Block Outlier Methods for Malicious User Detection in Cooperative Spectrum Sensing

Sanket S. Kalamkar, Praveen Kumar Singh, and Adrish Banerjee
Department of Electrical Engineering, Indian Institute of Technology Kanpur, India
Email: {kalamkar, adrish}@iitk.ac.in

***Abstract*—Block outlier detection methods, based on Tietjen-Moore (TM) and Shapiro-Wilk (SW) tests, are proposed to detect and suppress spectrum sensing data falsification (SSDF) attacks by malicious users in cooperative spectrum sensing. First, we consider basic and statistical SSDF attacks, where the malicious users attack independently. Then we propose a new SSDF attack, which involves cooperation among malicious users by masking. In practice, the number of malicious users is unknown. Thus, it is necessary to estimate the number of malicious users, which is found using clustering and largest gap method. However, we show using Monte Carlo simulations that, these methods fail to estimate the exact number of malicious users when they cooperate. To overcome this, we propose a modified largest gap method.**

***Index Terms*—Block outlier detection, cooperative spectrum sensing, malicious user, spectrum sensing data falsification attack.**

I. Introduction

A. Data Falsification in Cooperative Spectrum Sensing

In cooperative spectrum sensing (CSS), multiple secondary users (SUs) cooperate to effectively detect a primary user (PU), by exploiting the spatial diversity. However, the cooperation among SUs raises concerns about reliability and security of CSS, as some of the SUs may report the falsified spectrum sensing data to the fusion centre. The falsified reported data can easily influence the spectrum sensing decision taken by the fusion centre. The falsification of data may occur either by malfunctioning of SUs or by intentional manipulation of data by certain SUs, called malicious users (MUs). The data reported by malfunctioning SUs may differ from the actual data. In addition, MUs can attack by manipulating the reported data with selfish intention, i.e., to gain access to the channel, or to cause interference to PU. Since the spectrum sensing data is falsified in this attack, this is called spectrum sensing data falsification (SSDF) attack [1].

An outlier is the data, that appears to be inconsistent with rest of the data [2]. The local spectrum sensing data reported by MUs may differ from the actual sensed data. Thus, MUs reporting the falsified spectrum sensing data, can be considered as outliers and detected using outlier detection techniques.

B. Summary of Results and Related Work

1) Summary of Results: Firstly, we propose two block outlier detection methods, based on Tietjen-Moore (TM) test [3] and Shapiro-Wilk (SW) test [4], to counter different SSDF attacks in CSS as shown in Fig. 1, and compare them with box plot and median absolute deviation (MAD) tests [5]. We show that TM and SW tests are more robust to SSDF attacks than the box plot and MAD tests. Secondly, we propose a new SSDF attack, called *cooperative attack*, in CSS framework, which involves cooperation among MUs by masking. Thirdly, for cooperative attack, we propose a modified largest gap method, which can accurately estimate the number of outliers, required by TM and SW tests, whereas clustering [6] and the largest gap method [3] fail to estimate the exact number of outliers.

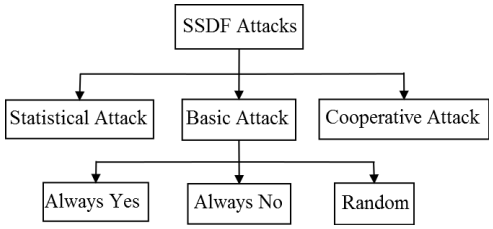

Fig. 1. SSDF attack models

2) Related Work: The basic SSDF attacks like "Always Yes," "Always No" and "Random" are studied in [1], [7]. In [8], [9], the statistical attack is considered, where MUs act maliciously with a certain probability. However, in these attacks, no cooperation among MUs is considered. A consensus-based method is proposed to overcome the basic SSDF attacks [7]. To counter the statistical attack, in [8], an onion-peeling approach based on calculation of suspicious levels is adopted, while in [9], belief propagation is used. The reputation and weight based methods try to alleviate the detrimental effects of MUs by assigning trust values or weights to SUs based on the credibility of SUs, and are studied in [10]–[14]. In [15], a scenario is considered where multiple MUs can overhear the honest SU sensing data. Two attack-prevention mechanisms based on direct and indirect punishment are proposed to foil such attacks.

