Always One/Zero Malicious User Detection in Cooperative Sensing Using the FCME Method

Johanna Vartiainen
University of Oulu
Centre for Wireless Communications (CWC)
P.O. Box 4500, FI-90014 University of Oulu, FINLAND

***Abstract*—In cognitive radio (CR) systems, cooperative sensing is advantageous when compared to single user detection. Cooperative sensing means that multiple CRs detect the spectrum holes collaboratively. The presence of malicious users (MU) can severely degrade the performance of cooperative CR system. In this paper, we are adopting a signal detection method called the forward consecutive mean excision (FCME) algorithm for 'always one/zero' MU detection in cooperative sensing. Simulation results show that the FCME method is able to work even though 80% of the secondary users are 'always one' MUs.**

***Index Terms*—outlier detection, diagnostic methods, malicious users.**

I. INTRODUCTION

Cognitive radio (CR) enables efficient spectrum usage via releasing temporarily unused frequencies so that secondary users (SU) may transmit unless they do not cause harm to licenced/primary users (PU) [1]. Spectrum sensing that uses signal detection methods to decide if the investigated frequency band is occupied or not can be seen to be a key function of cognitive radio [2]. Cooperative sensing where multiple CRs detect the free spectrum collaboratively mitigates sensing problems like multipath fading, receiver uncertainty and shadowing [3], [4], [5]. Cooperative sensing is very effective technique and improves detection performance at the expense of cooperative cost.

As long as there has been a human activity has also been frauds. Usually, fraud is defined to be criminal deception. Traditional fraudulent behavior include, for example, money laundering, computer intrusion, credit card fraud and telecommunications fraud [6], [7]. Also cognitive radios suffer frauds called malicious users (MU). In cognitive radios, malicious behavior may be unintentional (device malfunctioning) or intentional (selfish and malicious users). Malicious user sending 'always yes (=one)' is probably due to device malfunctioning which leads to wrong sensing reports or there is a simple MU having no intelligence. Selfish SU may sense that there is no signal present but tells to other ones that there is a signal so it can use the free space itself. The SU can send false sensing information always ('always yes' or 'always no (=zero)') or only sometimes. Primary user emulation (PUE) attack [8] means that MUs mimic PU in order to prevent other SUs coming to the band. The goal in PUE attacks is to prevent spectrum resource usage. In selfish PUE situation, the goal is to maximize own spectrum usage, as in malicious PUE situation the goal is to cause denial of service. According to [9], devices can be taught things by malicious elements of their environment thus leading to sensory manipulation attacks, belief manipulation attacks and cognitive radio viruses. Malicious user sending false sensing data to the fusion center in order to increase the probability of incorrect sensing results is known as Byzantine attack or spectrum sensing data falsification (SSDF) attack [10]. 'Denial of service' attacks include, for example, common control channel attacks and location/ sensing/ transmitter/ receiver failures [11].

Malicious users cause severe problems. For example, in cooperative systems many sensor selection methods are vulnerable to MUs because false sensing data may degrade the performance of cooperative sensing [12]. Pure prevention is not enough as the MUs may be adaptive and unpredictable. Thus, MU detection methods are required. Various approaches have been developed for MU detection problem. Pre-filtering of sensing data based on outlier detection is proposed in [12], [13]. Outliers aka nonstandard observations are data samples which differ from the rest of the data. In [14], robust outlier detection techniques are studied and a heuristic algorithm is proposed in [15]. In [16], *a posteriori* probabilities are computed using Bayesian rule and in [17], the method is generalized to handle more than one malicious user. Bayesian detection can be applied only when the strategy of the malicious user is known. In [8], a transmitter verification scheme localization based defence (LocDef) is proposed to handle PUE attacks. Abnormality-detection approach has been proposed in [18]. In [19], method that detects malicious users without any *a priori* knowledge is proposed. In [10], simplified symmetric attack strategy based on the usage of reputation metric is used to count mismatches between the decisions.

However, computationally simple and efficient MU detection methods are still required because MU detection is a demanding and critical task. In this paper, we are focused on simple but nasty SSDF attacks called 'always yes/no' MU attacks. 'Always yes' decision means that the channel is

The research leading to these results was derived from the European Community's Seventh Framework Programme (FP7) under Grant Agreement number 248454 (QoSMOS).

