韓國IT서비스學會誌
第15卷 第1號
2016年 3月, pp.167-178

Journal of Information Technology Services
http://dx.doi.org/10.9716/KITS.2016.15.1.167

Malicious Users Detection and Nullifying their Effects on Cooperative Spectrum Sensing*

Prakash Prasain** · Dong-You Choi***

■ Abstract ■

Spectrum sensing in cognitive radio (CR) has a great role in order to utilize idle spectrum opportunistically, since it is responsible for making available dynamic spectrum access efficiently. In this research area, collaboration among multiple cognitive radio users has been proposed for the betterment of detection reliability. Even though cooperation among them improves the spectrum sensing performance, some falsely reporting malicious users may degrade the performance rigorously. In this article, we have studied the detection and nullifying the harmful effects of such malicious users by applying some well known outlier detection methods based on Grubb's test, Boxplot method and Dixon's test in cooperative spectrum sensing. Initially, the performance of each technique is compared and found that Boxplot method outperforms both Grubb's and Dixon's test for the case where multiple malicious users are present. Secondly, a new algorithm based on reputation and weight is developed to identify malicious users and cancel out their negative impact in final decision making. Simulation results demonstrate that the proposed scheme effectively identifies the malicious users and suppress their harmful effects at the fusion center to decide whether the spectrum is idle.

Keyword : Cognitve Radio, Energy Detection, Cooperative Spectrum Sensing

Submitted : October 27, 2015 1st Revision : March 20, 2016 Accepted : March 24, 2016

* This study was supported by research fund from Chosun University, 2015.

** Dept. of Information and Communication Engineering, Chosun Univ.

*** Dept. of Information and Communication Engineering, Chosun Univ, Corresponding Author

1. Introduction

In the recent years, the rapid growth in wireless communication has led us to problems with spectrum utilization. The demand of the usable frequency spectrum is increasing. Lack of additional spectrum will become a serious limitation in the next few years. The solution how to deal with this problem is to share available bandwidths between licensed users. But in practice this solution leads to significant underutilization, resulting in spectrum wastage. For example, studies by the Federal Communications Commission (FCC) show that the spectrum utilization in the 0-6 GHz band varies from 15% to 85% (FCC, 2002). Cognitive radio was born as the solution for such a contradiction. The concept was first proposed by Joseph Mitola III at a seminar at the Royal Institute of Technology in Stockholm in 1998 and published in an article by Mitola and Gerald Q. Maguire, Jr. in 1999 (Mitolla and MaGuire, 1999). Cognitive radio is basically a software defined radio with a cognitive engine brain. Full cognitive radio or so called Mitola radio is observing and adjusting every possible parameter of a transceiver in order to maximize its performance. Those parameters include operating frequency, power, waveform, protocol and networking.

In the past few years, significant progress has been made in this field. Showing support for the cognitive radio idea, the FCC allowed for usage of the unused television spectrum by unlicensed users wherever the spectrum is free. IEEE has also supported the cognitive radio paradigm by developing the IEEE 802.22 standard for wireless regional area network (WRAN) which works on unused TV channels (Stevenson et al., 2009). This research area is still at an immature stage because various research challenges have to be addressed and solved. The key enabling technologies of CR networks are the cognitive radio techniques that provide the capability to share the spectrum in an opportunistic manner.

Currently, the frequency spectrum is statically allocated to licensed users, i.e., primary users (PUs) only, in a traditional wireless communication system. Since licensed users may not always occupy the allocated radio spectrum, this static spectrum allocation results in spectrum underutilization. Thus, new spectrum allocation policies were introduced to allow unlicensed users, i.e., secondary users (SUs) to access radio spectrum when it is not occupied by PUs. The SUs are equipped with cognitive radio capability that can be split into cognitive capability and re-configurability. Cognitive capability refers to the ability to sense opportunities in the spectrum where channels are not utilized by PUs. These opportunities are called spectrum holes. Re-configurability means the capability to reconfigure its communication parameters and utilize the spectrum hole. However, SUs should access channels such that there is not any interference with PUs. Therefore, whenever the PU tries to access channel back, the SU should immediately refrain from its transmission. Hence, they need to employ efficient spectrum sensing techniques that ensure the quality of service for PUs and exploit all dynamic spectrum sharing chances. That is to say, in order to facilitate dynamic spectrum access in licensed bands, effective spectrum sensing algorithm needs to be developed whereby high reliability along with effective utilization is achieved.

