H_1\right)\right) \\ d_{00}(j) &= D\left(\Pr\left(Z(i)|H_0\right)\middle\|\Pr\left(E_j(i)|H_0\right)\right) \end{aligned} \tag{8}$$

We define (μ_1, μ_0), (σ_1^2, σ_0^2) as the mean and variance of *Z*, respectively, under the hypotheses H_1 and H_0, respectively. Also, ($\mu_{j,1}, \mu_{j,0}$), ($\sigma_{j,1}^2, \sigma_{j,0}^2$) are defined as the mean and variance of E_j, under the hypotheses H_1 and H_0, respectively. Since E_j and *Z* have Gaussian distribution, Eqn. (8) can also be expressed as shown below.

$$\begin{aligned} d_{11}(j) &= D\left(\mu_1, \mu_{j,1}, \sigma_1^2, \sigma_{j,1}^2\right) \\ d_{10}(j) &= D\left(\mu_1, \mu_{j,0}, \sigma_1^2, \sigma_{j,0}^2\right) \\ d_{01}(j) &= D\left(\mu_0, \mu_{j,1}, \sigma_0^2, \sigma_{j,1}^2\right) \\ d_{00}(j) &= D\left(\mu_0, \mu_{j,0}, \sigma_0^2, \sigma_{j,0}^2\right) \end{aligned} \tag{9}$$

Generally, in the case of the normal CR user, the distribution of data samples under the same hypothesis (H_1 or H_0) is “closer” together than those distributed under different hypotheses. Therefore, we have

$$\begin{cases} d_{10}(j) > \max\left(d_{11}(j), d_{00}(j)\right) \\ d_{01}(j) > \max\left(d_{11}(j), d_{00}(j)\right) \end{cases} \tag{10}$$

On the other hand, this conclusion is incorrect for malicious users (i.e, always *YES*, always *NO*, *opposite*, *random opposite*), as is clearly shown by the illustrations in **Fig. 1**. Consequently, the criterion to distinguish between a normal CR user and a malicious user can be expressed as

$$\begin{cases} \text{Normal CR user}, \quad \textit{if} \begin{cases} d_{10}(j) > \max\left(d_{11}(j), d_{00}(j)\right) \\ d_{01}(j) > \max\left(d_{11}(j), d_{00}(j)\right) \end{cases} \\ \text{Malicious user}, \quad \textit{otherwise} \end{cases} \tag{11}$$

Because we do not know exactly when the PU signal is present or absent, it is not possible to determine real values for (μ_1, μ_0), (σ_1^2, σ_0^2), ($\mu_{j,1}, \mu_{j,0}$), ($\sigma_{j,1}^2, \sigma_{j,0}^2$) which are needed for calculating the KL-divergence, as shown by Eqn. (7). Therefore, we must use estimated values. In CSS, the global decision is close to the real status of the PU signal. Therefore, we use the global decision, *B(i)*, expressed by Eqn. (5), as the estimation of the PU signal, such that

$$\begin{aligned} Z_1 &= \{Z(i)|H_1\} \approx \{Z(i)|B(i)=H_1\} \\ Z_0 &= \{Z(i)|H_0\} \approx \{Z(i)|B(i)=H_0\} \\ E_{j,1} &= \{E_j(i)|H_1\} \approx \{E_j(i)|B(i)=H_1\} \\ E_{j,0} &= \{E_j(i)|H_0\} \approx \{E_j(i)|B(i)=H_0\} \end{aligned} \tag{12}$$

Because *B(i)* is not the same as the status of the PU signal, the sample data, Z_1, Z_0, $E_{j,1}$ and $E_{j,0}$, may have outlier values (e.g., sample data under hypothesis H_1 (or H_0) that may include several sample points under hypothesis H_0 (or H_1)). Hence, we propose using an efficient and robust estimation algorithm to estimate the mean and variance of sample sets for the case of existing outlier values, termed *bi-weight estimate* and *bi-weight scale*, respectively [10].