CROWNCOM 2012, June 18-20, Stockholm, Sweden

DOI 10.4108/icst.crowncom.2012.248180

always said to be occupied, i.e., 'always one', as 'always no' means that the channel is always said to be free, i.e., 'always zero'. These are usually caused by device malfunctioning or selfish user. Because the pattern of 'always one/zero' attack is simple and MUs do not have to know any spectrum status information, these kind of attacks are easy to realize. Prevention of these attacks is an important task because many sensor selection methods are vulnerable to MUs always sending ones, see, for example, [20] and references therein. In cooperative sensing, the fusion center makes the final decision is PU present or not, and wrong sensing information may affect that decision. Malicious users also manipulate other SUs adaptation. 'Always one' MUs have been studied, for example, in [21] and in [22].

This paper considers 'always one' and 'always zero' malicious user detection using the forward consecutive mean excision (FCME) [23], [24] signal detection method whose applications have been proposed to be used in spectrum sensing [25]. Here, the FCME algorithm is run to combined binary sensing decisions. The FCME algorithm is a computationally simple but effective diagnostic outlier detection method that is able to find large amount of outliers. It operates blindly so no *a priori* information is required. It is also possible that the FCME method or its application [25] is used first sensing and then MU detection. This reduces the overall complexity.

II. 'Always One' and 'Always Zero' Malicious Users

In cooperative sensing, MUs like 'always yes' and 'always no' can be identified by comparing energy distributions. Energy value of a MU differs in distribution from the energy value distribution of non-malicious users [12]. Fig. 1 presents some examples about distributions for decisions (probability mass functions). Usually, the distribution is binomial and it depends on the probability. Note, that usually the probability p is not known. 'Always yes' and 'always no' lead to uniform distribution. 'Always yes' users increase the false alarm probability P_{fa} as 'always no' users decrease the detection probability P_d of a fusion center. Malicious users sending 'always one' are more harmful than malicious users sending 'always zero' [20].

III. System Description

We have a CR network that consists of one fusion center called central user (CU) and N SUs, which are denoted by SU$_i$, $i = 1, \ldots, N$. There is one PU occupying the observed band with a certain probability. Each SU finds PU signal with probabilities P_d and P_{fa}. Channels between PU and SUs are assumed to be i.i.d. In the system there are $M \leq N$ malicious users. Without loss of generality we can assume that SU$_i$, $i = 1, \ldots, M$ are assumed to be malicious and continuously providing false information. Average SNR values for SUs are equal. Each SU sends hard (binary) sensing decision information to CU, that is, 0 or 1, and CU makes the decision based on individual SUs sensing information. Malicious user detection is performed before the decision making. The MU detection method does not know the number or type of MUs, the number of PUs or the probabilities.

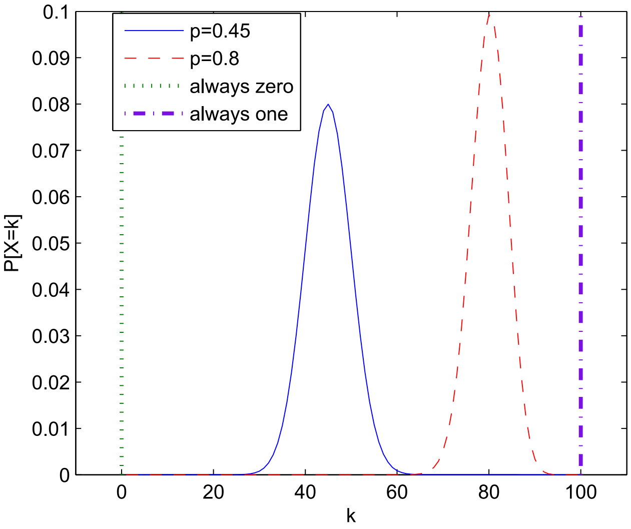


Fig. 1. Examples about distributions for decisions, $n = 100$. Binomial distribution for $p = 0.45$ and $p = 0.8$, uniform distribution for 'always zero' ($p = 0$) and 'always one' ($p = 1$). Here, n denotes the sequence of experiments and p denotes the probability.