If SUs have lack of knowledge about the

characteristics of PU signal, energy detection is the optimal choice among many spectrum sensing techniques because of the least complexity (Sahai et al., 2004) and generally adopted by most of the recent research work. Since sensing performance of a single unlicensed or SU may degrade due to the presence of various channel effects such as fading, shadowing and due to the hidden terminal problem experienced by SU, cooperative spectrum sensing (CSS) has been proposed to increase the detection reliability (Visotsky et al., 2005; Ghasemi and Sousa, 2005). It involves many SUs and they can share their sensing information for making a combined decision more accurate than individual decisions. They send their local sensing results to fusion center (FC) through a control channel. Then, the FC combines the received local sensing information and determines the presence of PU. Even though collaboration among them improves the spectrum sensing performance, some falsely reported local sensing results by malicious users degrade the performance rigorously(Mishra et al., 2006). This is what; we call spectrum sensing data falsification (SSDF) attack. Hence, existing cooperative spectrum sensing algorithm has to be modified so that it can identify those malicious users and nullify their harmful effects in final decision making to ensure the reliability of the sensing decisions.

In general, malicious users continuously transmit extreme values indicating “Always Yes” or “Always No” decision. An “Always Yes” user gives a value above the threshold which means it declares that a PU is present all the time. Similarly, an “Always No” user gives a value below the threshold which means PU is absent all the time. Hence, the current CSS algorithm has to be modified so that it can identify the malicious or malfunctioning SUs and suppress their effects in final decision making. Thus, the main objective of this study is to optimize the CSS by identifying the malicious SUs and nullifying their negative effect on CSS. In our previous work (Prakash and Choi, 2014), the performances of different outlier detection techniques based on Grubb’s test, Boxplot method and Dixon’s test (Barnett and Lewis, 1994) are compared initially. Their performances of those techniques have been evaluated through simulation, illustrated the limitations. In this study, we further propose a new scheme based on reputation and weight to detect the presence of malicious users and nullify the falsely reported sensing data from them.

In (Le et al., 2010), the authors have compared several outlier detection methods for the low SNR scenario. In (Ruiliang et al., 2008), the weighted SPRT with a reputation-based mechanism is proposed as the robust cooperative sensing scheme to address the data falsification problem. In (Praveen et al., 2010), simple outlier detection is proposed for pre-filtering of the extreme values in sensing data. The trust factor that measures the CR user’s reliability is then evaluated as the weights in calculating the mean value of receiving sensing data (Akyildiz et al., 2011). In this article, we have studied different outlier detection techniques based on Grubb’s test, Boxplot method and Dixon’s test to detect the presence of malicious users and compared their performances (Lee et al., 2015; Kim et al., 2012).

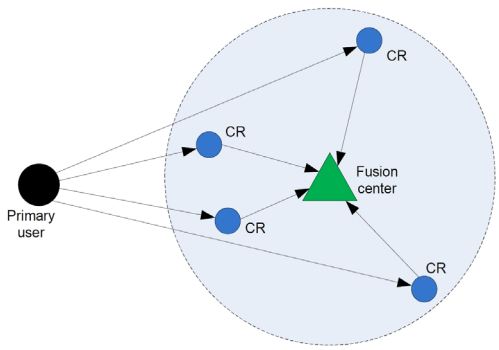
The rest of the article is organized as follows. In section 2, we discuss the system model for cooperative spectrum sensing using energy de-

tection technique. Then, we state three outlier detection techniques based on Grubb's test, Boxplot method and Dixon's test in section 3. In section 4, we propose a newly developed algorithm based on reputation and weight to suppress the malicious users present in cooperative sensing. The performance of each outlier detection method and the proposed algorithmare analyzed through simulation results in section 5. Finally, we draw some conclusions of this study in section 6.