The bi-weight estimate **[10] for the mean (** $\hat{\mu}$ **) is**

$$\hat{\mu}(k) = \frac{\sum_{i=k-D}^{i=k} w(i)e(i)}{\sum_{i=k-D}^{i=k} w(i)} \tag{13}$$

where $\{e(i)\,|\,i=1,\ 2,\ ...,\ k\}$ is the sample set that represents Z_1, Z_0, $E_{j,1}$ and $E_{j,0}$, *k* is the current index of the sample set, *D* is the window size for estimating the mean value, and

$$w(i) = \begin{cases} \left(1-\left(\dfrac{e(i)-\hat{\mu}(k)}{c_1 S}\right)^2\right)^2 & : \left(\dfrac{e(i)-\hat{\mu}(k)}{c_1 S}\right)^2 < 1 \\ 0 & : otherwise \end{cases} \tag{14}$$

and

$$S = \underset{i=k-D,k-D+1,...k}{median}\left[\left|e(i)-\hat{\mu}(k)\right|\right]. \tag{15}$$

It is noteworthy that the sensing interval, *D* is related to the history of sensing information which is stored in the FC. If the value of *D* is bigger, then estimation error of means and variances will be smaller. However, for larger value of *D* it will be harder for estimation process to adapt with the change of the PU signal. **Fig. 2** illustrates the window size *D* used for estimating means and variances.

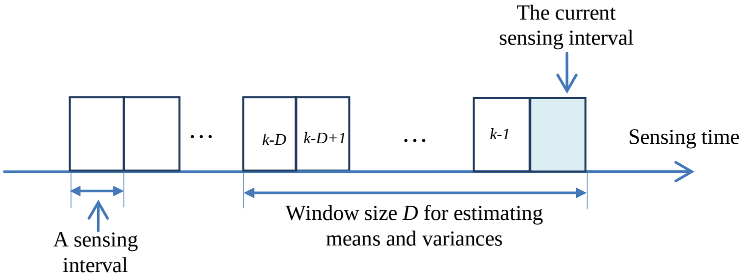

Fig. 2. Window size *D* for estimating means and variances.

The bi-weight estimate calculates a weighted mean with lowered weighting being given to the observations further from the estimate. Initially, all of the data points are assigned equal weights and then the bi-weight estimate is calculated recursively. S measures the median absolute deviation from the estimated mean, $\hat{\mu}$. The parameter c_1 is called the tuning constant and is generally set at $c_1 = 6$ [12].

The bi-weight scale **[10] for variance value ($\hat{\sigma}^2$) is**

$$\hat{\sigma}^2(k) = \sqrt{\frac{g \sum_{u^2(i)<1} \left(e(i) - \hat{\mu}(k)\right)^2 \left(1 - u^2(i)\right)^4}{s(-1+s)}} \tag{16}$$

where

$$s = \sum_{u^2(i)<1} \left(1 - u^2(i)\right)\left(1 - 5u^2(i)\right) \tag{17}$$

and

$$u(i) = \frac{e(i) - \hat{\mu}(k)}{c_2\, \underset{i}{median}\left[\left|e(i) - \hat{\mu}(k)\right|\right]} \tag{18}$$

where $i = k - D,\ k - D + 1,\ ...,k$, g is the number of data samples included in the data window such that $u^2(i) < 1$, and c_2 is the tuning constant.

Based on the estimated values of the means and variances of the sample data obtained using Eqns. (13) and (16), $Z_1(\hat{\mu}_1, \hat{\sigma}_1^2)$, $Z_0(\hat{\mu}_0, \hat{\sigma}_0^2)$, $E_{j,1}(\hat{\mu}_{j,1}, \hat{\sigma}_{j,1}^2)$ and $E_{j,0}(\hat{\mu}_{j,0}, \hat{\sigma}_{j,0}^2)$, the estimation of KL-divergences, $\hat{d}_{11}(j)$, $\hat{d}_{10}(j)$, $\hat{d}_{01}(j)$ and $\hat{d}_{00}(j)$, can be determined by Eqn. (7).

