Robust Statistics Evidence Based Secure Cooperative Spectrum Sensing for Cognitive Radio Networks

Oluyomi Simpson and Yichuang Sun
School of Engineering and Computer Science
University of Hertfordshire, Hatfield, Hertfordshire, AL10 9AB, UK
o.simpson@herts.ac.uk and y.sun@herts.ac.uk

***Abstract*—Cognitive radio networks (CRNs), an assemble of smart schemes intended for permitting secondary users (SUs) to opportunistically access spectral bands vacant by primary user (PU), has been deliberated as a solution to improve spectrum utilization. Cooperative spectrum sensing (CSS) is a vital technology of CRN systems used to enhance the PU detection performance by exploiting SUs' spatial diversity, however CSS leads to spectrum sensing data falsification (SSDF), a new security threat in CR system. The SSDF by malicious users can lead to a decrease in CSS performance. In this work, we propose a CSS scheme in which the presence and absence hypotheses distribution of PU signal is estimated based on past sensing received energy data incorporating robust statistics, and the data fusion are performed according to an evidence based approach. Simulation results show that the proposed scheme can achieve a significant malicious user reduction due to the abnormality of the distribution of malicious users compared with that of other legitimate users. Furthermore, the performance of our data fusion scheme is improved by supplemented nodes' credibility weight.**

Keywords—Security, Robust Statistics, Evidence, Cooperative Spectrum Sensing, Cognitive Radio

I. INTRODUCTION

Cognitive Radio Networks (CRNs) provides a promising solution to reliable and time-efficient spectrum utilization by mitigating the spectrum scarcity issues created by the requirement for wireless bandwidth growing significantly due to the explosive growth of wireless devices [1]. It enables primary user (PU) networks to share their spectrum with the secondary users (SUs), on condition that that the SU's transmission does not affect the PU's performance adversely. Notwithstanding, CRNs have been found to be susceptible to external malicious threats, due to the broadcast nature of the PU-SU cooperation transmission techniques which may allow for a malicious eavesdropper to acquire the transmission information of Pus [1]. The ability to sense accurately the presence of PU is of the absolute importance of CRNs. In situations where individual SU sensing is shadowed by severe multipath fading and shadowing effects, the SU may not reliably detect the PU signal and access the channel when there is a PU signal present leading to interference of the licensed PU [1, 2]. To overcome this hidden terminal problem and increase the spectrum sensing credibility, cooperative spectrum sensing (CSS) has been studied in [1, 3]. In CSS, each sensing result from multiple SU are sent and fused at a data fusion centre (FC).

On the other hand, the flexibility of CRNs system brings about susceptibilities that may allow an attacker to masquerade as a SU leading to a spectrum sensing data falsification (SSDF) attack [4]. In SSDF attacks, malicious SUs forward falsify local sensing results to the FC to mislead the universal decision. The SSDF attack may knowingly impair the CSS process and may lead to either reduction in the spectrum utilization or extreme interference on the PU network. Conversely, some authentic SUs may appear like attackers because of their bad sensing performance caused by either the hiding terminal problem, a noisy reporting channel, or a faulty sensor.

In recent research [2, 5], cooperative SU techniques did not consider the SU's sensing credibility. Malicious SUs therefore maybe selected for cooperation in these schemes, which degrades the detection performance and the system performance. Some SSDF attack detection algorithms have been proposed to detect malicious SUs in CSS [6], however, the problem in the CRN with SSDF attack is still an open issue. In [4], SSDF in CSS was solved via a trust-based system; however, this technique required prior knowledge of the PU signal. These requirements are incongruous when applying to high mobile CRN, and to such systems in which the information of the PU is not entirely known. In [6], an algorithm to detect and isolate outliers was proposed. The SUs were tested for normality in this algorithm by comparing their sensing results. If the sensing results of a SU was too far from the reports of other SUs they are considered malicious. The limitations of this work were that some of the reports from legitimate unintentionally misbehaving SUs would be secluded if they were not near the sensing results from neighboring SUs.

In this work, in order to deal with the SSDF attack and incent SUs to increase their sensing credibility a robust statistics evidence based CSS technique that incorporates statistical approximation of the distributions for both the hypotheses of all SUs based on their previous sensing data is proposed. The main contributions of this paper are listed as follows:

- Firstly, realized parameters are used for the testing of malicious users as well as the calculation of necessary information for data fusion by means of an improved evidence based D-S theory taking into consideration the unintentionally misbehaving SUs.
- Secondly, the proposed scheme takes advantage of an appropriate method of data fusion as well as benefit of robust statistics for outlier testing based on two separately estimated distribution, can operate without prior knowledge of the primary systems, even in the case of a very bad circumstance where numerous attacks from malicious users occur.