2. System Model

We consider a network composed of N SUs and a fusion center as shown in Figure 1. We assume that each SU consists of an energy detector and performs sensing independently. Then, the local sensing data are sent to the FC which can fuse all available information to decide the absence or presence of PU. The essence of spectrum sensing for PU detection is a binary hypothesis-testing problem :

H0 : primary user is absent;
H1 : primary user is present;



〈Figure 1〉 Cooperative Spectrum Sensing Structure in CRN

$$Y_i(n) = \begin{cases} u_i(n), & H0 \\ h_i(n).s(n) + u_i(n), & H1 \end{cases} \quad (1)$$

where, is the received signal at the i^{th} CR, s(n) is the signal from PU, each sample is assumed to be an independent identically distributed (i.i.d.) random process with zero mean and variance $E[|s(n)|^2] = \sigma_s^2$. Similarly, $u_i(n)$ is the additive white Gaussian noise (AWGN) with zero mean and variance $E[|u_i(n)|^2] = \sigma_u^2$, and $h_i(n)$ denotes the channel gain of the sensing channel between PU and the i^{th} CR. It has the same variance $E[|h_i(n)|^2] = \sigma_h^2$. The area of coverage of the cognitive radio system is assumed to be small enough so that the variations in path loss can be neglected. The average received SNR at each SU is $\gamma = \sigma_s^2\sigma_h^2/\sigma_n^2$. All of the SUs use energy detector output Y_i at the i^{th} SU is given by

$$Y_i = \left(\frac{1}{M}\right)\sum_{n=1}^{m} |y_i(n)|^2 \text{ for } i = 1, 2, \cdots, N. \quad (2)$$

where, M is the number of signal samples that are collected at each SU during the sensing period, which is the product of the sensing time τ and the sampling frequency f_s. We assume perfect channel conditions for the control channels between SUs and FC.

We consider that each SU sends their received energy values through an error free control channel to the FC. Then, FC runs algorithms for detecting malicious users. For this, we follow average combination scheme due to simplicity. The mean received energy by all SUs is calculated and FC compares it with a fixed threshold. Then the decision made by FC is given by

$$D = \begin{cases} H0, \text{ if } Y < \lambda_{FC} \\ H1, \text{ if } Y \geq \lambda_{FC} \end{cases} \quad (3)$$

Where, λ_{FC} is threshold at FC and is the mean of received energies which is given by,

$$Y = \left(\frac{1}{N}\right) \sum_{i=1}^{N} Y_i \quad (4)$$

3. Outlier Detection Techniques

There are several well studied methods to determine outliers in a statistical data. We select only Grubb's test, Boxplot method and Dixon's test (Barnett and Lewis, 1994).

3.1 Grubb's Test

Grubb's test is one of the most commonly used for the detection of a single outlier in univariate data. This test for outliers compares the deviation of the suspect value from the sample mean with the standard deviation of the sample. The suspect is the value that is furthest away from the mean. In order to use Grubb's test for an outlier, the statistic G is calculated :

$$G = \frac{|Suspect\ value - \bar{x}|}{s} \quad (5)$$

where, $\bar{x}$ and are mean and standard deviation respectively. They are calculated with the suspicious value included. If the calculated value of exceeds the critical value, the suspicious value is taken as an outlier, and it is rejected. A table of critical values of specified significance level for different sample size has been provided in (Barnett and Lewis, 1994). This test is used to detect single outlier. To detect more than one outlier, we have applied this test iteratively so that it can test one value at a time until and unless the sample data set of received energies is free from the extreme values produced by malicious users.