Subsequently, the criteria to detect a malicious user can be defined as

$$\begin{cases} \text{Normal CR user, } if \begin{cases} \hat{d}_{10}(j) > \max\left(\hat{d}_{11}(j), \hat{d}_{00}(j)\right) \\ \hat{d}_{01}(j) > \max\left(\hat{d}_{11}(j), \hat{d}_{00}(j)\right) \end{cases} \\ \text{Malicious user, } otherwise. \end{cases} \tag{19}$$

Step 3: Global combining

After distinguishing between normal CR users and malicious users, all sensing data obtained by normal CR users will be combined using the EGC, such that

$$Z(i) = \frac{1}{n_\Omega(i)} \sum_{j \in \Omega(i)} E_j(i) \tag{20}$$

where *Ω(i)* is the set of normal CR users at the i^{th} sensing interval, and $n_{\Omega(i)}$ is the number of elements of *Ω(i)*.

Finally, the global decision on the presence or absence of a PU signal will be made as shown by Eqn. (5). Because the estimation algorithm for means and variances requires many samples in order to provide robustness, we therefore need a training state for maintaining reliable estimation. The training state can be set as the first of *D* sensing intervals. In the training state, only sensing data from the FC, which is known not to be malicious, will be used to make a global decision. After *D* sensing intervals in the training state, the sensing data of CR users will be evaluated in order to detect malicious users, as shown by Eqn. (19), after which only normal CR users will contribute to making a global decision.

4. Simulation Results

For simulations, we consider a CR network with $N = 10$ CR users (including the FC). SNR=-*10*dB is set for all CR users. Four types of malicious users may appear in the network: always *YES*, always *NO*, *opposite* and *random opposite* malicious users with $r=0.6$. The effects of the various values of window size and number of sensing samples on the sensing performance are evaluated. For estimating the means and variances, tuning constants of $c_1 = 6$ and $c_2 = 9$ [12] are chosen. In order to compare the sensing performances of the considered sensing schemes, we utilize the probability of error, P_e, which is defined as

$$P_e = P_f P(H_0) + P_m P(H_1) \tag{21}$$

where P_f is the probability of false alarms and P_m is the probability of missed detection.

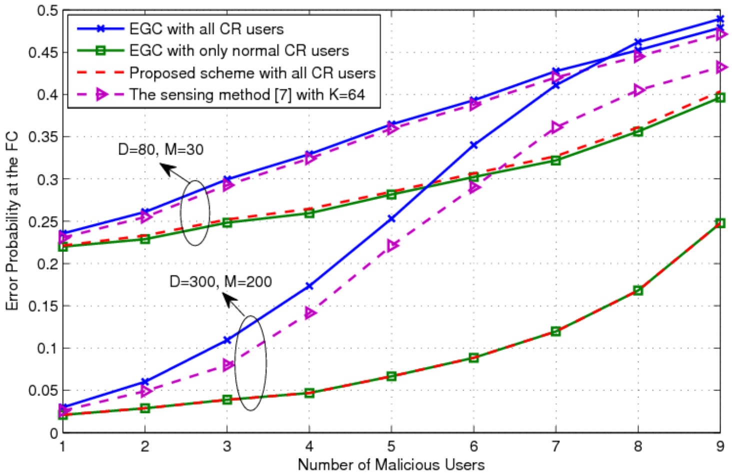

Fig. 3. Error probabilities of the sensing schemes according to the number of always *NO* malicious users when 10 CR users are given.

