Research Article

An SETM Algorithm for Combating SSDF Attack in Cognitive Radio Networks

S. Tephillah and J. Martin Leo Manickam

1Department of Electronics and Communication, St. Joseph’s Institute of Technology, St. Joseph’s Group of Institutions, Anna University, Chennai, Tamil Nadu, India
2Department of Electronics and Communication, St. Joseph’s College of Engineering, St. Joseph’s Group of Institutions, Anna University, Chennai, Tamil Nadu, India

Correspondence should be addressed to S. Tephillah; tephisam@gmail.com

Received 23 January 2020; Revised 13 April 2020; Accepted 4 June 2020; Published 21 July 2020

Academic Editor: Daniel G. Costa

Copyright © 2020 S. Tephillah and J. Martin Leo Manickam. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Security is a pending challenge in cooperative spectrum sensing (CSS) as it employs a common channel and a controller. Spectrum sensing data falsification (SSDF) attacks are challenging as different types of attackers use them. To address this issue, the sifting and evaluation trust management algorithm (SETM) is proposed. The necessity of computing the trust for all the secondary users (SUs) is eliminated based on the use of the first phase of the algorithm. The second phase is executed to differentiate the random attacker and the genuine SUs. This reduces the computation and overhead costs. Simulations and complexity analyses have been performed to prove the efficiency and appropriateness of the proposed algorithm for combating SSDF attacks.

1. Introduction

Exploitation of a licensed spectrum by unlicensed users without interference is a prodigy for wireless communications. Cognitive radio technology (CR) has introduced the issue of the utilisation of the spectrum based on the process of dynamic spectrum access (DSA). The CR is anticipated to be a vital technology for fifth-generation (5G) communications. The CR technology enables the unlicensed or secondary users (SUs) to access opportunistically the prescribed channels of the licensed or primary users (PUs) without interference. DSA involves spectral sensing, analysis, and allocation by sensing the white spaces (holes) in the frequency bands. Cooperative spectrum sensing (CSS) increases the accuracy of the PU occupancy detection by collecting sensing information from the SUs [1]. However, CSS paves the way for malicious attacks that modify the sensing reports given that the channel used for reporting is common.

The alteration of the sensing report by malicious users (MU) is the spectrum data falsification attack (SSDF) that typically occurs at the data link layer. The SSDF attack can be classified into five classes [2]: (a) always yes: in the absence or presence of the PU, the malicious user always reports the presence of a PU to divest the genuine SU; (b) always no: to induce interference, the malicious user always reports the absence of the PU even in its presence; (c) alternator: the malicious user always conflicts the genuine SUs detection output; (d) selfish: at times, the malicious attacker does not participate in the sensing process to save energy; and (e) contingent: report data falsely in a random manner. They play smartly such that identification becomes difficult.

2. Methodology

Trust is a firm belief in reliability. Thus, the genuine nature of the user (SU) can be quantified by measuring the degree of trust. However, the evaluation of trust for all the SUs may increase the complexity with respect to time and space. To address this particular issue in trust-based security systems, a new algorithm is proposed in this study referred to as sifting and evaluation trust management (SETM). The algorithm comprises two phases: (i) sifting and (ii) evaluation. In the first phase, identification of MUs subject to the first four categories is achieved by screening the sensing reports of the SUs with
the fusion centre (FC) outputs over a period of time. Thus, most of the MUs are filtered in this phase. The second phase aids in the identification of contingent attackers from the genuine SUs by evaluating the trust of different categories, such as past events, registries, requites, and reliabilities. Additionally, the efficiency and appropriateness of SETM are proven using simulations and complexity analyses.

The rest of the study is organised as follows: Section 3 introduces related works pertaining to trust-based systems. Section 4 provides insights on the system model, the spectrum sensing process, and the identification of MUs. Section 5 provides the proposed SETM algorithm. Finally, the results, discussion, and conclusion sections are outlined in Sections 6 and 7.

3. Related Works

Chen et al. [3] have proposed a reputation-based cooperative spectrum sensing model in which the reputation is set by the FC for each SU based on the sensing results. The SU is then weighted according to the reputation value. However, the reputation degree is not adaptable. Kar et al. [4] proposed multi-weighted spectrum sensing model in which the reputation is set by the SUs. Chen et al. [3] have proposed a reputation-based cooperative spectrum sensing model in which the reputation is set by the SUs.

Singh et al. [7] for CSS–SSDF attacks. The methodology exploits the data stored in the FC to identify the MUs. The prior knowledge of the user is needed in the implementation of the method. Furthermore, an adaptive reputation evaluation for individual and collaborative SSDF attackers based on a linear weighted combination scheme has been proposed by Wang et al. [8]. Consistency measures are executed to detect outliers. Relying on a weighted scheme may not prove appropriate in random attack scenarios. Also, Wang et al. [9] have proposed a combatting technique for SSDF by calculating the suspicious level and consistency level of trust for the all the SUs that participate in the sensing. But detection of all types of SSDF attackers cannot be resolved by just measuring the consistency levels.