- Thirdly, a credibility evaluation stage from the past performance of each node by a counting rule is added to our scheme to improve cooperative gain of data fusion and the efficiency of malicious user detection.

The proposed scheme is evaluated by simulation. Simulation results presented demonstrate that the robustness of the CSS CRN with SSDF attack can be enriched. Explicitly, malicious SUs with small sensing credibility are allocated with few resources and fewer opportunities to take part in CSS.

This paper is organized as follows: Section II presents the system model. Section III presents the robust statistics evidence based secure CSS for CRNs. Critical parameters which simultaneously enable both the powerful malicious user resistance and the high gain for the data fusion scheme are presented in section IV. In Section V, the eavesdropper user detection algorithm is presented. Section VI, presents the simulation results with detailed analysis and finally Section VII, provides concluding remarks.

II. SYSTEM MODEL

The system model scheme considered for a robust statistics evidence based secure CSS for CRNs is shown in Figure 1. Each SU performs a local sensing process under different channel conditions such as shadowing and multi-path fading and subsequently reports the sensing data to the FC. The universal decision based on the occupation of the PU signal is made at the FC. It is assumed that the CSS CRN is in an adversarial environment which means that a malicious SU known as an eavesdropper user (EU) can carry out an SSDF attack.

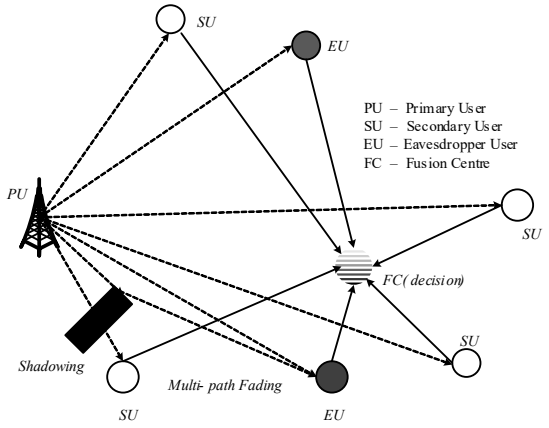

Figure 1. Cooperative spectrum sensing system model:

A. Spectrum Sensing at Primary Users

Single SUs carry out local spectrum sensing in a cooperative manner for detecting the PU signal. Local sensing is effectively a binary hypotheses testing predicament. Comparing the various algorithms for spectrum sensing, energy detection has been established to be the least complex detection scheme that decreases overhead, and is rapidly able to detect the PU signal, even without prior knowledge of the PU signal [7]. For local spectrum sensing we consider energy detection, To measure the value of a received power in a practical frequency band in time domain, a band pass filter (BPF) is applied to the received PU signal at the SUs and the power of the signal samples is subsequently measured. The decision statistic is an estimation of the received signal power which is given at each SU by the sensing matrix:

$$y_E = \sum_{i=1}^{N} |y_i|^2 \tag{1}$$

where y_i is the i-th sample of received signal and $N = 2TW$, where T and W are correspondent to detection time and signal bandwidth in Hz, respectively. It was proved in [8] that the probability density function (PDF) of the received PUs signal energy at an SU y_E , is a Chi-square distribution such that

$$f(y_E) = \begin{cases} \chi_N^2, & H_0 \\ \chi_N^2(N\gamma), & H_1 \end{cases} \tag{2}$$

where H_0 and H_1 are the hypotheses of indicating a vacant channel and occupied channel of the PU's signal, respectively, χ_N^2 is the central Chi-square distribution with N degree of freedom, and $\chi_N^2(N\gamma)$ is a non-central Chi-square distribution with N degree of freedom and a non-centrality parameter $N\gamma$. γ is the SNR of the PU signal at the SUs. In the absence of knowledge of the PU signal, when the number of required samples N is relatively large, y_E can be approximated as a Gaussian random variable under both hypotheses H_0 and H_1, with mean μ_1 , μ_0 and variance σ_1^2 , σ_0^2 , respectively, such that [7]:

$$\begin{cases} \mu_0 = N, & \sigma_0^2 = 2N \\ \mu_1 = N(\gamma+1), & \sigma_1^2 = 2N(2\gamma+1) \end{cases} \tag{3}$$

where the γ is a constant in a non-fading additive white Gaussian noise (AWGN) environment. Though, in a fading channel scenario, the SNR γ is a random variable [7].

To improve detection credibility of a CRN, a CSS scheme is considered as an alternative of a single SU as shown in Figure 1. Each SUs conduct local spectrum sensing by applying an energy detector to measure the PU's signal energy in each sensing frame. Subsequently after the spectrum sensing process, each SU computes its own local detection and the decision along with a corresponding credibility denoted by *crd* are then forwarded to the FC, where a universal decision is made. The whole CSS process can be grouped into two stages:

- SUs local sensing
- FC universal decision.

