Malicious User Suppression for Cooperative Spectrum Sensing in Cognitive Radio Networks using Dixon's Outlier Detection Method

Sanket S. Kalamkar and Adrish Banerjee
Department of Electrical Engineering
Indian Institute of Technology
Kanpur 208016, India
Email: {kalamkar, adrish}@iitk.ac.in

Ananya Roychowdhury
Department of Electronics and Communication Engineering
National Institute of Technology
Jamshedpur, India

***Abstract*—Cooperation among multiple secondary users improves the cognitive radio sensing system performance, but the presence of malicious secondary users may severely degrade the same. In this paper, we study the detection and elimination of such malicious users in a cooperative sensing system using Dixon's outlier test and compare its performance with Grubb's test and boxplot test. We have shown using receiver operating characteristics curves that Dixon's test outperforms Grubb's test and boxplot test for the case of a single malicious user. We also illustrate the limitations of Dixon's test for several malicious users using an example of two malicious users in a cooperative spectrum sensing setting for cognitive radio.**

I. Introduction

According to a survey conducted by the Federal Communication Commission (FCC) [1], most of the allocated spectrum is underutilized which leads to inefficient usage of allotted spectrum. To improve usage of allotted spectrum, cognitive radio based on Software Defined Radio (SDR) allows opportunistic usage of frequency bands that are not used by licensed users [2]. Cognitive radio relies on efficient spectrum sensing to detect vacant spectrum bands.

Sensing performance of a single unlicensed or secondary user (SU) sensing may degrade due to presence of various channel effects such as fading, shadowing and due to hidden terminal problem experienced by the secondary user. Cooperative spectrum sensing (CSS) involves exchange of local sensing decisions between multiple secondary users using a centralized or decentralized fusion center to arrive at a final decision regarding presence or absence of primary user (PU) [3]. However, collaboration between multiple SUs also raises a number of security risks. One of the security issues is the Spectrum Sensing Data Falsification (SSDF) attack, where a malicious secondary user purposely report false local sensing reports to other secondary users, and thereby wrongly influencing the overall decision. Also, it is possible that a malfunctioning sensing terminal unwillingly reports incorrect local sensing reports, thereby degrades its performance. Cooperative spectrum sensing has to be robust against such deceitful local spectrum sensing results reported by malicious or malfunctioning secondary users, and hence the need for good outlier detection schemes for cooperative spectrum sensing.

In [4], authors have used Weighted Sequential Probability Ratio Test (WSPRT) to identify malfunctioning or malicious terminals based on reputation rating assigned to every cooperating terminal. In [5], authors compute the suspicious level of secondary users based on their past sensing reports. Trust values as well as consistency values of cooperating secondary users are calculated which are then used to eliminate the influence of malicious users on the primary user detection. Outlier based malicious user detection is proposed in [6] where untrustworthy terminals are detected by applying an outlier detection methods and corresponding sensing reports are ignored while making final decision on the availability of a spectrum band. In [7], authors have compared several outliers detection methods for low SNR scenario. In this paper, we have proposed a new outlier detection scheme based on Dixon's test [8] to detect the presence of malicious users. We have compared the same with outlier detection schemes based on Grubb's test and modified test mentioned in [6]. We also compare boxplot method with Dixon's test. Finally we illustrate the limitation of Dixon's test for the case of multiple malicious users.

The rest of the paper is organized as follows. In section II, we present the system model for cooperative spectrum sensing system. In Section III we enumerate different attack models that we have considered in this paper for spectrum sensing data falsification attacks. In Section IV, we state the outlier detection technique based on Dixon's test. In section V, we compare the performance of Dixon's test with some other techniques such as test based on Grubb's method [6], and boxplot method for cooperative spectrum sensing using energy detection technique for different SSDF attack models. We conclude the paper with some comments and scope for future work in section VI.