4. System Model

Let “K” be the number of SUs who sense the spectrum over a time slot “T,” and “M” be the number of MUs pertaining to all the attacking strategies. The system model is depicted in Figure 1. Additionally, the FC is considered to be the most powerful user with considerable potential and accumulated data to identify all types of SSDF attackers. The channel conditions are assumed to be perfect for transmission (control channels), and all the SUs use the energy detection technique to detect the presence and absence of the PU. Furthermore, the path loss is neglected given that the area of coverage of the CR system is assumed to be small [10].

4.1. Spectrum Sensing of SU. The presence and absence of PUs are determined by the FC based on hypothesis testing (statistical testing). Mathematically, it can be expressed according to Equations (1) and (2) as,

\[ H_0 : Y_\delta(k) = \omega_i(K) \]

\[ H_1 : Y_\delta(k) = \omega_i(K) + h_3P(K) \]

where \( Y_\delta(k) \) is the received signal, and \( \omega_i(K) \) is the white Gaussian noise function for “K” SUs (K = 1, 2, 3, …, S). It is also considered that the noise has a zero mean and a variance \( \sigma \). \( P(K) \) is the \( K^\text{th} \) sample of the primary user signal detected by the SUs. \( H_0 \) represents the absenteeism of PU, and \( H_1 \) represents the existence of PU. Mathematically, Equation (3) represents the hypothesis.

\[ H_0 : \sum_{i=0}^{K} \delta_i \leq k \]

\[ H_1 : \sum_{i=0}^{K} \delta_i \geq k \]
bandwidth and implementation. Each of the SUs sends a binary output to the FC indicating the presence (binary “1”) or absence (binary “0”) for the formulation of a final decision. FC decides in favour of the SUs if K out of S users vote for the same output. The FC calculates the received signal based on Equation (4) [11].

Mathematically, the FCO is the final decision by the FC based on the consideration of the K out of N rule. The details listed in different rows of the table show the output of “SU” SUs at different timeslots, and the details listed in different columns show the sensing results of each SU.

### 5. The SETM Algorithm

#### 5.1. Sifting Phase

In this study, the SETM algorithm is presented to identify all the aforementioned types of MUs, where S is the symbol used to denote sifting, and E is used to denote evaluation. As the name indicates, sifting means filtering. Therefore, by analysing the columns of the reports of each SU, it is possible to infer the nature of the malicious behaviours of the MUs. For example, by analysing the first column of the Table 1 for time slot t0 to t8, it can be inferred that the SU belongs to the MU class “always yes,” if all the columns have the sensing report set to binary “1.” After “K” timeslots, this phase can be continued to the next timeslot (t8 + 1 to ts9) during which the MUs can even change their behaviours from MU1 to MU5, wherein i and j ∈ {1, 2, 3, 4, 5}. Thus, during the sifting phase, the necessity of calculating the trust values is neglected. This reduces the computational complexity. The following algorithm performs the sifting phase of the SETM method.

#### 5.2. Evaluation Phase

This evaluation process is conducted only for SUs categorised as random or genuine. The evaluation of trust is based on the weighted average of four different types of trust. Past events include trust (TP), participation trust (TP), participation trust (TP), participation trust (TP), and reliability trust (TP). The FCO is the final decision by the FC based on the consideration of the K out of N rule. The details listed in different rows of the table show the output of “SU” SUs at different timeslots, and the details listed in different columns show the sensing results of each SU.

#### 4.2. Identification of MU’s

Trust is a time-varying parameter expressing the assured reliance on someone’s ability, strength, and truth. Thus, the study of past events of the SU would reveal their worthiness. In our proposed system, the trust analysis is pursued and completed in two phases, namely, the sifting and evaluation phases. In the sifting phase, the worthiness of the SU is observed based on the recording of past SU events over a period of time. Consider a sliding time window from 0 to T comprising equal timeslots denoted by t8,j, t8,1, ..., t8,k. During each timeslot, the spectrum sensing is completed by each SU. Let the sensing output of each SU be (SU1, SU2, ..., SU8), and let the time of the observation range from t8,0 to t8,k, where k ∈ 2n + 1, where n is an integer. The FC accumulates all the reports in a record table, as shown in Table 1.

| Time slots/SU’s | SU1 | SU2 | SU3 | SU4 | SU5 | SU6 | SU7 | SU8 | FCO |
|-----------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| t8,0            | 1   | 0   | 1   | 1   | 0   | 1   | 1   | 1   | 1   |
| t8,1            | 1   | 1   | 0   | X   | 0   | 0   | 0   | 1   | 0   |
| t8,2            | 1   | 0   | 1   | 1   | 0   | 1   | 0   | X   | 1   |
| ...             |     |     |     |     |     |     |     |     |     |
| t8,k            | 1   | 1   | 0   | 1   | 0   | 0   | 0   | 0   | 0   |
where \( T(ts(j-1)) \) is the initial trust or cumulative trust of the previous time slots. \( SU_j^r(ts_j) \) represents the spectrum sensing report of \( SU_j \) over the timeslot \( ts_j \). \( FCO(ts_j) \) represents the final decision of the FC at time slot \( j \).