In [16], an outlier detection method is proposed to pre-filter the extreme data, followed by the calculation of weights based on mean of the received spectrum sensing data. This method is further extended in [17], where the outlier factors are calculated using weighted sample mean and standard deviation of the received sensing data. Based on the dynamic PU activity and the sensing data from the closest SUs, the outlier factors are adjusted. In [5], the detection performances of different outlier methods like MAD, box plot and median rule, are compared under low SNR nodes scenario (similar to "Always No" attack). Anderson-Darling goodness-of-fit test is used in [18] to detect MUs by checking whether empirical distribution of SUs fit the expected distribution of a MU. In [19], the outlier

This work was supported in part by the TCS research scholarship program at Indian Institute of Technology Kanpur, India.

TABLE I
NOTATIONS

Notation	Meaning
H_1	Hypothesis when the primary user is present.
H_0	Hypothesis when the primary user is absent.
M	Number of sensing samples.
α	Received signal-to-noise ratio (SNR) at SU.
P_{FA}	Probability of false alarm at a single SU.
P_D	Probability of detection at a single SU.
Q_{FA}	Probability of false alarm at fusion centre.
Q_D	Probability of detection at fusion centre.
L	Number of malicious SUs.
P	Number of honest SUs.
N	Number of cooperating SUs.

tests like Dixon's test, box plot and Grubbs' test are studied to detect a single MU with basic attacks in CSS.

II. System Model

Consider a centralized CSS scenario with N SUs, one PU and a fusion centre. Secondary users perform local spectrum sensing using energy detection [20] and report the sensed energies to the fusion centre. Let H_1 and H_0 denote the binary hypothesis corresponding to the presence and absence of PU respectively. Then the detection problem of PU can be formulated as follows:

$$y(m) = \begin{cases} s(m) + u(m), & H_1, \\ u(m), & H_0, \end{cases} \tag{1}$$

where $y(m)$ is the mth sample of the received signal by a SU with $m = 1, \ldots, M$, $s(m) \sim \mathbb{CN}(0, \sigma_s^2)$, is the PU signal, and $u(m) \sim \mathbb{CN}(0, \sigma_u^2)$, is additive white Gaussian noise (AWGN). We assume that $s(m)$ and $u(m)$ are independent. The primary signal samples are assumed to be independent. Also, we assume that the noise samples are independent. The received signal-to-noise ratio (SNR) is $\alpha = \frac{\sigma_s^2}{\sigma_u^2}$.

The test statistic T for the energy detector is given by [20]

$$T(y) = \frac{1}{M} \sum_{m=1}^{M} |y(m)|^2, \tag{2}$$

and it is chi-squared distributed. However, for large M ($M > 10$), the test statistic can be approximated by Gaussian distribution according to central limit theorem. For this, the expressions of the probability of false alarm P_{FA} and the probability of detection P_D are given as follows [21]:

$$P_{FA} = Q\left[\left(\frac{\lambda}{\sigma_u^2} - 1\right)\sqrt{M}\right]; P_D = Q\left[\left(\frac{\lambda}{\sigma_u^2} - \alpha - 1\right)\frac{\sqrt{M}}{\alpha + 1}\right],$$

where λ is a predetermined threshold. The fusion centre uses majority logic [21] as a fusion rule, i.e., the final decision taken by the fusion centre is consistent with the local decisions taken by majority of SUs. The probability of false alarm and the probability of detection after fusing the local decisions at the fusion centre are denoted by Q_{FA} and Q_D respectively.

Let L and P be the number of the malicious and the honest SUs respectively. We assume that the majority of SUs are honest ($L < P$). Thus, the falsified spectrum sensing data (falsified energy values in our case) by MUs, do not agree with the majority of the data reported by the honest users. Using outlier techniques, such malicious SUs are detected, and removed from cooperation to detect PU. The final decision about PU is made by fusing the local spectrum sensing decisions of only honest SUs.