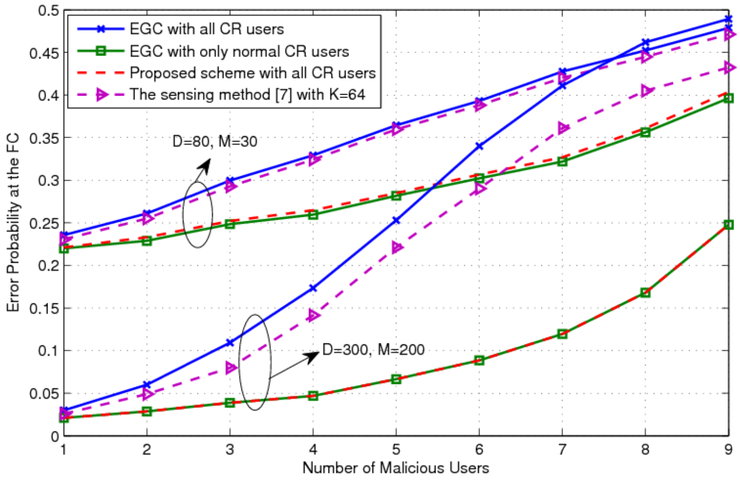

Fig. 4. Error probabilities of the sensing schemes according to the number of always *YES* malicious users when 10 CR users are given.

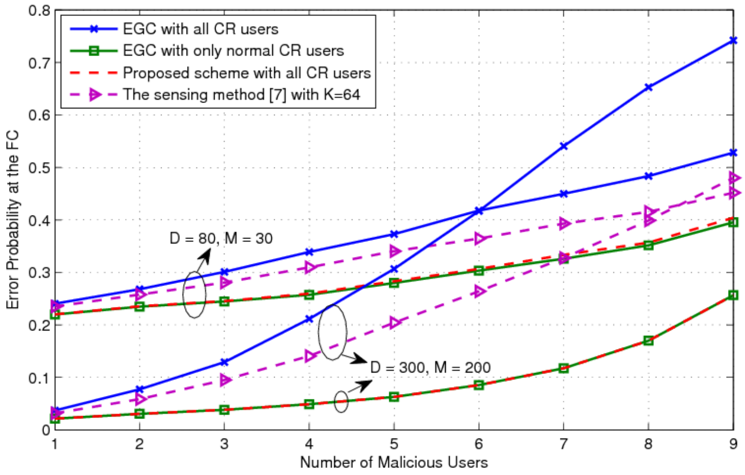

Fig. 5. Error probabilities of the sensing schemes according to the number of *opposite* malicious users when 10 CR users are given.

Fig. 3, **4**, **5**, and **6** show the error probabilities of the sensing schemes according to the number of always *NO*, always *YES*, *opposite* and *random opposite* malicious users, respectively for two cases of *D* and *M*. That is, *D=80*, *M=30* and *D=300*, *M=200*. The performances of EGC with all of the CR users including malicious users (denoted as “EGC with all CR users”) and only normal CR users (denoted as “EGC with only normal CR users”) and the sensing method II proposed in reference [7] (denoted as “the sensing method [7]”) are provided as references. For the simulation of “the sensing method [7]”, in the paper we set the number of estimated means and variances of the previous sensing which is used to calculate outliers factor (denoted as *K* in the reference [7]) be *64*. In all cases of malicious users, the error probability of “EGC with all CR users” is always higher than in the other cases, which means that EGC scheme is very vulnerable to the attack of malicious users. On the other hand, the error probability of the proposed scheme is similar to that of the "EGC with only normal CR users" in all considered cases of *D* and *M* values. This means that the proposed scheme successfully identified each of the four types of malicious users and removed their negative influences on the sensing process. For the smaller values of *M* (*D=80*, *M=30*), the sensing performance of the proposed scheme is degraded compared to the case that *D=300* and *M=200*. However, the proposed scheme still provides better performance than "EGC with all CR users" and "the sensing method [7]". From the above observation and the fact that the smaller *M* means the faster spectrum sensing, we can say that the selection of the number of sensing samples is related to the tradeoff between the sensing time and sensing performance of the CR network.