3.2 Boxplot Method

In this method, different energy values obtained from different SUs are arranged in ascending order from smallest to largest $Y_1 \leq Y_2 \leq \cdots Y_n$. Then, lower and upper bounds are calculated as follows (Barnett and Lewis, 1994) :

$$Q_{lower} = Q_1 - 1.5\, Q_{intqtr} \quad (6)$$

$$Q_{upper} = Q_3 - 1.5\, Q_{intqtr} \quad (7)$$

where, Q_{lower} and Q_{upper} are lower and upper threshold respectively. Q_1 is first quartile, Q_3 is third quartile and Q_{intqtr} is interquartile range. The values of obtaining energies below Q_{lower} and above Q_{upper} are considered as outliers.

3.3 Dixon's Test

It is based on the ratios of differences between the observations, and the calculation of the ratio depends on the number of observations. As in the previous two techniques, it avoids the calculation of mean and standard deviation. This test is also for detecting a single outlier. In this method, outlier factors for each SU are calculated based on their local sensing results to detect the presence of malicious users. The received energy values are arranged in ascending order $Y_1 \leq Y_2 \leq \cdots Y_N$, and outlier factor f_i for i_{th} SU is calculated as :

For $3 \leq N \leq 7$,

$$f_i \begin{cases} \dfrac{Y_2 - Y_1}{Y_N - Y_1}, & \text{if } smallest\ value\ is\ suspected \\ \dfrac{Y_N - Y_{N-1}}{Y_N - Y_1}, & \text{if } largest\ value\ is\ suspected \end{cases} \quad (8)$$

For $8 \leq N \leq 10$,

$$f_i \begin{cases} \dfrac{Y_2 - Y_1}{Y_{N-1} - Y_1}, & \text{if } smallest\ value\ is\ suspected \\ \dfrac{Y_N - Y_{N-1}}{Y_N - Y_2}, & \text{if } largest\ value\ is\ suspected \end{cases} \quad (9)$$

For $11 \leq N \leq 13$,

$$f_i \begin{cases} \dfrac{Y_3 - Y_1}{Y_{N-1} - Y_1}, & \text{if } smallest\ value\ is\ suspected \\ \dfrac{Y_N - Y_{N-2}}{Y_N - Y_2}, & \text{if } largest\ value\ is\ suspected \end{cases} \quad (10)$$

For $14 \leq N \leq 25$,

$$f_i \begin{cases} \dfrac{Y_3 - Y_1}{Y_{N-2} - Y_1}, & \text{if } smallest\ value\ is\ suspected \\ \dfrac{Y_N - Y_{N-2}}{Y_N - Y_3}, & \text{if } largest\ value\ is\ suspected \end{cases} \quad (11)$$

where, is the number of statistical data, i.e., number of SUs in our case. The calculated outlier factor f_i is compared with a critical value Q, which depends on and the significance level. The table of the critical values for different values of N for three significance levels can be found in(Barnett and Lewis, 1994). If the outlier factor is less than the critical value Q, this energy value is assumed to be normal, otherwise if it exceeds the critical value Q, it is assumed to be high energy reported by corresponding SU. The Outlier factor for the smallest suspect value and largest value are calculated individually.

4. Malicious User Detection Technique based on Reputation and Weight

The main purpose our proposed scheme is to identify the malicious SUs and nullify the falsely reported data from them. In the previous section, the three outlier detection methods were discussed to detect and avoid the falsified sensing data in making global decision in CSS. Two methods out of three are designed for detecting only one outlier at a time. Thus, those methods do not perform better and the performance is degraded if more than one outlier exists.

Thus, a new scheme based on the reputation and the weight of each SU is proposed. In this scheme, every SU is assigned with a reputation value based on the reliability of their sensing data. Then, the weight of each SU is calculated from their reputation and finally their weights are utilized to make global decision. In this way, this scheme is performed in three phases: pre-filtering of the sensing data, reputation assignment and data combining.