III. Cooperative Attack

The basic and statistical attack models assume that MUs act independently, i.e., they do not cooperate among themselves. However, the more effective SSDF attacks may be launched if MUs cooperate with each other. In the proposed model, we consider that MUs cooperate using *masking*. It is seen that the outlier tests suffer from the problem of masking [22]. In masking, there exists extreme as well as not-so-extreme (mild) outliers. The extreme outliers modify the test statistic of an outlier test used to detect outliers such that, the presence of not-so-extreme outliers is shadowed by the extreme outliers, i.e., the outlier test fails to detect the not-so-extreme outliers, and only the extreme outliers are detected.

In the framework of CSS with energy detection, masking can be done as follows: A fraction of MUs report significantly different energy values than the actual sensed values, and the remaining MUs report slightly different energy values than the actual sensed values. This alters the test statistic used by an outlier test to detect outliers. The alteration in the test statistic is made such that, MUs which have reported slightly different energy values, escape from getting declared as outliers. Thus, they can continue to send the falsified sensing data to the fusion centre to influence the spectrum sensing decision.

IV. Multiple Outliers Detection

The multiple outliers can be present in three locations of the sorted data as follows:

- Upper outlier: Unexpected large values.
- Lower outlier: Unexpected small values.
- Bi-directional outliers: Both upper and lower outliers are present.

An outlier test should be able to identify all types of outliers. To know the type of an outlier, it is required to apply outlier tests designed for upper, lower or bi-directional outliers, on the received data. The data declared as outliers, are categorized as upper, lower or bi-directional outliers, based on which outlier test has detected them as outliers. An outlier test can be applied using either of the following two procedures:

- Consecutive procedure: It is also called recursive procedure, that makes repeated use of a single outlier detection test, to remove outliers one by one. However, it is inappropriate to use a test for a single outlier detection recursively to detect multiple outliers [2]. Also, even though consecutive tests are easy to apply, they are inefficient for large data with many outliers.
- Block procedure: In this procedure, the outliers are tested in a block. The test requires calculation of the test statistic based on the received data. The test statistic is compared with the critical value, and based on this comparison, the whole block of data is adjudged as either outlier or non-outlier. In this paper, we consider two multiple outliers detection tests based on block procedure as follows:

– Tietjen-Moore (TM) test
– Shapiro-Wilk (SW) test.

A. Tietjen-Moore Test

Tietjen and Moore proposed three test statistics [3] to detect multiple outliers. All types of outliers, whether upper, lower or bi-directional, can be tested by choosing a suitable test statistic. The algorithm to detect upper or lower outliers is given by Algorithm 1.

Algorithm 1 TM Test for Upper/Lower Outliers

1: Sort the received energy values $y_1, \ldots, y_N$ of N SUs in ascending order. Let this sorted values be denoted by $x_1, \ldots, x_N$.
2: Estimate t, the number of outliers (discussed in Section IV-C).
3: Calculate the test statistic given in (3) (for upper outliers), or given in (4) (for lower outliers).
4: Compare this test statistic with the critical value for significance level of 0.05, from the table given in [3].
5: If the test statistic is less than the critical value, then the suspected data are declared as outliers.

The test statistic for testing upper outliers is as follows [3]:

$$T = \frac{\sum_{j=1}^{N-t}(x_j - \bar{x}_t)^2}{\sum_{j=1}^{N}(x_j - \bar{x})^2}, \tag{3}$$

where $\bar{x}$ is the sample mean of the sorted data and $\bar{x}_t$ is given by $\bar{x}_t = \frac{\sum_{j=1}^{N-t} x_j}{N-t}$. Similarly, the test statistic to test lower outliers is given by [3]

$$T^* = \frac{\sum_{j=t+1}^{N}(x_j - \bar{x}_t^*)^2}{\sum_{j=1}^{N}(x_j - \bar{x})^2}, \tag{4}$$

where $\bar{x}_t^* = \frac{\sum_{j=t+1}^{N} x_j}{N-t}$. The algorithm for applying TM test to detect bi-directional outliers is as follows:

Algorithm 2 TM Test for Bi-directional outliers

1: Compute the mean $\bar{y}$ of the received energy values $y_1, \ldots, y_N$.
2: Compute N absolute residuals $r_j = |y_j - \bar{y}|$, where $j = 1, \ldots, N$.
3: Arrange r_j's in ascending order. Let this arranged data be denoted by $x_1, \ldots, x_N$.
4: Estimate t, the number of outliers.
5: Calculate the test statistic as per (3).
6: Perform steps 4 and 5 of Algorithm 1.

B. Shapiro-Wilk Test

This test, proposed by Shapiro and Wilk [4], is composed by considering a linear combination of ordered data, squaring it and then dividing it by an estimate of variance. The proposed test statistic is location and scale invariant, and is suitable for all types of data. The algorithm to apply SW test is given by Algorithm 3. The test statistic for SW test is given as [4]

$$T = \frac{\sum_{j=1}^{[\frac{N}{2}]} a_{N,N-j+1}(x_{N-j+1} - x_j)^2}{S^2}, \tag{5}$$

where,

$$S^2 = \sum_{j=1}^{N}(x_j - \bar{x})^2 \text{ with } \bar{x} = \frac{\sum_{j=1}^{N} x_j}{N}. \tag{6}$$

Here, $[\frac{N}{2}]$ is the integer part of $\frac{N}{2}$, and $a_{N,j}$ is the tabulated constant. The tables of tabulated constants and the critical values for significance level of 0.05 are given in [4].

Algorithm 3 SW Test

1: Sort the received energy values $y_1, \ldots, y_N$ of N SUs in ascending order. Let this sorted values be denoted by $x_1, \ldots, x_N$.
2: Estimate t, the number of outliers.
3: Calculate the test statistic as per (5) and (6).
4: If the test statistic is less than the critical value for significance level of 0.05, then the suspected data are declared as outliers.

C. Estimating the Number of Outliers

In practice, the number of MUs is not known. Also, to apply TM and SW tests, an estimate of the number of outliers is required. For this, we consider clustering and the largest gap method proposed in the literature, and are described as follows:

1) Clustering method: We consider clustering as a tool to estimate the number of outliers. We use k-means clustering algorithm [6] to group the data set into two clusters. The smaller of these clusters is treated as a cluster of suspected outliers, and is tested against TM and SW tests, to decide whether this assumption is true or not.

2) Largest gap method: Tietjen and Moore proposed a method based on the largest gap between the data points, as a basis to estimate the number of outliers [3]. For upper/lower outliers, the procedure for the largest gap method is as follows:

Algorithm 4 Largest Gap method for Upper/Lower Outliers

1: Sort the received data (energy values) in ascending order for upper outliers (descending order for lower outliers).
2: Calculate the gaps between successive data points.
3: Find the position of the largest gap.
4: The number of data points to the right of this position gives an estimate of number of outliers.

The largest gap method for bi-directional outliers is given as follows:

Algorithm 5 Largest Gap Method for Bi-directional Outliers

1: Sort the received data set (energy values) D in ascending order and divide it into two halves, lower half D_{LH} and upper half D_{RH}.
2: Apply largest gap method for upper outliers, proposed in Algorithm 4 to D_{RH} and largest gap method for lower outliers to D_{LH}, to get an estimate of number of outliers in both halves.
3: Apply TM/SW test on both D_{RH} and D_{LH} separately, to decide which half contains outliers.

We show in Section V that, when MUs launch cooperative attack using masking, both clustering and largest gap method fail to estimate the correct number of outliers. Thus, to overcome this, we propose a modified largest gap (MLG) method, which can give the suspected number of outliers accurately under cooperative malicious users attack.