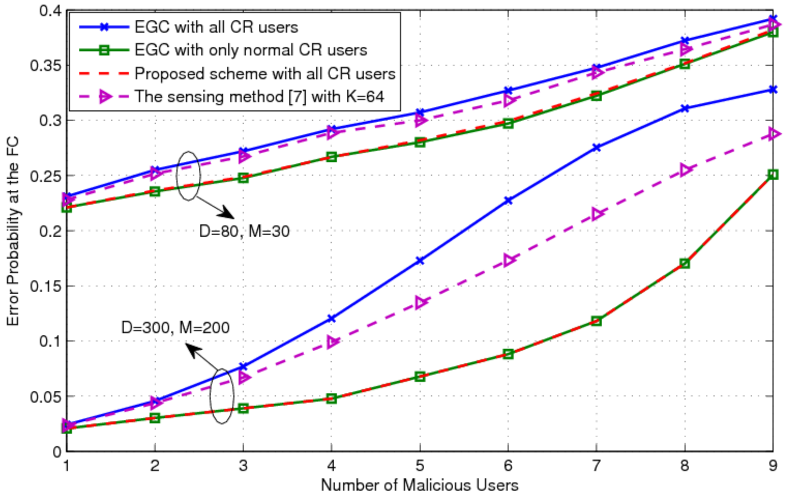

Fig. 6. Error probabilities of the sensing schemes according to the number of *opposite malicious users with the random manner* when 10 CR users are given.

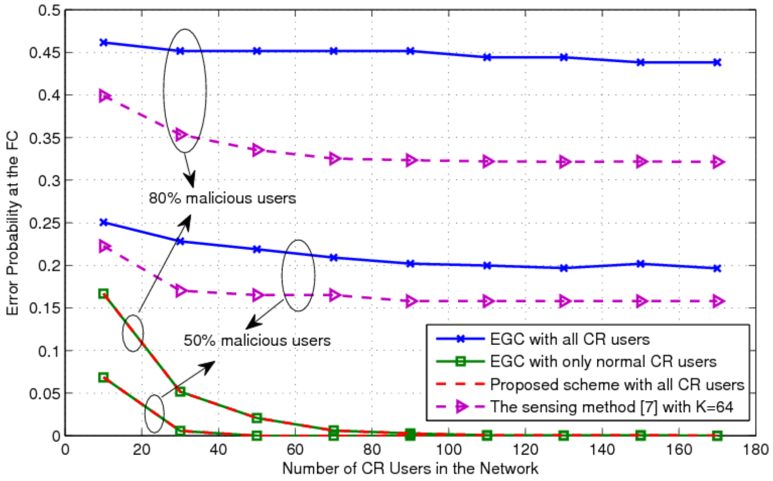

Fig. 7. Error probabilities of the sensing schemes according to the number of CR users for different percentage of *NO* malicious users.

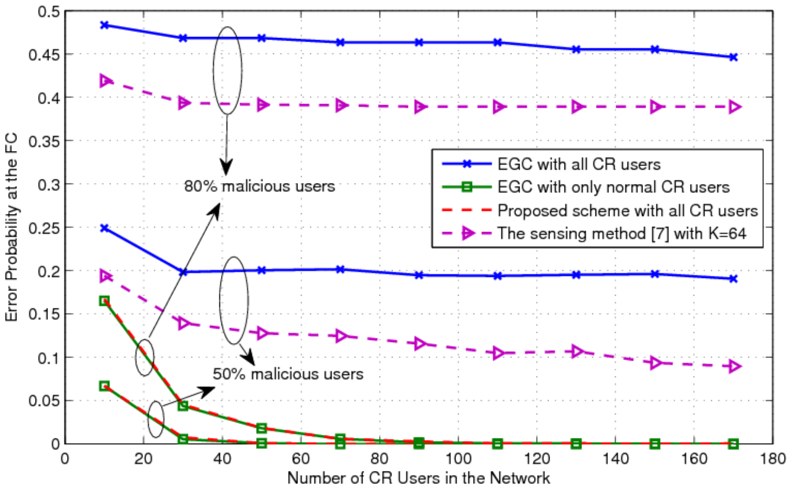

Fig. 8. Error probabilities of the sensing schemes according to the number of CR users for different percentage of *YES* malicious users.