II. System Model

We have considered a system model similar to that of [6]. In this model, we have N SUs cooperating among each

other to detect the presence of a single PU. Secondary users employ energy detection to detect the presence or absence of primary user locally. Then they send their energy values through an errorfree control channels to the fusion center. Let H_0 and H_1 be the hypotheses representing absence and presence of PU respectively. We denote energy received by a n^{th} SU in decibels during k^{th} sensing iteration by $e_n[k]$. Under hypothesis H_0, this is given by

$$e_n[k] = 10\log_{10}\left(\int_{T_k}^{T_k+T-1} |v_n(t)|^2 dt\right) \tag{1}$$

while under hypothesis H_1,

$$e_n[k] = 10\log_{10}\left(\int_{T_k}^{T_k+T-1} |x(t)+v_n(t)|^2 dt\right) \tag{2}$$

where the length of sensing interval is denoted by T, the time when k^{th} time interval begins is represented by T_k. $x(t)$ denotes the primary user signal and $v_n(t)$ denotes Additive White Gaussian Noise (AWGN) received by n^{th} SU.

III. Attack Models for SSDF

Here we have considered three types of malicious user data falsification attacks, namely Always YES attack, always NO attack and malicious user randomly sending true or false value of received energy to the fusion center. In always YES case, every time malicious user reports comparatively higher received energy than the other cooperating SUs to the fusion center. The intention of this kind of malicious user is to fool other SUs to believe that the spectrum is occupied. This type of malicious user is known as *selfish user* and this attack is known as *selfish SSDF* [9]. This attack results in increase in false alarm probability. In always NO case, the malicious user always reports very low received energy suggesting absence of primary user so that SUs start using corresponding channel. The intention of this kind of attack is to cause interference to the primary user and it is known as *interference SSDF* [9]. In the third type of attack which is known as *confusing SSDF* [9], malicious user sends randomly true or false value of received energy to fusion center with the purpose to confuse other SUs.

IV. Dixon's Test

Outlier factor is a measure of deviation of a data point from the rest of the data. In outlier detection techniques, outlier factors are used to detect presence of malicious users in the cooperative spectrum sensing (CSS) system. Each SU in CSS is assigned a set of outlier factors based on its local energy detection based spectrum sensing. In this test for outliers, the data values are arranged in ascending order and outlier factor $o_n[k]$ for n^{th} user for k^{th} sensing iteration is calculated as follows [10]:

$$o_n[k] = \begin{cases} \dfrac{e_{sN}[k]-e_{s(N-1)}[k]}{e_{sN}[k]-e_{s1}[k]} & 3 \le N \le 7 \\ \dfrac{e_{sN}[k]-e_{s(N-1)}[k]}{e_{sN}[k]-e_{s2}[k]} & 8 \le N \le 10 \\ \dfrac{e_{sN}[k]-e_{s(N-2)}[k]}{e_{sN}[k]-e_{s2}[k]} & 11 \le N \le 13 \\ \dfrac{e_{sN}[k]-e_{s(N-2)}[k]}{e_{sN}[k]-e_{s3}[k]} & 14 \le N \le 20 \end{cases} \tag{3}$$

$$o_n[k] = \begin{cases} \dfrac{e_{s2}[k]-e_{s1}[k]}{e_{sN}[k]-e_{s1}[k]} & 3 \le N \le 7 \\ \dfrac{e_{s2}[k]-e_{s1}[k]}{e_{s(N-1)}[k]-e_{s1}[k]} & 8 \le N \le 10 \\ \dfrac{e_{s3}[k]-e_{s1}[k]}{e_{s(N-1)}[k]-e_{s1}[k]} & 11 \le N \le 13 \\ \dfrac{e_{s3}[k]-e_{s1}[k]}{e_{s(N-2)}[k]-e_{s1}[k]} & 14 \le N \le 20 \end{cases} \tag{4}$$

where

N :	Number of cooperating secondary users
$e_{sN}[k]$:	The highest energy value received
$e_{s(N-1)}[k]$:	Second highest energy value received
$e_{s(N-2)}[k]$:	Third highest energy value received
$e_{s1}[k]$:	Lowest energy value received
$e_{s2}[k]$:	Second lowest energy value received
$e_{s3}[k]$:	Third lowest energy value received

The value of $o_n[k]$ is compared with a critical value Q, that depends on N and the significance level. Critical values can be obtained from standard table [11] available for Dixon's test. If calculated $o_n[k]$ is less than critical value for given significance level, then the energy value under evaluation is assumed to belong the same normal population as the rest of values. It is also known as null hypothesis. On the other hand, if $o_n[k]$ is greater than that of the critical value, it is considered that the energy value under evaluation comes from an outlier. This is called as alternate hypothesis. Equation (3) is used when there is a presence of suspicious high value of received energy, while equation (4) is used if there is an outlier representing very low energy value. Whether an outlier (if it exists) is of low energy or high energy value can be found out from equation (3) and (4). Initially outlier factor $o_n[k]$ is calculated using equation (3) and if it exceeds critical value Q, then it favors presence of outlier reporting high energy. Similar is the case for detection low energy outlier. Dixon's test can detect at most a single outlier from a set of data points.