III. EVIDENCE BASED COPERATIVE SPECTRUM SENSING

Individual SUs forward their received signal power measurement to a FC where the universal sensing decision is computed. A robust statistics evidence based secure CSS scheme as shown in figure 2 is considered for increasing security and CSS gain.

A. Basic Probability Assignment (BPA) Estimation in CSS

In be able to apply the DS theory of evidence to make a universal decision, a frame of discernment denoted by Ω is defined as $\{H_1, H_0, \Omega\}$, where Ω denotes either hypotheses is true. Once each sensing period is completed, each SU will estimate its self-assessed decision, which is equivalent to the basic probability assignment (BPA) assignment for the two hypotheses H_0 and H_1, respectively. The DS fusion rule is commutative and associative hence, an appropriate BPA function is a cumulative distribution function (CDF) represented as [9, 10]:

$$H_0 : m_i\left(y_{E_i} \mid H_0\right) = \int_{y=y_{E_i}}^{\infty} \frac{1}{\sqrt{2\pi\sigma_{0i}^{\,2}}} \exp\left(-\frac{\left(y-\mu_{0i}\right)^2}{2\sigma_{0i}^{\,2}}\right) dy \quad (4)$$

$$H_1 : m_i\left(y_{E_i} \mid H_1\right) = \int_{y=-\infty}^{y_{E_i}} \frac{1}{\sqrt{2\pi\sigma_{1i}^{\,2}}} \exp\left(-\frac{\left(y-\mu_{1i}\right)^2}{2\sigma_{1i}^{\,2}}\right) dy \quad (5)$$

where $m(.)$ is equivalent to $Crd(.)$ $m_i\left(y_{E_i}\middle|H_0\right)$ and $m_i\left(y_{E_i}\middle|H_1\right)$ are the BPAs of hypothesis H_0 and H_1 of the i-th SU, respectively. By means of these functions, the BPA of hypotheses H_0 and H_1 are distinctive for each test statistics value y_{E_i} and differ in such a way that the bigger y_{E_i} is the bigger $m_i\left(y_{E_i}\middle|H_1\right)$ and the reduced $m_i\left(y_{E_i}\middle|H_0\right)$ are and vice versa [9]. The credibility from individual SUs and uncertainty are subject to the following constraint [11]:

$$m_i(H_1) + m_i(H_0) + m_i(\Omega) = 1 \quad (6)$$

B. BPA Modification

To modify the BPA using the credibility association calculation, the weight w_i of the i-th SU is evaluated by normalizing the SU credibility $crd_i(n)$:

$$w_i(n) = \frac{crd_i(n)}{\max_i(crd_i(n))} \quad (7)$$

C. DS Rule of Combination: Universal Decision

According to DS theory of evidence, the combination of the averaged BPA can be obtained by [12]:

$$m(H_0) = \bar{m}_1 \oplus \bar{m}_2 \oplus \ldots \oplus \bar{m}_n(H_0) = \frac{\sum_{A_1 \cap A_2 \cap \ldots A_n = H_0} \prod_{i=1}^{n} \bar{m}_i(A_i)}{1-K} \quad (8)$$

$$m(H_1) = \bar{m}_1 \oplus \bar{m}_2 \oplus \ldots \oplus \bar{m}_n(H_1) = \frac{\sum_{A_1 \cap A_2 \cap \ldots A_n = H_1} \prod_{i=1}^{n} \bar{m}_i(A_i)}{1-K} \quad (9)$$

where

$$k = \sum_{A_1 \cap A_2 \cap \ldots A_n = \varnothing} \prod_{i=1}^{n} \bar{m}_i(A_i) \quad (10)$$

The universal decision calculated at the FC is given by:

$$H_1 : m(H_1) > m(H_0) \quad (11)$$

$$H_0 : m(H_0) > m(H_1), \quad (12)$$

IV. Robust Statistics Evidence Based Secure CSS: Criteon Update

For a secure and non-complexity CSS CRN, the proposed combination scheme only requires the energy detection data from the SUs. No prior knowledge about the PU signal is necessary. The proposed algorithm can take advantage of combination of the "D-S theory fusion rule" as well as the use of outlier resistance of robust statistical analysis. Hence, the criterion updating process plays a significant role in the proposed algorithm. This process is responsible for obtaining critical specifications which concurrently enable both the powerful malicious EU counteraction and the improved gain at the FC.

A. Source Evaluation

In comparison with the local decision, the universal decision at the FC is consistently more credible in CSS. Hence, the universal decision can be employed as an overseer for the estimation of the SUs by means of a weight factor.