IV. The FCME method

The FCME algorithm is an iterative forward-type method that uses a detection threshold in order to separate the samples into two sets: outliers above the threshold and majority of the data below the threshold [23], [24], [25]. Usually, time or frequency domain samples are considered. First, the used threshold parameter $T_{cme1} > 1$ is selected. Proper threshold setting is considered, for example, in [25]. Second, squared samples are rearranged in an ascending order according to the sample energy to form vector $\mathbf{V}$, and m, usually $m = 10\%$, smallest samples are selected to form the initial set Q. The threshold is

$$T_{h1} = T_{cme1} * \overline{Q}, \tag{1}$$

where $*$ denotes multiplication and $\overline{Q} = \frac{1}{Q}\sum_{i=1}^{Q} |x_i|^2$ is the sample mean. Samples below the threshold T_{h1} are added to the set Q. This is repeated until there are no new samples below the threshold to be added to the set Q. Thus, there are Q samples below the threshold and $N - Q$ samples above the threshold. The computational complexity of the FCME method is $N \log_2 N$. The most complex parts are sorting and possible Fourier transformation.

V. The Modified FCME Method

Let us consider K consecutive sensing period results from one SU and define the following vector

$$\mathbf{x}_i = \begin{pmatrix} x_i(1) & x_i(2) & \cdots & x_i(K) \end{pmatrix}^T$$

where samples x_i, $x_i \in \{0, 1\}$, $i = 1, \ldots, K$, denote received sensing result by the ith SU. Accordingly, the received sensing period result matrix $\mathbf{x}$ for N SUs can be defined as following $K \times N$ matrix

$$\mathbf{x} = \begin{pmatrix} \mathbf{x}_1 & \mathbf{x}_2 & \cdots & \mathbf{x}_N \end{pmatrix} = \begin{pmatrix} x_1(1) & x_2(1) & \cdots & x_N(1) \\ x_1(2) & x_2(2) & \cdots & x_N(2) \\ \vdots & \vdots & \ddots & \vdots \\ x_1(K) & x_2(K) & \cdots & x_N(K) \end{pmatrix}$$

Means for every vector $\mathbf{x}_i$ are calculated and included to vector

$$\mathbf{V} = \begin{pmatrix} v_1 & v_2 & \cdots & v_N \end{pmatrix} = \begin{pmatrix} \overline{\mathbf{x}_1} & \overline{\mathbf{x}_2} & \cdots & \overline{\mathbf{x}_N} \end{pmatrix},$$

where $\overline{\mathbf{x}_i} = \frac{1}{K}\sum_{j=1}^{K} x_i(j)$. Thus, the first sample in vector $\mathbf{V}$ is the mean of sensing period results (1 or 0) of SU_1. The FCME is run to vector $\mathbf{V}$ as illustrated in Section IV. Samples that have too high mean, i.e., samples above the threshold T_{h1} are classified to be from 'always one' MUs. Thus, sensing information from MUs are not taken into account, i.e., these columns are rejected from the matrix $\mathbf{x}$ before sensing results are handled by CU. It is also possible to modify the FCME algorithm so that also 'always zero' -malicious users are detected. Thus, samples that have too low mean are classified to be from MUs. This is possible using threshold parameter $T_{cme2} < 1$ and classifying decisions below the threshold T_{h2} to be from MUs (Fig. 2). It should be taken into account that if there is lot of 'always zero' MUs, the initial set consists of zeros, and the FCME algorithm does not operate at all. However, it is assumed here that the number of 'always zero' MUs is small.

Malicious user detection is a basic binary hypothesis testing problem so that H_0: MU is not present and H_1: MU is present. For T_{h1}, detection probability P_d is defined to be $P(\tilde{X} > T_{h1}|H_1)$ and missed detection probability P_m can be defined to be $P(\tilde{X} < T_{h1}|H_1)$. False alarm probability P_{fa} is $P(\tilde{X} > T_{h1}|H_0)$, where $\tilde{X}$ means detection information that is transmitted to central user. Consequently, for T_{h2}, corresponding probabilities are $P_d = P(\tilde{X} < T_{h2}|H_1)$, $P_m = P(\tilde{X} > T_{h2}|H_1)$ and $P_{fa} = P(\tilde{X} < T_{h2}|H_0)$.