Pre-filtering of the sensing data : Let $Y_i(K)$ for i = 1, 2, ···. N represents the output of energy detectors of each SU at time instant k. Initially, it is essential to filter those sensing data which are extremely far from the rest of the data. For this, one of the common outlier detection methods, i.e., a Boxplot method is applied to identify the extreme outliers which has already been discussed in the previous section. $Q_{lower}(k)$ and $Q_{upper}(k)$ are calculated according to equations (6) and (7). If a particular value does not lie in the interval $[Q_{lower}(k), Q_{upper}(k)]$, then this is considered as an outlier and is not included further for making global decision. Let F_k re-

presents the set of the SUs whose energy values lie in the range [Q_{lower}, Q_{upper}] and the number of SUs in the set is P.

Reputation assignment : After the pre-filtering of the sensing data, each SU is assigned a reputation value in accordance with their reliability of sensing data. Here, the decision made by individual SU is regarded as local decision and the decision made by fusion center (FC) as global decision. For each SU, if the local decision is matched with the global decision, the reputation value is increased, otherwise it will be decreased. Initially, an equal reputation value of '1' is assigned for each SU. Thus, the reputation value for the ith SU at time k is updated as (Ruiliang et al., 2008) :

$$r_i(k) = r_i(k-1) + (-1)^{d_i(k)+d(k)} \quad (12)$$

where d(k) is the global decision value which will be given in the next data combining phase and d_i(k) is the local decision which is given by :

$$d_i(k) = \begin{cases} 0, \text{ if } Y_i < \lambda \\ 1, \text{ if } Y_i \le \lambda \end{cases} \quad (13)$$

where denotes the threshold for SU. As already mentioned, all SUs that lie on the set Fk and use the same threshold , so that $\lambda_1 = \lambda_2 = \cdots \lambda_p = \lambda$.

Data combining : In this phase, all the cooperating SUs that fall on the set Fk are included in CSS based on their corresponding reputation value. For this, a weighted CSS is used to make global decision. Then, global decision made by FC is given by,

$$d(k) = \begin{cases} 1, & \text{if} \sum_{F_k} W_i(k)\, Y_i(k) \ge \lambda_{FC} \\ 0, & otherwise \end{cases} \quad (14)$$

where F_k represents the set of energy values after pre-filtering, λ_{FC} is the threshold used by FC. In this study, the Neyman-Pearson formulation λ_{FC} is considered and the threshold is determined so that the probability of false alarm is fixed at a certain value P_f. Similarly, W_i(k) is the reputation weight, which is the function of reputation value such that $W_i(k)$-$f(r_i(k-1))$. Here, the weighted function used in(Ruiliang et al., 2008) is followed, which is given below:

$$W_i(k) = \frac{W_i'(k)}{\sum_i W_i'(k)} \quad (15)$$

where,

$$W_i'(k) = \frac{r_i(k-1)}{\max(r_i(k-1))} \quad (16)$$

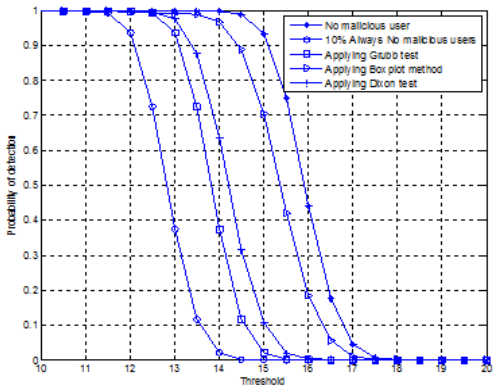
Based on the above discussion, the proposed scheme can be described using the following algorithm :

a. Initialize reputation r_i = 1 for all SUs.
b. For each spectrum sensing attempt {
c. Obtain spectrum sensing report Y_i from all SUs
d. Apply pre-filtering for the extreme outliers
e. Calculate local decision d_i for all remaining P SUs after pre-filtering.
f. Calculate weight w_i for each P SUs.
g. Combine weight w_i with Y_i and compare it with threshold λ_{FC} at FC.
h. If $w_i \times Y_i \ge \lambda_{FC}$, accept H1, i.e. global decision d = 1. Otherwise, accept H0, i.e., global decision d = 0.
i. Update reputation value as $r_i \leftarrow r_i + (-1)^{di+d}$.
}