D. Proposed Method: Modified Largest Gap

The proposed modified largest gap method involves applying the largest gap method recursively until all the outliers are detected. The algorithm to apply MLG for detection of upper outliers is given as follows:

Algorithm 6 MLG method for Upper Outliers

1: Sort the received data set (energy values) D' in ascending order to obtain D.
2: Divide D in two halves: Lower half (D_{LH}) and upper half (D_{UH}).
3: As the number of outliers is in minority, D_{UH} may consist of the energies reported by malicious users.
4: Calculate the gap between successive data points in D_{UH}.
5: Find the position of the largest gap (denoted by G_{pos}).
6: Let S_1 be the set of data points to the left of the G_{pos} in D_{UH}, and let S_2 be the set of data points to the right of the G_{pos} in D_{UH}. Form a new set $S = D_{LH} \cup S_1$.
7: Test whether S_2 is outlier (using TM test).
8: If S_2 is outlier, then reject S_2; let $D = S$, and go to Step 2. Else, $S \cup S_2$ is a data set of honestly reported energy values.

For lower outliers, the MLG method is the same as that of upper outliers, except that the data is sorted in descending order. The procedure to apply MLG for bi-directional outliers is same as Algorithm 5, except the largest gap method is replaced by the MLG method.

V. Simulation Results

In this section, we present Monte Carlo simulation results to show the spectrum sensing performance of CSS with outlier tests, to defend different SSDF attacks as shown in Fig. 1. In simulations, we have considered the following parameters: σ_u^2 = 1, M = 10000, N = 20, L = 4. The energy value reported by a MU differs from the actual sensed value by 0.5 dB.

A. Suppressing malicious users in the basic attack model

For "Always Yes" attack (Fig. 2), all the outlier tests considered in this paper are able to detect all the MUs successfully. It is shown that Q_{FA} can be decreased by refraining MUs from participating in CSS, compared to when all SUs including MUs participate in CSS. Also, the outlier tests perform similarly for "Always No" attack (results are not shown due to space constraint). However, for "Random" attack (Fig. 3), TM and SW tests are more robust than the box plot and MAD tests. This is because TM and SW tests are able to detect all randomly behaving 4 MUs, but the box plot and MAD tests can detect only a fraction of MUs, giving

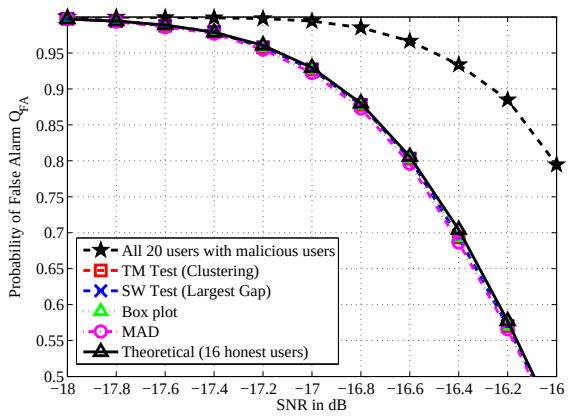

Fig. 2. "Always Yes" attack: Comparison of outlier tests, Q_D = 0.99.

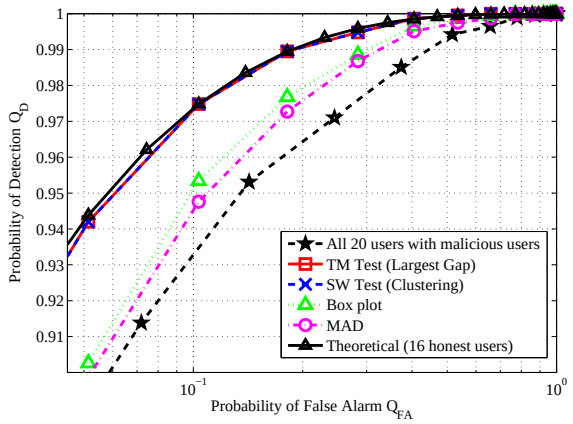

Fig. 3. "Random" attack: Comparison of outlier tests, SNR = -20 dB.

worse performance. Both clustering and the largest gap method perform the same, when they are used to estimate the number of outliers (Figs. 2 and 3). It can also be noticed that TM and SW tests perform the same.