Next, two examples are presented to illustrate the MU detection method. Let us consider the situation when there are $N = 5$ cognitive SUs that send their sensing decisions to the fusion center so that '1' means that the channel is occupied and '0' means that channel is unoccupied. PU signal is present randomly 50% of the time and each SU locally finds PU signal with probabilities $P_d = 0.8$ and $P_{fa} = 0.1$. One decision matrix for these 5 SUs for $K = 10$ sensing periods is presented at Fig. 3. Therein, SU_4 is a MU sending always one, i.e., $M = 1$. That is, column n:o 4 consists of ones. The modified FCME algorithm computes mean of each column. In this case, the received vector of means is $V = [0.5, 0.5, 0.2, 1.0, 0.5]$. Having threshold parameter $T_{cme1} = 1.7$, the threshold is $T_{h1} = 0.7225$. Values in vector V which exceed the threshold T_{h1} are considered to be from MU. Now, $V(4) = 1 > 0.7725$ so SU_4 is decided to be a MU.

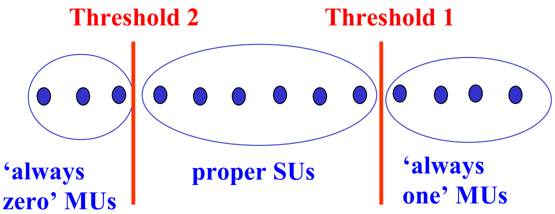
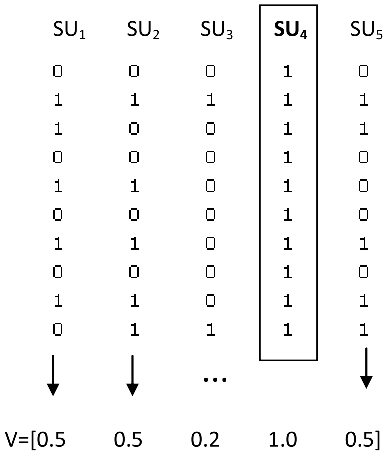
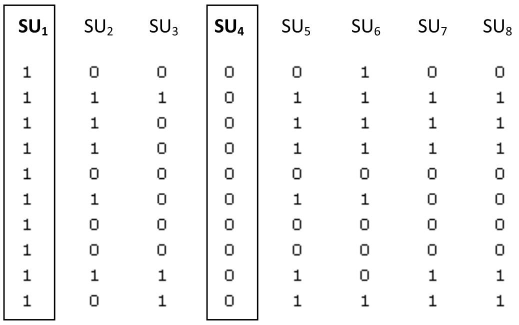


Fig. 2. The threshold setting. The threshold 1 separates 'always one' MUs as the threshold 2 separates 'always zero' users. The original FCME method uses only the threshold 1 thus detecting only outliers with too high values.



SU_1	SU_2	SU_3	SU_4	SU_5
0	0	0	1	0
1	1	1	1	1
1	0	0	1	1
0	0	0	1	0
1	1	0	1	0
0	0	0	1	0
1	1	0	1	1
0	0	0	1	0
1	1	0	1	1
0	1	1	1	1
V=[0.5	0.5	0.2	1.0	0.5]

Fig. 3. One example. $N = 5$ cognitive SUs and sensing results from 10 consecutive sensing periods are presented. PU signal is present randomly 50% of the time and each SU locally finds PU signal with probabilities $P_d = 0.8$ and $P_{fa} = 0.1$. SU_4 is 'always one' malicious user.



SU_1	SU_2	SU_3	SU_4	SU_5	SU_6	SU_7	SU_8
1	0	0	0	0	1	0	0
1	1	1	0	1	1	1	1
1	1	0	0	1	1	1	1
1	1	0	0	1	1	1	1
1	0	0	0	0	0	0	0
1	1	0	0	1	1	0	0
1	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0
1	1	1	0	1	0	1	1
1	0	1	0	1	1	1	1

Fig. 4. One example. $N = 8$ cognitive SUs and sensing results from 10 consecutive sensing periods are presented. PU signal is present randomly 50% of the time and each SU locally finds PU signal with probabilities $P_d = 0.8$ and $P_{fa} = 0.1$. SU_1 is 'always one' and SU_2 is 'always zero' malicious user.