In the case that the local decision does not contradicts the universal decision, it is assumed that the local decision is

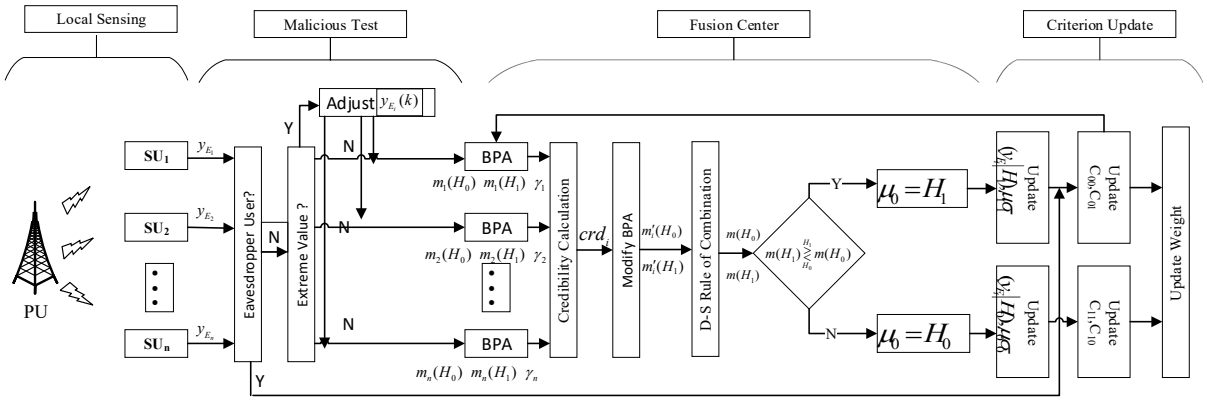

Figure 2. Robust statistics evidence based secure CSS for CRNs scheme.

accurate. Alternatively, in the case the local decision and the universal decision do not match, the local decision is incorrect. By computing the local and universal decisions the SUs can be exactly estimate. For the *i*-th SU at the *d*-th time, where the present decision state is represented by $C_i(d)$, which occurs in the states presented in Table I:

TABLE I

State	Universal decision	Local Decision
C_{00}	H_0	H_0
C_{01}	H_0	H_1
C_{10}	H_1	H_0
C_{11}	H_1	H_1

The accumulative state $P_i(n)$ of *n* detection time slot is given by:

$$\begin{aligned} P_i(n) &= \sum_{k=1}^{n} C_i(d) \\ &= n_{00_i}(n)C_{00} + n_{01_i}(n)C_{01} + n_{10_i}(n)C_{10} + n_{11_i}(n)C_{11} \end{aligned} \tag{13}$$

where $n_{00_i}(n)$, $n_{01_i}(n)$, $n_{10_i}(n)$ and $n_{11_i}(n)$ represent the times that state C_{00}, C_{01}, C_{10} and C_{11} have occurred over *n* time slot, respectively. A static window length over the observed data is considered.

$$P_i(n) = \sum_{d=n-Q+1}^{n} C_i(d) \tag{14}$$

where Q is the window length of the observation.

The credibility of an SU ought to have increased when it has robust performance. Subliminally, such an increased SU performance is the terminal that concurrently has together a low false alarm rate and a low missed detection rate. Accordingly, the credibility of each SU is given by the product of the complementary missed detection rate and complementary false alarm rate, as follow:

$$crd_i = (1 - P_{md})(1 - P_f) \tag{15}$$

where P_{md} and P_f represent the missed detection rate and false alarm rate, respectively. From (16) and (15) the credibility of the SUs as can be estimated by:

$$crd_i(n) = \frac{n_{00_i}(n)}{n_{00_i}(n) + n_{01_i}(n)} \times \frac{n_{11_i}(n)}{n_{11_i}(n) + n_{10_i}(n)} \tag{16}$$

From (17), the credibility of SUs can be realised by a non complex computing rule from their previous performance.

B. Hypothesis distribution criterion estimation

Hypotheses H_0 and H_1 can be estimated from the PU received signal at the SU, as presented in section II. Nevertheless, in such a situation, as with our system model where there can be various SSDF attacks by malicious EUs, to improve security the hypothesis distribution criterion is estimated based on previous SU sensing results. To exploit the advantages of the evidence based scheme and to concurrently enhance robust security sensing capability without any prior PU signal knowledge, the mean and variance estimation of H_0 and H_1 are made from existing sensing results using robust statistics. It is vital to accurate estimate the distribution of H_0 and H_1, improved accuracy permits increased performance and malicious EU counteraction for the proposed evidence based scheme.