B. Suppressing malicious users in statistical attack model

It is shown in Fig. 4 that, TM and SW tests are good enough to counter the statistical attack, when MUs act maliciously with a certain probability. Clustering is used to estimate the number of MUs for both TM and SW tests. Box plot's detection performance is almost the same as TM and SW tests, while MAD test performs the worst.

C. Suppressing malicious users in cooperative attack model

As aforementioned, MUs may cooperate using masking. We consider that all MUs are upper outliers. Masking is done, as half of the outliers are extreme outliers reporting significantly high energy values (6.5 dB greater than the actual sensed energy in our case), and the rest are mild outliers reporting slightly higher energy values than the actual energy values (0.5 dB greater than the actual sensed value). Then, as shown in Fig. 5, TM or SW tests fail to counter cooperative attack when

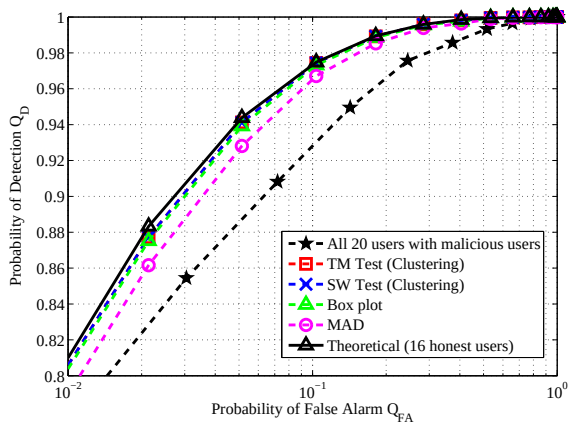

Fig. 4. Statistical attack: Comparison of outlier tests, SNR = -20 dB.

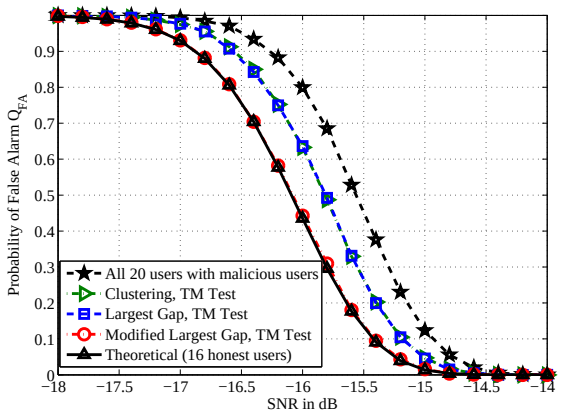

Fig. 5. Cooperative "Always Yes" attack: TM test with different methods to estimate number of outliers, Q_D = 0.99.

clustering or the largest gap method is used to estimate the number of MUs. In clustering, the smaller cluster might consist of only extreme outliers, and no mild outliers as the latter ones may be masked by the former ones. For the largest gap method, the largest gap occurs between mild outliers and extreme outliers, as the energies reported by the extreme outliers are significantly different from rest of the energy values. However, the proposed modified largest gap method is highly effective in estimating the accurate number of cooperating MUs, as it finds the largest gap recursively until all the outliers are detected, thus nullifying their harmful effects.

VI. Conclusions

In this paper, two block outlier tests, TM test and SW test, are proposed to suppress an unknown number of the malicious users in cooperative spectrum sensing, and compared with box plot and MAD tests. We have shown that TM and SW tests are more robust than the box plot and MAD tests for "Random" and statistical attacks. We have also proposed a cooperative SSDF attack, which adopts cooperation among malicious users by masking, where the presence of extreme outliers mask the mild outliers. Also, it is shown using Monte Carlo simulations that, clustering and the largest gap method fail to accurately estimate the number of outliers in cooperative attack. Thus, to overcome this shortcoming, we propose a modified largest gap method, which can accurately estimate the number of outliers under cooperative attack.