Consider $N = 8$ cognitive SUs with parameters as in the previous case. Now, there is also two MUs ($M = 2$) so that SU_1 sends always ones and SU_4 sends always zero (Fig. 4). The received vector of means is $V = [1.0, 0.5, 0.3, 0, 0.6, 0.6, 0.5, 0.5000]$. Having threshold parameters $T_{cme1} = 1.9$ and $T_{cme2} = 0.7$, the thresholds are $T_{h1} = 0.8143$ and $T_{h2} = 0.1867$. Values in vector V which are above the threshold T_{h1} and below the threshold T_{h2} are from MUs. Now, $V(1) > 0.8143$ and $V(4) < 0.1867$ so SU_1 and SU_4 are correctly decided to be MUs.

VI. Simulation Results

Monte Carlo simulations were performed in the case of considering the performance of the FCME algorithm. In the simulations there were 10000 rounds. PU signal was present randomly 50% of the time and each SU finds PU signal with probabilities $P_d = 0.8$ and $P_{fa} = 0.1$. The FCME algorithm does not know these probabilities. It is assumed that average SNR values for SUs are equal, i.e., PU is far away from SUs. Size of the initial set was $m = 4$, threshold parameters were $T_{cme1} = 1.9$ and $T_{cme2} = 0.7$ [25], there were $N = 12$ SUs and $K = 20$ consecutive decisions were taken into account. When there was one 'always one' malicious user, it was detected in 96% of the cases. No 'always one' malicious users were falsely found. When there was one 'always zero" malicious user, it was found in 99.7% of the cases. 'Always one' malicious users were falsely found in 0.3% of the cases. When there was one 'always one' malicious user and one 'always zero' malicious user present at the same time, the FCME algorithm found 'always one' malicious user in 80% of the cases and 'always zero' malicious user in 99.7% of the cases. When there were no malicious users at all, the FCME algorithm falsely found 'always one' malicious user in 0.1% of the cases and 'always zero' malicious user in 0.5% of the cases.

In the presence of 'always zero' MUs, the initial set affects to the detection performance of the FCME algorithm, because it takes the smallest samples to the initial set. The performance of the FCME algorithm can be enhanced by leaving some of the smallest samples outside the initial set. In that case, the FCME algorithm found 'always one' malicious user in 93% of the cases and 'always zero' malicious user in 93% of the cases. This type of initial set selection has slight effect to the detection performance of 'always one' malicious users.

Next, $N = K = 20$, $T_{cme1} = 1.7$ and $T_{cme2} = 0.7$, and the number of MUs varies. The detection is performed only if all the MUs are detected. In Fig. 5, the number of 'always one' MUs varies and there are no 'always zero' MUs. It can be seen that the 'always one' MUs are detected in about 95% of the cases until the 'always one' MUs cover more than 80% of the SUs, i.e., until the initial set (20% of SUs) consists MUs. No 'always zero' MUs were found, as expected, because there are no 'always zero' MUs present. The larger K the better P_d. For example, when $K = 30$, $P_d = 98\%$, and when $K = 10$, $P_d = 70\%$. In Fig. 6, there is also one 'always zero' MU. The detection performance of 'always one' MUs is about in the same level as in the previous case. The 'always zero' MU is found over 95% of the cases until the 'always one' MUs cover more than 80% of the SUs. When there were no malicious users at all, the FCME algorithm falsely found 'always one' malicious user in 0.2% of the cases and 'always zero' malicious user in 0.3% of the cases.

The FCME method is a threshold setting method so the used threshold parameter T_{cme} affects to its performance [25]. The larger T_{cme1} is, the larger the mean must be before SU is classified as MU (Fig. 7). It depends on the situation which one is better, to classify too many or too less SUs as MUs and, thus, reject their decisions.

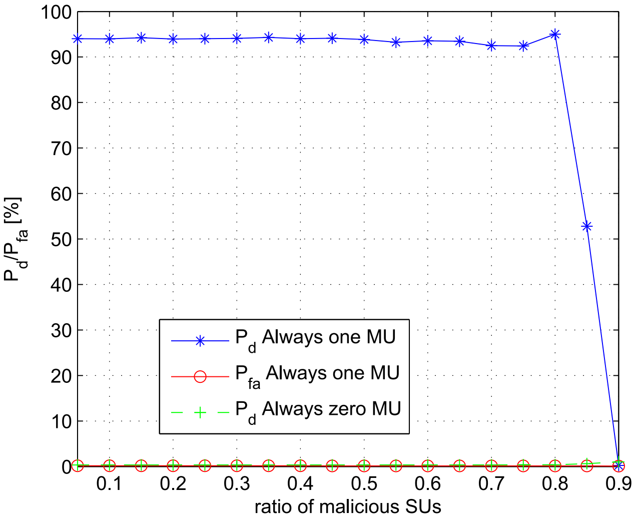


Fig. 5. Detection probability of MUs with varying number of 'always one' MUs. There are no 'always zero' MUs.