In comparison with the local decision, the universal decision at the FC is consistently more credible in CSS. Therefore, the measured energy result at individual SUs after one combination interval will be allocated to data sets $\{y_{E_i} \mid H_0\}$ or $\{y_{E_i} \mid H_1\}$ corresponding to H_0 and H_1 of the universal decision.

C. Hubber's Robust Statistical Process

The next stage is the estimation of the criterion of H_0 and H_1 by Hubber's robust statistics [13], which uses the SUs data for precisely estimating the mean μ and variance σ of the distribution. At this step, we progressively transform the data by a repetitive process called winsorization as shown in the following stages.

Stage I: Fix initial parameter μ and σ

$$\begin{cases} \mu^{(0)} = MED(X) \\ \sigma^{(0)} = R \cdot MAD(X) \end{cases} \tag{17}$$

where $MED(X)$ is the sample median, $MAD(X)$ represents the median of *n* distances and *R* is a constant factor (1.4826) modifying the resulting robust value to the corresponding normal distribution.

Stage II: Test and modify outlier information
Unlike in [4] where uncertain data is removed robust statics is used:

$$\tilde{X} = \begin{cases} \mu^{(0)} - 1.7\sigma^{(0)} \ \ if \ \ \mu^{(0)} - 1.7\sigma^{(0)} > X_i \\ \mu^{(0)} + 1.7\sigma^{(0)} \ \ if \ \ \mu^{(0)} + 1.7\sigma^{(0)} > X_i \\ X_i \qquad\qquad\qquad elsewhere \end{cases} \tag{18}$$

where 1.7 is the multiplier for the winsorization.

Stage III: Compute an improved estimation of the mean as:

$$\mu^{(1)} = mean(\tilde{X}_i) \tag{19}$$

Compute an improved estimation of the standard deviation as:

$$\sigma^{(1)} = 1.14 stdev(\tilde{X}_i) \tag{20}$$

where the factor 1.14 is calculated from the normal distribution.

Stage IV: reiterate stage II and III, after *i* iterations, the algorithm converges to an acceptable degree of precision when the results are not modified in stage II. The resulting values are the robust statistical estimates mean $\mu^{(i)}$ and standard deviation $\sigma^{(i)}$.

Furthermore, as in our system model, a fixed length window Q of observation sensing results for estimating distribution parameters is considered. Therefore, the criterion $\{\hat{\mu}_{0i}, \hat{\sigma}_{0i}\}$ and $\{\hat{\mu}_{1i}, \hat{\sigma}_{1i}\}$ are estimated from $\{y_{E_i}(1+L-Q),..., y_{E_i}(L) | H_1\}$ and $\{y_{E_i}(1+L-G),..., y_{E_i}(G) | H_0\}$, respectively, where L is the length of $\{y_{E_i} | H_0\}$ and G is the length of $\{y_{E_i} | H_1\}$.

Therefore, H_0 and H_1 of individual SUs can be estimated with regards to its previous sensing data and also its previous performance evaluation.

V. Eavesdropper User detection

Two types of malicious EU are considered. Firstly, a "consistent malicious" user which is characterized into two modes as follows:

- **Mode I**: "constantly-yes" EU
- **Mode II** "constantly-no" EU.

A "constantly-yes" EU will continually inform the presence of a PU and a "constantly-no" EU will continuously report the absence of the PU signal. A "constantly-yes" EU improves the probability of false alarm P_f while the "constantly-no" EU reduces the probability of detection P_d.

Secondly, an attack type termed as the "constantly-inverse" EU attacker is considered. The foremost tenacity of this EU is to fatally break down the CSS CRN process by reporting the reverse of the SU local spectrum sensing results. In this case, the EC may produce sporadic dangerous false results that will significantly disturb the performance of the CSS CRN in the course of those specific sensing intervals, on the other hand will give accurate results the rest of the time. This type is designated as the "extreme false" malicious node.

A. Consistent malicious node test

A consistent malicious EU can be detected by the following conditions:

Condition 1: $\varepsilon_1 > |\hat{\mu}_{1i} - \hat{\mu}_{0i}|$

Condition 2: $\hat{\mu}_{1i} < \hat{\mu}_{0i}$

Condition 3: $\varepsilon_2 > \hat{\sigma}_{1i}$ or $\varepsilon_2 > \hat{\sigma}_{0i}$

Condition 4: $\varepsilon_3 < |\hat{\mu}_{0i} - N|$

where ε_1, ε_2 and ε_3 are detection thresholds.