References

[1] R. Chen, J. Park, Y. Hou, and J. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 50–55, 2008.

[2] V. Barnett and T. Lewis, *Outliers in statistical data.* John Wiley & Sons Ltd., 2nd ed., 1978.

[3] G. Tietjen and R. Moore, "Some Grubbs-type statistics for the detection of several outliers," *Technometrics*, vol. 14, no. 3, pp. 583–597, 1972.

[4] S. Shapiro and M. Wilk, "An analysis of variance test for normality (complete samples)," *Biometrika*, vol. 52, no. 3, pp. 591–611, 1965.

[5] H. Le, M. Ohta, K. Inage, T. Fujii, K. Muraoka, and M. Ariyosh, "Outlier detection methods of low snr nodes for cooperative spectrum sensing," in *Proc. Int. Symp. Wireless Commun. Syst.*, (York, UK), pp. 966–970, Sep. 2010.

[6] J. MacQueen, "Some methods for classification and analysis of multivariate observations," in *Proc. Berkeley Symp. Math., Stat. and Prob.*, vol. 1, pp. 281–297, 1967.

[7] F. Yu, H. Tang, M. Huang, Z. Li, and P. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in *Proc. IEEE MILCOM,*, (Boston, MA), pp. 1–7, Oct. 2009.

[8] W. Wang, H. Li, Y. Sun, and Z. Han, "Catchit: Detect malicious nodes in collaborative spectrum sensing," in *Proc. IEEE GLOBECOM*, (Hawaii, USA), pp. 1–6, 2009.

[9] F. Penna, Y. Sun, L. Dolecek, and D. Cabric, "Detecting and counteracting statistical attacks in cooperative spectrum sensing," *IEEE Trans. Signal Process.*, vol. 60, pp. 1806–1822, Apr. 2012.

[10] T. Zhao and Y. Zhao, "A new cooperative detection technique with malicious user suppression," in *Proc. IEEE ICC*, (Dresden, Germany), pp. 1–5, June 2009.

[11] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Proc. Annual Conf. Information Sciences and Syst., 2009*, (Baltimore, MD), pp. 130–134, Mar. 2009.

[12] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. IEEE INFOCOM*, (Phoenix, AZ), pp. 1876–1884, April 2008.

[13] K. Zeng, P. Paweczak, and D. Cabric, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Commun. Lett.*, vol. 14, no. 3, pp. 226–228, 2010.

[14] K. Arshad and K. Moessner, "Robust collaborative spectrum sensing in the presence of deleterious users," *IET Commun.*, vol. 7, no. 1, pp. 49–56, 2013.

[15] L. Duan, A. Min, J. Huang, and K. Shin, "Attack prevention for collaborative spectrum sensing in cognitive radio networks," *IEEE J. Sel. Areas in Commun.*, vol. 30, no. 9, pp. 1658–1665, 2012.

[16] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *Proc. IEEE ICC*, (Beijing, China), pp. 3406–3410, May 2008.

[17] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Trans. Wireless Commun.,*, vol. 9, pp. 2488–2497, Aug. 2010.

[18] G. Noh, S. Lim, S. Lee, and D. Hong, "Goodness-of-Fit-based malicious user detection in cooperative spectrum sensing," in *IEEE VTC-Fall*, (Quebec City, Canada), pp. 1–5, 2012.

[19] S. Kalamkar, A. Banerjee, and A. Roychowdhury, "Malicious user suppression for cooperative spectrum sensing in cognitive radio networks using Dixon's outlier detection method," in *Proc. National Conf. Commun.*, (IIT Kharagpur, India), pp. 1–5, Feb. 2012.

[20] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE*, vol. 55, pp. 523–531, Apr. 1967.

[21] Y. Liang, Y. Zeng, E. Peh, and A. Hoang, "Sensing-Throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326–1337, 2008.

[22] S. Bendre and B. Kale, "Masking effect on tests for outliers in normal samples," *Biometrika*, vol. 74, pp. 891–896, Dec. 1987.