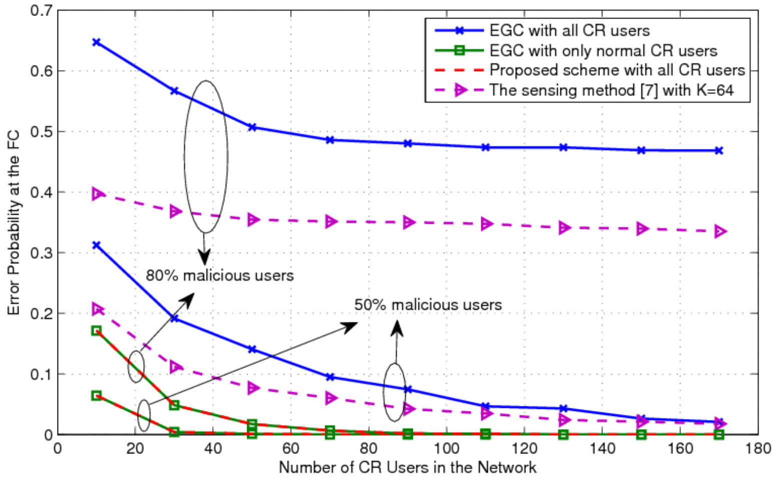

Fig. 9. Error probabilities of the sensing schemes according to the number of CR users for different percentage of *opposite* malicious users.

Fig. 7, **8**, **9**, and **10** illustrate the sensing error probabilities of the considered schemes according to the number of CR users when *50%* and *80%* of CR users are malicious users, respectively. The performances of “EGC with all CR users”, “EGC with only normal CR users” and “the sensing method [7]” are also considered for the sake of comparison. The sensing performances of all sensing schemes are improved as the number of CR users, *N*, increases. For the fixed value of *N*, the proposed scheme not only provides similar sensing performance to the “EGC with only normal CR users” but also provides better sensing performance than “EGC with all CR users” and “the sensing method [7]”. Even for the larger value of *N*, the proposed scheme is able to completely nullify the bad influence from malicious users regardless of the types of malicious users.

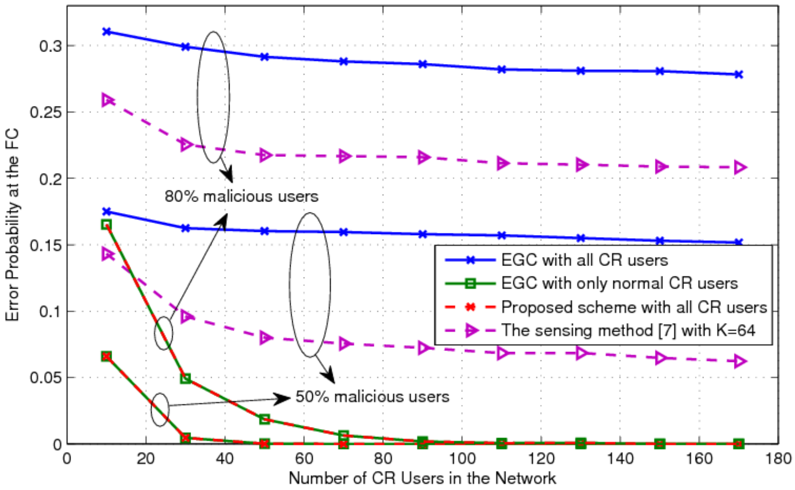

Fig. 10. Error probabilities of the sensing process according to the number of CR users for different percentage of *opposite malicious users with the random manner.*

5. Conclusion

In this paper, we propose a malicious user suppression scheme based on KL-divergence for cooperative sensing in a CR network. The proposed scheme uses the KL-divergence as the criterion for detecting malicious users. The simulations show that the proposed scheme is able to successfully identify all types of malicious users and remove their negative network influences even when the number of malicious users is *90%* of the total number of users.