Condition 1 is used for detecting "consistent malicious" EC that generate false sensing results from either H_0 or H_1. A "constantly-yes" or "constantly-no" EU will contain a very insignificant difference between the two hypotheses means and deviations since their data sets $\{y_{E_i} | H_0\}$ and $\{y_{E_i} | H_1\}$ are calculated from H_0 or H_1 distribution or conceivably even from a constant value. If an SU has a distance which when compared to a minimum tolerable value between two mean values of two hypotheses is smaller, it will be classified as a "consistent malicious" EU. The hypothetical lowest distance of two mean values is given as ε_1 and can be calculated from (3) as

$$\varepsilon_1 = (\mu_1 - \mu_0)_{\min} = N\gamma_{\min} \tag{21}$$

Condition 2 is employed for removing the "constantly-inverse" EU attacker, which has a mean result estimation of hypothesis of H_1 that is lesser than that of H_0 because its results are reversed to the local spectrum sensing values.

Condition 3 is used for quick testing and for identifying a "consistent malicious" EC that produces wrong constant values. ε_2 measures the least allowable result of estimated variance for H_0 or H_1. Subliminally, it is fixed to twenty times smaller than the theoretical σ_0 value in (3) and therefore ε_2 is given as:

$$\varepsilon_2 = \frac{\sigma_0}{20} = \frac{\sqrt{2N}}{20} \tag{22}$$

Condition 4 is used to detect the "constantly-yes" EU attacker that produces a huge result for H_0 or H_1. It also have a fast computation time when compared to condition 1 is because all SUs have the same detection time and signal bandwidth meaning they have equal mean value for H_0 The ε_3 is the maximum acceptable range around the theoretical result of estimation mean for H_0. The EU attacker will be detached from data fusion at the test sensing interval if it goes above one of the earlier conditions.

B. Extreme malicious test

To test for "extreme malicious" EU, As a substitute of discounting the results in making the final decision, for the "extreme false" cases, a simple test condition is employed to modify as follows:

$$\tilde{y}_{E_i} = \begin{cases} \hat{\mu}_{0i} - 3\hat{\sigma}_{0i} \ \ if \ \ \hat{\mu}_{0i} - 3\hat{\sigma}_{0i} > y_{E_i} \\ \hat{\mu}_{1i} - 3\hat{\sigma}_{1i} \ \ if \ \ \hat{\mu}_{1i} - 3\hat{\sigma}_{1i} > y_{E_i} \\ y_{E_i} \qquad\qquad elsewhere. \end{cases} \tag{23}$$

The EC result will far within the interval $\{\hat{\mu}_{0i} - 3\hat{\sigma}_{0i}, \hat{\mu}_{1i} - 3\hat{\sigma}_{1i}\}$. The sensing results not inside the interval will pushed to the boundary, and used for the BPA evaluation. To accurately minimize the negative effect, the risky false results will be modified so the smaller value becomes the larger BPA and vice versa. Thus, the weight in subsection III.B, the BPA of $\tilde{y}_{E_i}$ is weighted via w_{E_i}, and given by:

$$w_{E_i} = \begin{cases} \dfrac{3\hat{\sigma}_{0i}}{\hat{\mu}_{0i} - y_{E_i}} \ \ if \ \ \hat{\mu}_{0i} - 3\hat{\sigma}_{0i} > y_{E_i} \\ \dfrac{3\hat{\sigma}_{1i}}{y_{E_i} - \hat{\mu}_{1i}} \ \ if \ \ \hat{\mu}_{1i} - 3\hat{\sigma}_{1i} < y_{E_i} \\ 1 \qquad\qquad elsewhere. \end{cases} \tag{24}$$

VI. SIMULATION RESULTSAND ANLAYSIS

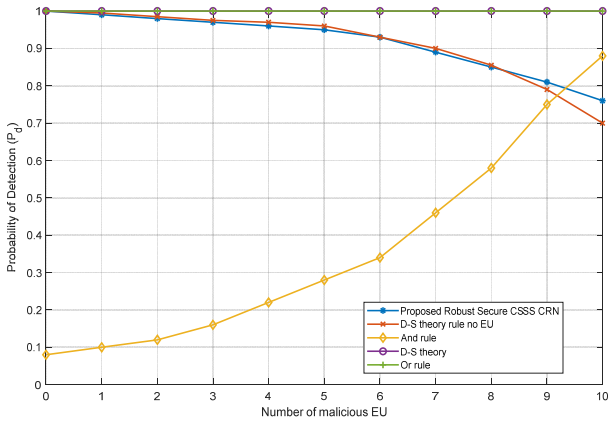

Figure 3. Probability of detection vs. number of "constantly-yes" malicious EU.