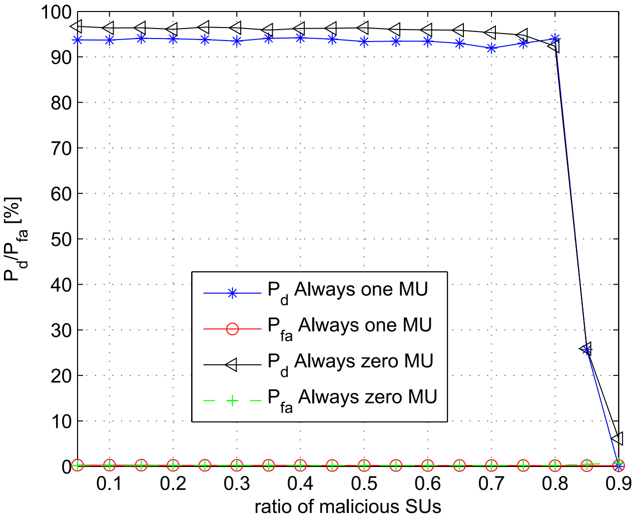


Fig. 6. Detection probability of MUs with varying number of 'always one' MUs. There is one 'always zero' MU.

The benefit of using the blind and simple FCME algorithm is that about 80% of the SUs can be MUs and the FCME method still operates. In addition, the FCME algorithm and its applications can be used in sensing [25], so it is possible that individual SUs make their sensing using the FCME method or its application, send their decision (1 or 0) to CU, and 'always one/zero' MUs are detected using that same method. This reduces the overall computational complexity when the same method can be used to both sensing and MU detection.

Assuming equal SNRs is commonly used assumption in the literature. However, the problem is that the received SNRs may vary between SUs. Sending 'always ones' can be due to good SNR and a SU with a poor received SNR does not

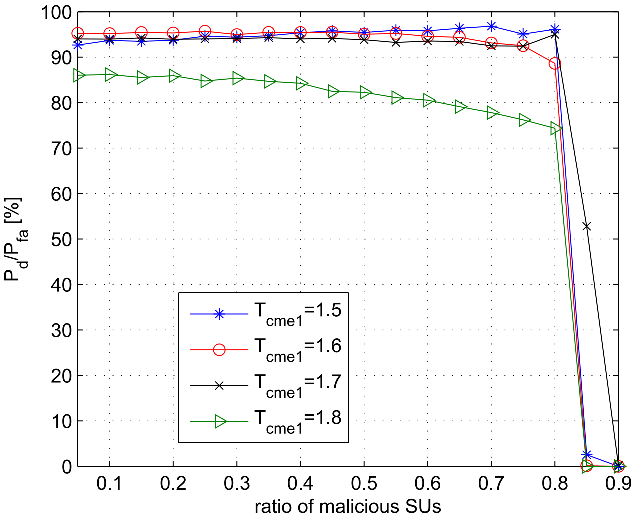


Fig. 7. Detection probability of MUs with varying number of 'always one' MUs and different values of threshold parameter T_{cme1}. There are no 'always zero' MUs.

detect the signal and, thus, sends zero even though there is a signal present. In some situations it can be assumed that PU is far away from all SUs so that SNRs are equal but this is not always the case. This SNR problem can be avoided, for example, using so called trust metrics that define how fairly the SUs are behaving [9], [26]. Thus, SUs that have high trust metric are known not to be MUs and their decisions are not rejected even though they transmit continuously ones/zeros.

In future work, comparison between other methods could be done, and deciding proper parameters like initial set and threshold parameters in different network environments could be investigated.

VII. Conclusions

The computationally simple and effective forward consecutive mean excision (FCME) algorithm is proposed for 'always one/zero' MU detection in cooperative sensing. Simulation results show that the FCME method is able to operate even when 80% of the secondary users are 'always one' MUs.

References

[1] J. Mitola III, "Cognitive radio architecture evolution," *IEEE Proceedings*, vol. 97, no. 4, pp. 626–641, 2009.