V. Simulation Results

For the purpose of simulation, we have taken N=20 co-operating SUs. We assume Additive White Gaussian Noise

(AWGN) channel. Also primary user signal is assumed to be BPSK modulated. At fusion center, energy values received from all the sensors are combined by averaging and it is then compared with the threshold as follows:

$$\frac{1}{N}\sum_{n=1}^{N} e_n[k] \lessgtr_{H_0}^{H_1} e_T \tag{5}$$

where e_T is the threshold used at fusion center. The threshold is calculated by fixing probability of false alarm to pre-defined value. We assume that the malicious user providing always NO decision, reports energy corresponding to SNR that is 20dB lower than that of average received SNR for normal user, while for the case of malicious user with always YES decision, it reports energy corresponding to SNR that is 20dB higher than that of average received SNR. For random YES-NO case, it is assumed that the SNR is either 20 dB higher or lower than the average received SNR for normal user. The significance level taken is 0.10. For simulation, we fixed the average received SNR for normal user to be 0 dB.

We have compared Dixon's test with test based on Grubb's test and boxplot method. We have simulated two methods based on Grubb's test which were presented in [6]. For sake of completeness, we state the equations governing the calculation of outlier factors for those two methods based on Grubb's test. Grubb's Test assigns outliers $o_n[k]$ for n^{th} SU in k^{th} iteration based on received energy values in decibels $e_n[k]$ as follows [6]:

$$o_n[k] = \frac{e_n[k] - \mu_n[k]}{\sigma_n[k]} \tag{6}$$

where $\mu_n[k]$: Sample mean of $e_n[k]$
$\sigma_n[k]$: Sample standard deviation of $e_n[k]$

As addressed in [6], mean and standard deviation represent the estimation of location and scale respectively, that are susceptible to malicious user attacks. A robust estimate of location is the bi-weight scale (BWS), which can be used to replace mean to calculate the outlier factor [12]. It is given by:

$$\mu^*[k] = \frac{\sum w_n[k] e_n[k]}{\sum w_n[k]} \tag{7}$$

where

$$w_n[k] = \begin{cases} \left\{\left(1 - \left(\frac{e_n[k] - \mu^*[k]}{c_1 S}\right)^2\right)\right\}, & \left(1 - \left(\frac{e_n[k] - \mu^*[k]}{c_1 S}\right)^2\right) < 1 \\ 0, & \text{Otherwise} \end{cases} \tag{8}$$

and

$$S = \text{median } \{|e_n[k] - \mu^*[k]|\} \tag{9}$$

At first, all data points are allocated equal weights and then the bi-weight estimate is calculated recursively using equation (8) in equation (7) and then using equation (7) in equation (9). S is the median absolute deviation from the location estimate $\mu^*[k]$. The parameter c_1 is the tuning constant and has a value of 6 [13]. Observations at a distance of more than $c_1 S$ have been allocated zero weight.

A robust alternative to standard deviation can be given by BWS as follows:

$$\sigma^*[k] = \sqrt{\frac{N \sum_{u_n^2<1} (e_n[k] - \mu^*[k])^2 (1-u_n^2)^4}{s(s-1)}} \tag{10}$$

where

$$s = \sum_{u_n^2<1} (1-u_n^2)(1-5u_n^2) \tag{11}$$

and

$$u_n = \frac{e_n[k] - \mu^*[k]}{c_2 \text{ median } \{|e_n[k] - \mu^*[k]|\}} \tag{12}$$

Here, c_2 is another tuning constant which is taken as 9 [13].

We refer to two test based on Grubb's test as "Grubb Method 1" and "Grubb Method 2"

A. Grubb Method 1

In this method, outlier factors are calculated using equation (6) with bi-weight as the location estimate and BWS as the scale estimate. These outlier factors are then compared with a threshold [6] for each iteration. If outlier factor lies above threshold, then the user is considered as malicious user.