5. Simulation Results

We carried out simulations to test and compare all the outlier detection methods discussed above. In the simulations, we assume Additive White Gaussian Noise (AWGN) channel and the primary user signal is BPSK modulated. In addition, we have taken cooperating SUs. The distance between any two SUs is small in comparison with the distance from any SU to PU, and the received PU signal at each SU experiences almost identical path loss. Moreover, we assume that the SUs use the same threshold λ, so that $\lambda_1 = \lambda_2 = \cdots \lambda_N = \lambda$. It means that probability of false alarm $P_{f,i}$ is independent of i and we can denote it as P_f. In case of AWGN channel, the probability of detection $P_{d,i}$ is independent of i, we denote this as P_d.

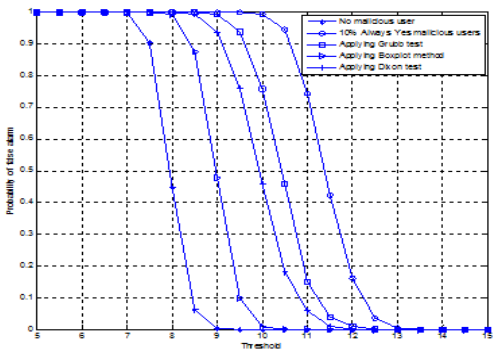
A SU might be malicious due to device malfunctioning or due to selfish reasons. We consider the different kind of malicious users. One is “Always Yes” user, and another is “Always No” user. An “Always Yes” node gives a value above the threshold which means it declares that a PU is present all the time. Similarly, an “Always No” node gives a value below the threshold which means PU is absent all the time. An “Always Yes” user increases the probability of false alarm and an “Always No” user decreases the probability of detection P_d. Additionally, there might be other malicious users that provide extreme false value once in a while and produce the correct valuesat rest of the time. In simulation, we have assumed that it reports energy 5dB lower than the normal SU for those providing “Always No” decision. Similarly, “Always Yes” user reports energy 5 dB higher than the normal SU. The significance level is taken 0.05.



〈Figure 2〉 Probability of Detection Versus threshold for Average Normal SNR = 5dB for ‘Always No’ Malicious User

In <Figure 2>, we consider a cooperative spectrum sensing scenario in which 10% of SUs are ‘Always No’ malicious users. We provide the curve of cooperative spectrum sensing, which shows the degradation in performance when we add ‘Always No’ malicious users. We can see that ‘Always No’ type malicious users have decreased the probability of detection, i.e., increased the probability of miss detection. It also shows the performance of cooperative spectrum sensing after nullifying the malicious effects by applying Grubb’s test, Boxplot method and Dixon’s test. Initially, we assume one ‘Always No’ malicious user, in which case; all the three tests show almost same performance, i.e., they successfully removed the effect of one malicious user. Later, when we introduced multiple ‘Always No’ users, we found some differences in their performances. We can see that probability of detection after applying Boxplot method is closest among three to that of without any malicious user. We have applied Grubb’s test iteratively two detect the multiple malicious users since this test is supposed to detect only one malicious user at a time. On the other hand, the performance of

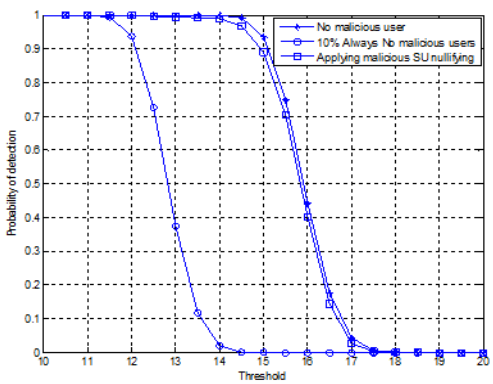
Dixon's test is better than the Grubb's test and worse than Boxplot method in case of multiple malicious users introduced. The Dixon's test cannot be easily implemented for detecting multiple malicious users. If the first three users observed almost same energy, the numerator of equation (11) for the case of lowest suspected, becomes so small and the outlier factor will be smaller than the critical value. This results in not detecting the malicious users present. This is because of method can detect multiple malicious users. This will degrade the performance of cooperative spectrum sensing.