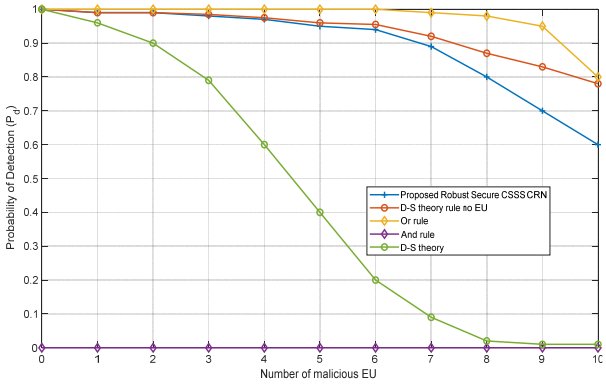

Figure 4. Probability of detection vs. number of "constantly-no" malicious EU.

In this section we evaluate the performance of the proposed robust statistics evidence based secure CSS for CRNs. Simulation results are shown to compare the proposed approach with other related approaches based on the receiver operating characteristic (ROC) in relation to number of malicious EU. The effects of different parameters on the proposed algorithm were examined. For the simulation in this paper, the PU network is assumed to be a DVB-T2 signal [14], the bandwidth of the PU signal is 10 MHz and modulation type is 4-PSK. The average occupancy rate for the PU is set to 50%, i.e. the probability of presence and absence of the PU signal is fixed to an equal probability (0.5), respectively. The simulation is based on the Monte Carlo method in MATLAB. An AWGN channels is assumed.

Figure 3 presents "constantly-yes" malicious EC in our proposed CSS scheme. Each "constantly-yes" EU arbitrarily creates a big value derived only from a high Signal to Noise Ratio (SNR) distribution of H_1. It can be seen that the malicious EC identification algorithm performs well. The P_d of the "Or rule" is one, implying that the "Or rule" is intensely affected by the "constantly-yes" malicious EU. For the "And rule", the performance is improved when compared to that of the "Or rule", the "And rule", P_d is slightly higher. Taking

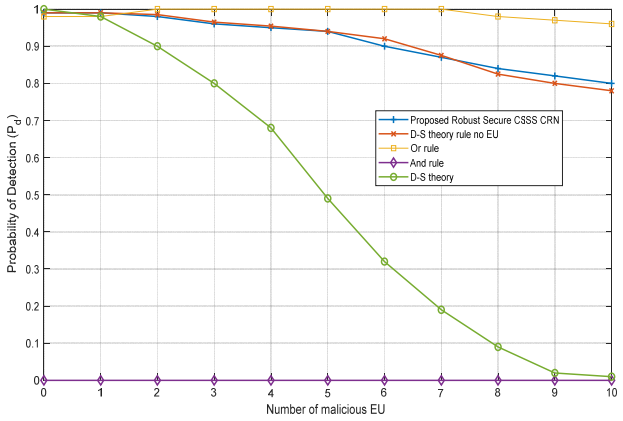

Figure 5. Probability of detection vs. number of "constantly-inverse" malicious EU.

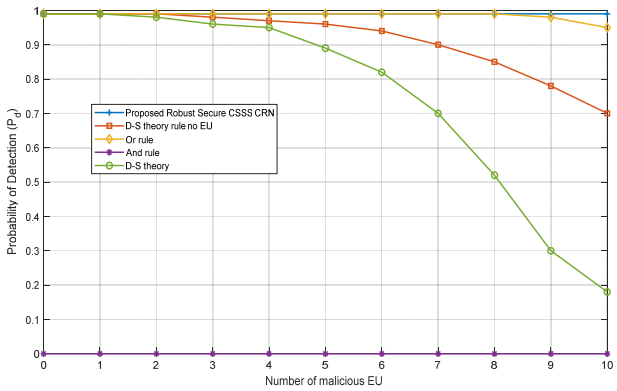

Figure 6. Probability of detection vs. number of "Extreme malicious" malicious EU.

the "D-S theory combination rule" into account which the BPAs are acquired from both the theoretical hypotheses distribution, the P_d is constantly roughly one due to the effect of "constantly-yes" EU. The D-S theory combination rule" without malicious nodes is used as a comparison boundary of data fusion. In the proposed scheme, the results can achieve a combination boundary until 87% SUs are malicious nodes.

Figure 4 presents the P_d vs the number of "constantly-no" malicious EU in in our proposed CSS scheme. With this mailicous EU, the data fusions, with no malicious EU identification capability, receives an inverse effect when compared to the constantly-yes" malicious EU.The P_d of the "And rule" is equal to zero and that of "D-S theory combination rule" decreases when the number of "constantly-no" EUs increases. For "Or rule", the P_d performance is increased and improved upon as the number of malicious EU increases. As with the aforementioned case, when the number of EUs increased to roughly eight per ten users, the proposed algorithm's P_d for this case are also close to the boundary combination obtained by the "D-S theory combination rule" without the malicious EU.