B. Grubb Method 2

In this method, Grubb's tests was modified to assign penalty factors [6]. Detailed analysis can be obtained from [6]. Penalty factors [6] were calculated as follows:

$$\begin{aligned} P_n[k] &= \sum_{k' \in S_+[k]} \left(o_n^+[k'-1] + o_n^-[k']\right) \\ &\quad + \sum_{k' \in S_-[k]} \left(o_n^-[k'-1] + o_n^+[k']\right) \end{aligned} \tag{13}$$

where

$$o_n^-[k'] = \begin{cases} \frac{-(e_n[k'] - \mu_a^*[k'])}{\sigma_a^*[k']} & e_n[k'] < \mu_a^*[k'] \\ 0 & \text{Otherwise} \end{cases} \tag{14}$$

$$o_n^+[k'] = \begin{cases} \frac{e_n[k'] - \mu_a^*[k']}{\sigma_a^*[k']} & e_n[k'] > \mu_a^*[k'] \\ 0 & \text{Otherwise} \end{cases} \tag{15}$$

where $\mu_a^*[k']$ and $\sigma_a^*[k']$ are adjusted bi-weight estimates of mean and standard deviation calculated from equation (7) and (10) respectively. $S_+[k]$ and $S_-[k]$ are sets of iterations such that $\Delta\mu_a^*[k'] = \mu_a^*[k] - \mu_a^*[k-1]$ is positive and negative in those corresponding iterations respectively.

New outlier factors are defined based on above penalty factors as follows:

$$\bar{o}_n[k] = \frac{P_n[k] - \mu_P^*[k]}{\sigma_P^*[k]} \tag{16}$$

where $\mu_P^*[k]$: Bi-weight location for $P_n[k]$
$\sigma_P^*[k]$: Bi-weight scale estimates for $P_n[k]$

C. Boxplot Method

In boxplot method, data is arranged in ascending order. In our case, data is energy values in decibels. Then lower and upper threshold are calculated as follows:

$$Q_{lower} = Q_1 - 1.5Q_{intqrt} \tag{17}$$

$$Q_{upper} = Q_3 + 1.5Q_{intqrt} \tag{18}$$

where Q_{lower} and Q_{upper} represent lower and upper threshold respectively. Q_1 is first quartile, Q_3 is third quartile and Q_{intqrt} is $Q_3 - Q_1$ i.e. interquartile range. There is uncertainty about the most appropriate multiplier that to be used in boxplot method [14]. We have taken multiplier as 1.5.

D. Comparison of tests

Figure 1 shows receiver operating characteristic (ROC) curve for always YES malicious user attack when reported energy of always YES malicious user is 20 dB higher than that of normal user. It can be seen that Dixon's test performs better than that of Grubb's modified tests and boxplot test. When probability of false alarm fixed to 0.02, probability of detection for Dixon's test, Grubb Method 1, Grubb method 2 and boxplot is 0.9172, 0.8758, 0.9086 and 0.815 respectively. Between two methods of Grubb's test, second method gives better performance than that of the first method as expected because of more robust calculation by assigning penalty factors [6]. The worst performance of boxplot test can be explained as follows. Boxplot test detects multiple malicious users. In our case it detects 3-4 malicious users out of 20 users even though in simulation setup we assumed the presence of only one malicious user. This removes 3-4 normal users from cooperation which degrades the performance of cooperative spectrum sensing.

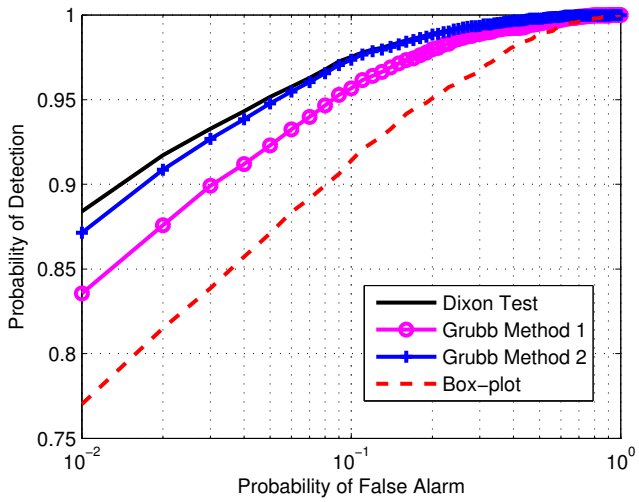

Fig. 1. Probability of detection versus probability of false alarm for average normal SNR = 0 dB for always YES malicious user