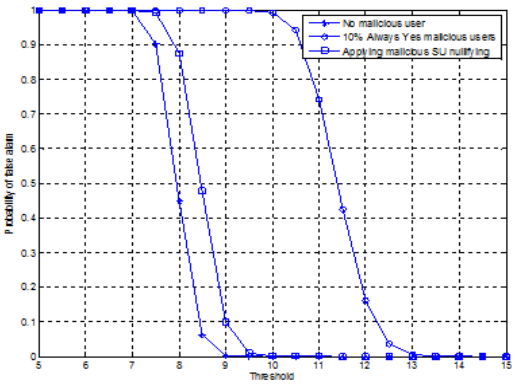
〈Figure 3〉 Probability of False Alarm Versus threshold for Average Normal SNR = 5 dB for 'Always Yes' Malicious User

Now, we plot the ROC curve as shown in <Figure 3>. It shows the performance of cooperative spectrum sensing after adding 10% of 'Always Yes' malicious users. 'Always Yes' type malicious users degrade the performance by increasing the probability of false alarm of the system. Similar to the previous case of adding 'Always No' malicious users, all the three outlier detection methods did not success to nullify the effects of malicious users completely. However, out of these three outlier detection methods, the Boxplot method performs better than that of the Grubb's test and Dixon's test, and it succeeded to bring the probability of detection and probability of false alarm of the system closer to that of the cooperative spectrum sensing system without any malicious user.

Now, the probability of detection and false alarm versus threshold is presented for the case without applying any malicious user detection scheme and applying the proposed scheme for nullifying the effect of malicious users. Figure 4 and 5 show the performance of our newly proposed scheme when applied in the system in which 10% of 'Always No' and 10% of 'Always Yes' malicious users are present respectively. From <Figure 4>, it can be seen that newly proposed scheme for nullifying the effect of malicious users has been able to bring the probability of detection of the system very close to that of cooperative spectrum sensing with no malicious users. Similarly, when a new scheme is applied in the system where 10% 'Always Yes' malicious is present, it brings the probability of false alarm very close to that of with no malicious users as in <Figure 5>.



〈Figure 4〉 The Performance of the Scheme for Nullifying Effects of Malicious Users for a System Containing 10% of 'Always No' malicious users



〈Figure 5〉 Performance of the Scheme for Nullifying Effects of Malicious Users for a System Containing 10% of 'Always Yes' Malicious Users

6. Conclusion

In this paper, we first studied the energy detection technique for spectrum sensing in cognitive radio networks. Later, it is applied in cooperative spectrum sensing and concentrated on the detection and nullifying the effects of falsely reported sensing data by malicious users in final decision making. We first studied techniques that detect the outliers in a statistical data and compared their performance applying in cooperative spectrum sensing. Even though, the first two techniques, i.e., Grubb's and Dixon's are supposed to detect one malicious user at a time, we iterated it to remove all possible malicious users. Through Monte Carlo simulations, we analyzed their performances and observed that Boxplot method performed better than the other two in the presence of multiple malicious users. However, none of them could able to nullify the negative effect of falsely reported sensing data completely. Hence, we proposed a new algorithm to identify and suppress the harmful effect of multiple outliers and the performance was analyzed. The scheme is based on reputation and weight. The purpose of the scheme was to nullify the harmful effects of malicious users by introducing both 'Always No' and 'Always Yes' type malicious users separately in the system. Even though it also could not completely suppress the effects of such malicious users, it performs better than the above mentioned outlier detection techniques. It was able to bring the probability of detection and false alarm of the system very close to that of a system without any malicious users.