[2] C. Cordeiro, K. Challapali, D. Birru, and S. N. Shankar, "Spectrum agile radios: Utilization and sensing architectures," in *DYSPAN*, Baltimore, USA, Nov. 2005, vol. 1, pp. 328–337.

[3] J. Lunden, V. Koivunen, A. Huttunen, and H. V. Poor, "Collaborative cyclostationary spectrum sensing for cognitive radio systems," *IEEE Transactions on Signal Processing*, vol. 57, no. 11, pp. 4182–4195, 2009.

[4] J. Lehtomäki, J. Vartiainen, Z. Khan, and T. Bräysy, "Selection of cognitive radios for cooperative sensing," in *3rd International Workshop on Cognitive Radio and Advanced Spectrum Management COGART 2010 (Invited paper)*, Rome, Italy, Nov. 2010.

[5] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communication*, vol. 4, pp. 40–62, 2011.

[6] T. Fawcett and F. Provost, "Adaptive fraud detection," *Mining and Knowledge Discovery*, vol. 1, no. 3, pp. 291–316, 1997.

[7] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," *Statistical Science*, vol. 17, no. 3, pp. 235–255, 2002.

[8] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, 2008.

[9] T. Clancy and N. Goergen, "Security in cognitive radio networks: threats and mitigation," in *3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, May 2008.

[10] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 2, pp. 774–786, 2011.

[11] T. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: A multi-dimensional analysis and assessment," *Mobile Netw. Applicat.*, vol. 13, no. 5, pp. 516–532, 2008.

[12] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *IEEE International Conference on Communications (ICC)*, May. 2008.

[13] V. Barnett and T. Lewis, *Outliers in Statistical Data*, Wiley Publisher, 1994.

[14] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Transactions on Wireless Communications*, vol. 9, no. 8, Aug. 2010.

[15] R. Chen, J. M. Park, and K. Bian, "distributed spectrum sensing in cognitive radio networks," in *IEEE Conference on Computer Communications (Infocom)*, 2008.

[16] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Conference on Information Sciences and Systems (CISS)*, 2009.

[17] W. Wang, H. Li, Y. Sun, and Z. Han, "Catchit: detect malicious nodes in collaborative spectrum sensing," in *IEEE Conference on Global Communications (Globecom)*, 2009.

[18] H. Li and Z. Han, "Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3554–3565, 2010.

[19] F. Adelantado and C. Verikoukis, "A non-parametric statistical approach for malicious users detection in cognitive wireless ad-hoc networks," in *IEEE International Conference on Communications (ICC)*, 2011.

[20] Z. Khan, J. Lehtomäki, K. Umebayashi, and J. Vartiainen, "On the selection of the best detection performance sensors for cognitive radio networks," *IEEE Signal Processing Letters*, vol. 17, no. 4, Apr. 2010.

[21] K. Zeng, J. Wang, S. Li, and D. Cabric, "Robust node selection for cooperative spectrum sensing with malicious users," in *MILCOM*, Baltimore, MD, USA, 2011.

[22] F. Gao, W. Yuan, W. Liu, W. Cheng, and S. Wang, "A robust and efficient cooperative spectrum sensing scheme in cognitive radio networks," in *ICC*, 2010.

[23] H. Saarnisaari, P. Henttu, and M. Juntti, "Iterative multidimensional impulse detectors for communications based on the classical diagnostic methods," *IEEE Trans. Commun.*, vol. 53, no. 3, pp. 395–398, March 2005.

[24] J. Vartiainen, J. J. Lehtomäki, H. Saarnisaari, and M. Juntti, "Analysis of the consecutive mean excision algorithms," *J. Elect. Comp. Eng.*, 2011.

[25] J. Vartiainen, *Concentrated Signal Extraction Using Consecutive Mean Excision Algorithms*, Ph.D. thesis, Acta Univ Oul Technica C 368. Faculty of Technology, University of Oulu, Finland, Nov. 2010, http://jultika.oulu.fi/Record/isbn978-951-42-6349-1.

[26] S. T. Zargar, M. B. H. Weiss, C. E. Caicedo, and J. B. D. Joshi, "Security in dynamic spectrum access systems: A survey," in *Telecommunications Policy Research Conference*, Arlington VA, 2009.