Figure 2 shows ROC curve performance for the case of always NO attack, when always NO malicious user reports energy lower than 20 dB than that of normal user. It shows similar trend in the performance curve as in the always YES attack. Dixon's test again outperforms Grubb's tests and boxplot test.

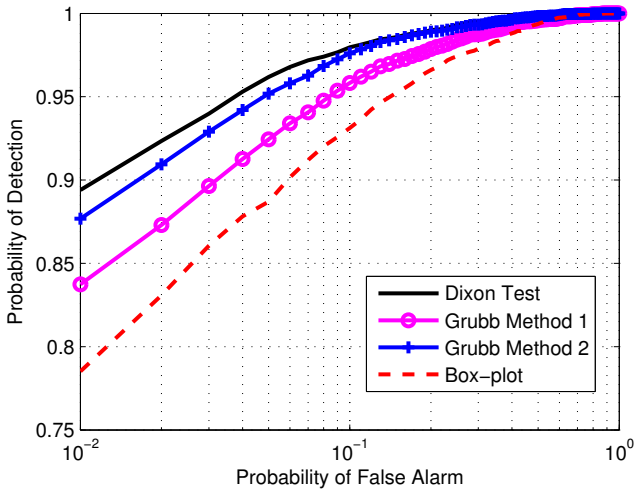

Fig. 2. Probability of detection versus probability of false alarm for average normal SNR = 0 dB for always NO malicious user

Figure 3 shows ROC curve performance for the case of confusing SSDF attacks. In this case, we have assumed that the malicious user randomly switches its reported energy between 20dB lower and 20 dB higher than that of the normal users. For this case also, Dixon's test gives better performance than Grubb's tests and boxplot test.

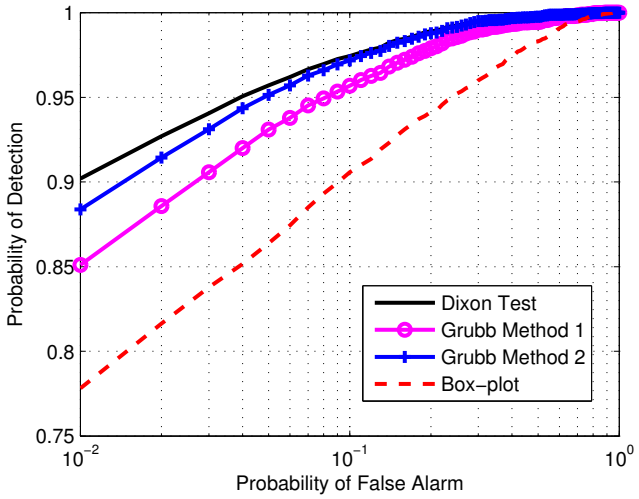

Fig. 3. Probability of detection versus probability of false alarm for average normal SNR = 0 dB for malicious user with random reporting

E. Limitations of Dixon's Test

Figure 4 shows the performance of Dixon's test when there are two malicious users present and compares it with the case when there is only one malicious user. We have considered the case of always YES malicious users. Since Dixon's test is applicable for detecting single malicious user, we can see that Dixon's test for detecting single malicious user performs better than detecting two malicious users. We also notice from the simulations that for the case of presence of one malicious user when we do not apply any malicious user detection technique, it is performing even better than the perfect removal of single malicious user case. This is because in this case, we have considered always YES attack where malicious user's energy is higher than normal user.