We expect this work shall be better to understand the decision making process that shall be helpful for further enhancement.

References

Akyildiz, I.F., F.L. Brandon, and B. Ravikumar, "Cooperative Spectrum Sensing in Cognitive Radio Networks : A Survey", *Physical Communication*, Vol.4, No.1, 2011, 40-62.

Barnett, V. and T. Lewis, *Outliers in Statistical Data*, 3rd Edition : John Wiley and Sons, 1994.

FCC, "Spectrum Policy Task Force report ET Docket", 2002.

Ghasemi, A. and E. Sousa, "Collaborative Spectrum Sensing for Opportunistic Access in Fading Environments", *First IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2005, 131-136.

Kim, J.W., J.Y. Yoon, C.M. Yang, S.B. Lee, and D.S. Eom, "A Study of Distributed Channel Assignment Algorithm Based on Traffic-Awareness in the Wireless Mesh Network", *Journal of Information Technology Services,* Vol.11, No.2, 2012, 291-306.

Lee, J.Y. J.I. Han, and Y.M. Kim, "A Study on Energy Savings in a Network Interface Card Based on Optimization of Interrupt Coalescing", *Journal of Information Technology Services*, Vol.14, No.3, 2015, 183-196.

Mishra, S., A. Sahai, and R. Brodersen, "Cooperative Sensing Among Cognitive Radios, *in IEEE International Conference on Communications*, 2006, 1658-1663.

Mitolla, J. and G.Q. MaGuire, "Cognitive Radio, Making Software Radios More Personal", *IEEE Personal Communications,* Vol.6, No. 4, 1999, 13-18.

Prakash, P. and D.Y. Choi, "Nullifying Malicious Users for Cooperative Spectrum Sensing in Cognitive Radio Networks", *UCAWSN-14,* Vol.331, 2014, 123-131.

Praveen K., K. Majid, and K.B. Vijay, "Malicious User Detection in a Cognitive Radio Cooperative Sensing", *IEEE Transaction on Wireless Communicaitons,* Vol.9, No.8, 2010, 2488-2497.

Ruiliang, C., J.M. Park, and K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks", *The 27th Conference on Computer Communications*, 2008.

Sahai, A., N. Hoven, and R. Tandra, "Some Fundamental Limits on Cognitive Radio", Wireless Foundations EECS, Univ. of California, Berkeley, 2004.

Stevenson, C., G. Chouinard, Z. Lei, W. Hu, S. Shellhammer, and W. Caldwell, "IEEE 802. 22: The First Cognitive Radio Wireless Regional Area Networks (WRANs) Standards", *IEEE Communications Magazine,* Vol.47, No.1, 2009, 130-138.

Visotsky, E., S. Kuffner, and R. Peterson, "On Collaborative Detection of TV Transmissions in Support of Dynamic Spectrum Sharing", *First IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2005, 338-345.

About the Authors

Prakash Prasain (prakashprasain@gmail.com)

Prakash Prasain obtained his Bachelor's Degree in Computer Engineering from Tribhuwan University, Nepal, in 2007. He received the M.S. degree in the Department of Information and Communication Engineering from Chosun University Gwangju, Korea, in 2014. His research interests include MAC protocols in cognitive radio wireless networks.

Dong-You Choi (dychoi@chosun.ac.kr)

Dong-You Choi was born in Seoul, Republic of Korea, on February 25, 1971. He received BS, MS, and PhD degree in the Department of Electronic Engineering from Chosun University, Gwangju, Korea in 1999, 2001, and 2004, respectively. Since 2007, he is a Professor in the Department of Information and Communications Engineering, Chosun University, Gwangju, Republic of Korea. His research interests include mobile communication, wave propagation, and energy harvesting. He is a Member of IEEE, IEICE, KEES, IEEK, KICS, and ASK.