Figure 5 shows the P_d vs the number of "constantly-inverse" malicious EU in in our proposed CSS scheme. Comparable to preceding cases, other data fusions that have not identified malicious node capabilities show a decreased performance while the proposed algorithm with a technique of detection for malicious EU accomplish the same performance of data combination boundary of "D-S theory fusion rule" without malicious nodes, even when the number of EUs is increased up to nine per ten nodes.

Figure 6 denotes the P_d vs the number of" Extreme malicious" malicious EU in in our proposed CSS scheme. The result of the EUs producing an extreme false value uninterruptedly for 10 times within each 100 sensing intervals is presented. The obtained results confirm that the proposed technique can not only efficiently detect but can moreover remove the effect of such malicious EUs and provide an improved performance even when compared to that of the "D-S theory combination rule" without malicious user.

VII. Conclusion

A robust statistics evidence based secure CSS for CRNs was proposed, evaluated, simulated and analyzed in this paper. The algorithm is based on previous SUs sensing data. Prior knowledge of the PU signal is not required. The scheme can utilized both the advantage of the "D-S theory combination rule" alongside an enhanced weighting algorithm. A robust statistical algorithm is deployed for SSDF attacks, where malicious SUs forward falsify local sensing results to the FC to mislead the universal decision. Simulation results and analysis presented shown that the technique performs adequately even when 75 percent of users are malicious and even when the channel among the SUs and the PU is affected by multipath fading or deep shadowing environment

References

[1] J. Wu, Y. Yu, T. Song, and J. Hu, "Sequential 0/1 for Cooperative Spectrum Sensing in the Presence of Strategic Byzantine Attack," *IEEE Wireless Communications Letters,* vol. 8, no. 2, pp. 500-503, 2019.

[2] J. Kim and J. P. Choi, "Sensing Coverage-Based Cooperative Spectrum Detection in Cognitive Radio Networks," *IEEE Sensors Journal,* vol. 19, no. 13, pp. 5325-5332, 2019.

[3] X. Chen, H.-H. Chen, and W. Meng, "Cooperative Communications for Cognitive Radio Networks — From Theory to Applications," *IEEE Communications Surveys & Tutorials,* vol. 16, no. 3, pp. 1180-1192, 2014.

[4] I. Ngomane, M. Velempini, and S. V. Dlamini, "Trust-Based System to Defend Against the Spectrum Sensing Data Falsification Attack in Cognitive Radio Ad Hoc Network," in *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, 2018, pp. 1-5.

[5] M. Zhang and Y. Liu, "Secure Beamforming for Untrusted MISO Cognitive Radio Networks," *IEEE Transactions on Wireless Communications,* vol. 17, no. 7, pp. 4861-4872, 2018.

[6] H. Chen, M. Zhou, L. Xie, and J. Li, "Cooperative Spectrum Sensing With M-Ary Quantized Data in Cognitive Radio Networks Under SSDF Attacks," *IEEE Transactions on Wireless Communications,* vol. 16, no. 8, pp. 5244-5257, 2017.

[7] F. F. Digham, M. S. Alouini, and M. K. Simon, "On the Energy Detection of Unknown Signals Over Fading Channels," *IEEE Transactions on Communications,* vol. 55, no. 1, pp. 21-24, January 2007.

[8] H. Urkowitz, "Energy Detection of a Random Process in Colored Gaussian Noise," *IEEE Transactions on Aerospace and Electronic Systems,* vol. AES-5, no. 2, pp. 156-162, March 1969.

[9] N. T. Nhan and K. Insoo, "Evidence-Theory-Based Cooperative Spectrum Sensing With Efficient Quantization Method in Cognitive Radio," *IEEE Transactions on Vehicular Technology,* vol. 60, no. 1, pp. 185-195, October 2011.

[10] K. Nguyen, S. Denman, S. Sridharan, and C. Fookes, "Score-Level Multibiometric Fusion Based on Dempster–Shafer Theory Incorporating Uncertainty Factors," *IEEE Transactions on Human-Machine Systems,* vol. 45, no. 1, pp. 132-140, October 2015.

[11] Q. Peng, K. Zeng, J. Wang, and S. Li, "A Distributed Spectrum Sensing Scheme Based on Credibility and Evidence Theory in Cognitive Radio Context," presented at the IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications, 11-14 Sept. 2006, Septmber 2006.

[12] G. Shafer, *A Mathematical Theory of Evidence*. Princeton, NJ: Princeton Univ. Press, 1976.

[13] P. J. Huber, *Robust Statistics*. John Wiley & Sons, Inc., Chichester 1981.

[14] European Telecommunications Standards Institute, "Digital Video Broadcasting (DVB); Frame structure channel coding and modulation for a second generation digital terrestrial television broadcasting system (DVB-T2)," September 2009.