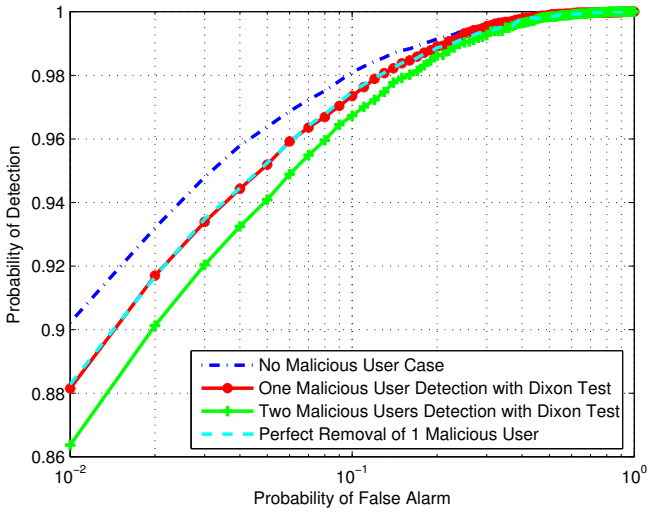

Fig. 4. Probability of detection versus probability of false alarm for average normal SNR = 0 dB for no, one and two malicious users for Dixon's test

Dixon's test cannot be repetitively applied for detection of more than one malicious users. We explain this with the help of an example. If we consider the case of three malicious users all employing always YES attack, i.e., they are all reporting high primary user energy. Let's assume that these three energy values reported by malicious users are almost equal. Then we can see from equation (3) for the case where N lies between 14 and 20, numerator becomes very small and $o_n[k]$ will be smaller than critical value. So even though there are three malicious users present representing always high value of primary user energy, it will not be detected by Dixon's test.

VI. Conclusion and Future Work

In this paper, we propose the use of Dixon's test based outlier based detection technique in cooperative spectrum sensing for cognitive radio to detect single malicious user. Monte-Carlo simulations are performed to compare Dixon's test with Grubb's based test and boxplot test. It is observed that Dixon's test performs better than Grubb's test and boxplot test. We also show the limitation of Dixon's test for the case of multiple malicious users. There is scope for improvement by finding more robust outlier detection techniques to detect multiple outliers.

References

[1] FCC, "Spectrum policy task force," *ET Docket 02-135*, Nov. 2002.

[2] J. Mitola and G. Q. Maguire, "Cognitive radio: Making software more personal," *IEEE Personal Communications*, vol. 6, pp. 13–18, Aug 1999.

[3] A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *Proc. IEEE Dynamic Spectrum Access Networks (DySPAN'05)*, (Baltimore, MD), pp. 131–136, Nov. 2005.

[4] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. 27th IEEE Conference on Computer Communications (INFOCOM'08)*, (Phoenix, AZ), pp. 1876–1884, April 2008.

[5] W. Wang, H. Li., Y. L. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Proc. 43rd Annual Conference on Information Sciences and Systems (CISS'09)*, (Baltimore, MD), pp. 130–134, March 2009.

[6] 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, pp. 2488–2497, 2010.

[7] H. V. 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. International Symposium on Wireless Communication Systems (ISWCS'10)*, (York, UK), pp. 966–970, Sep. 2010.

[8] R. B. Dean and W. Dixon, "Simplified statistics for small numbers of observations," *Analytical Chemistry*, vol. 23, no. 4, pp. 636–638, 1951.

[9] F. R.Yu, H. Tang, M. Huang, Z. Li, and P. C. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in *Proc. IEEE Military Communications Conference (MILCOM'09)*, (Boston, MA), pp. 1–7, Oct. 2009.

[10] V. Barnett and T. Lewis, *Outliers in Statistical Data*. New York, NY: John Wiley and Sons, 2nd ed., 1985.

[11] S. Verma and A. Quiroz-Ruiz, "Critical values for six dixon tests for outliers in normal samples up to sizes 100, and applications in science and engineering," *Revista Mexicana de Ciencias Geolgicas*, vol. 23, no. 2, pp. 133–161, 2006.

[12] F. Mosteller and J. Tukey, *Data Analysis and Regression : A Second Course in Statistics*. Reading: MA: Addison-Wesley, 1st ed., 1977.

[13] D. A. Lax, "Robust estimators of scale: finite-sample performance in log-tailed symmetric distributions," *J. American Statistical Association*, vol. 80, pp. 736–741, Sep. 1985.

[14] R. McGill, J. W. Tukey, and W. A. Larsen, "Variations of box plots," *The American Statistician*, vol. 32, pp. 12–16, Feb. 1978.