References

[1] Spectrum Policy Task Force report, technical report 02-135, *Federal Communications Commission*, Nov. 2002.

[2] Y. Hur, J. Park, W. Woo, K. Lim, C. H. Lee, H. S. Kim and J. Laskar, “A wideband analog multi-resolution spectrum sensing (MRSS) technique for cognitive radio (CR) systems,” in *Proc. of IEEE Int. Symp., Circuit and System*, Greece, pp.4090-4093, 2006. Article (CrossRef Link).

[3] A. Sahai, N. Hoven and R. Tandra, “Some fundamental limits on cognitive radio,” in *Proc. of Allerton Conf. on Communications, control and computing*, Monticello, 2004. Article (CrossRef Link).

[4] G. Ganesan and Y. G. Li, “Cooperative spectrum sensing in cognitive radio networks,” in *Proc. of IEEE Symp., New Frontiers in Dynamic Spectrum Access Networks (DySPAN05)*, Baltimore, USA, pp.137-143, 2005. Article (CrossRef Link).

[5] S. M. Mishra, A. Sahai and R. W. Brodersen, “Cooperative sensing among CRs,” in *Proc. of IEEE International Conf. Commun.*, vol. 4, pp. 1658-1663, 2006. Article (CrossRef Link).

[6] P. Kaligineedi, M. Khabbazian and V. K. Bhargava, “Secure cooperative sensing techniques for cognitive radio systems,” in *Proc. of IEEE International Conf. Commun. (ICC08)*, pp. 3406-3410, 2008. Article (CrossRef Link).

[7] P. Kaligineedi, M. Khabbazian and V. Bhargava, “Malicious user detection in a cognitive radio cooperative sensing system,” *IEEE Transactions on Wireless Communications*, vol.9, no.8, pp.2488-2497, 2010. Article (CrossRef Link).

[8] Haijun Wang, Yi Xu, Xin Su and Jing Wang, "Cooperative spectrum sensing with wavelet denoising in cognitive radio," in *Proc. of Vehicular Technology Conference (VTC 2010-Spring)*, pp.1-5, 2010. Article (CrossRef Link).

[9] Jun Ma and Ye Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," in *Proc. of Global Telecommunications Conference, GLOBECOM*, pp.3139-3143, 2007. Article (CrossRef Link).

[10] F. Mostseller and J. W. Tukey, *Data analysis and regression: a second course in statistics. Reading*, MA: Addison-Wesley.

[11] J. R. Hershey and P. A. Olsen., "Approximating the kullback-leibler divergence between gaussian mixture models," in *Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing*, vol. 4, pp. IV317-IV320, 2007. Article (CrossRef Link).

[12] D. A. Lax, "Robust estimators of scale: finite-sample performance in long-tailed symmetric distributions," J. *American Statistical Association*, pp. 736-741, 1985. Article (CrossRef Link).

Hiep-Vu Van received the B.E. degree in Electronics & Telecommunications Engineering from Ton Duc Thang University, Vietnam in 2005 and the B. degree in Business Administration from University of Economy Ho Chi Minh city, Vietnam in 2007, respectively. Since 2008 he has been involved in the combined degree programs (Master's and Ph.D.) in University of Ulsan, Korea. His current research interests include cognitive radio and next generation wireless communication systems.

Insoo Koo received the B.E. degree from the Kon-Kuk University, Seoul, Korea, in 1996, and received the M.S. and Ph.D. degrees from the Gwangju Institute of Science and Technology (GIST), Gwangju, Korea, in 1998 and 2002, respectively. From 2002 to 2004, he was with Ultrafast Fiber-Optic Networks (UFON) research center in GIST, as a research professor. For one year from September 2003, he was a visiting scholar at Royal Institute of Science and Technology, Sweden. In 2005, he joined University of Ulsan where he is now professor. His research interests include next generation wireless communication systems and wireless sensor networks.