(ii) Registry trust \((T_{RG})\) is a measure of the activity of the SU as selfish SUs may skip their participation in spectrum sensing to save their energy. The participation trust can be evaluated by considering the ratio of the total number of active participations \((W(i))\) to the total number of time slots. Mathematically,

\[
T_{RGi} = \frac{W(i)}{k} \tag{11}
\]

(iii) Requisite trust: this provides the reward to the genuine SU or punishment to the malicious SU. Equation (12) describes the evaluation of the requisite trust as,

\[
T_{RTi} = \frac{F(i)}{k} \tag{12}
\]

where \( F(i) \) represents the number of falsely reported decisions by the \( SU_i \), and \( k \) is the number of timeslots.

(iv) Reliability trust: reliability is the quality of being trustworthy on a consistent basis. Thus, the estimation of this trust will enable us to know to what extent the SU is consistently genuine. Additionally, the reliability of MU would change often. Consistency can be measured by summing up the squared deviation of each value in any distribution divided by the number of values in the distribution. Equation (13) lists the expression used to quantify consistency.

\[
T_{RIj} = 1 - \sqrt{\frac{\sum (T_{ai} - T_{aj})^2}{k-1}} \tag{13}
\]

where \( T_{ai} = T(i)/T(i) + F(i) + 2 \) and \( T_{aj} = \sum T_{ai}/k \). \( T_{ai} \) is the trust considered based on the beta distribution, and \( T_{aj} \) is the summation of all the individual trusts considered over the time slot \( k \).

After the calculation of all the above trust indices, the weighted combination of trust is estimated based on Equation (14)

\[
T_{tot} = T_{PEi}W_1 + T_{Pi}W_2 + T_{RTi}W_3 + T_{RIi}W_4 \tag{14}
\]

\[
T_{tot} = T_{PEi}w_1 + T_{Pi}w_2 + T_{RT}w_3 + T_{RI}w_4, \text{ where } w_1, w_2, w_3 \text{ and } w_4 \text{ are the weights, and } \sum w_j = 1.
\]

6. Results and Discussions

The efficacy and expediency of a trust management system can be evaluated based on performance augmentation parameters, such as the low-false alarm and low misdetection rates, low overhead, and high-sensing performance. The complexity analysis would also prove the appropriateness of the proposed system [13].
6.1. Performance Augmentation. In this section, the efficacy and expediency of the proposed SETM algorithm have been discussed based on the consideration of the variation of the probability of false alarms in conjunction with the trust value and threshold. The simulations were executed initially with ten SUs with MATLAB (2014, Math Works, Natick, MA, USA). The SUs were assumed to be randomly cited around the PU whose spectrum had to be sensed. The simulation parameters for evaluation are given in Table 2.

During the sifting phase of the SETM algorithm, the sensing reports from all the SUs are given to the FCO within the prescribed time slot. The FCO identifies the different types of MUs just by analysing the sensing outputs of SUs over the given time slot with its final decision. The FCO sorts the SU as always yes MU, if the sensed output of the SU is “1” for all the time slots. The SU is sorted as always no MU, if the sensed output of the SU is “0” for the prescribed timeslot. Further, if the SU sensing output alternates for every time slot, then it is sorted as alternator MU and for any of the sensing time the SU does not sense—then the SU is sorted as selfish MU. However, if any SU is not sorted as MU during the sifting phase, then to prove the honesty of SU, the evaluation phase is conducted. During this phase, five types of trust such as past events, registries, requisite, reliabilities, and cumulative trusts are evaluated. Depending on the value of the cumulative trust, the SU is classified as a random MU or as a genuine SU.

Table 3 provides an insight on the variation of past event, requisite, reliability, and cumulative trusts, with a noted increase in the percentage of malicious users. The registry trust is considered to be “1” on the assumption that the SU provides all the sensing results to the FCO within the given time slot. Further, the cumulative trust is calculated by considering the weights \( w_1 = 0.1, w_2 = 0.2, w_3 = 0.3, \) and \( w_4 = 0.4 \), as described by Equation (14). Specifically, when a SU reports falsely only once (10%), the cumulative trust value is equal to 1.67, when SU reports falsely more than once (20% to 90%) the cumulative trust decreases from the value of 1.434 to 0.264. The inference is that as the maliciousness of a SU increases, the trust value decreases. Thus, the cumulative trust can be used as a performance metric to prove whether the SU is genuine or malicious. Figure 2 shows the variation of trust as a function of the percentage of malicious behaviour in each SU, based on the use of the SETM algorithm. Specifically, for every 10% increase in malicious behavior of a SU, there is a decrease of approximately 15% in the value of cumulative trust.

Theoretically, the threshold for finding the MU is calculated by setting the variance to unity \((\nu = 1)\) and the probability of the false alarm to 0.1 \((P_f = 0.1)\) in Equation (6). The theoretical threshold value is 1.57; signifying that for the trust value of above 1.57, the SU is genuine and below that it is malicious. From Table 2, it is clear that the SU having a trust value of 1.67 and above, it is considered as genuine SU else malicious. Thus, the evaluated threshold and theoretical threshold more or less satisfies the criteria of finding the MU. Figure 3 shows the variation of the threshold as a function of the probability of the false alarm \( (P_f) \). As the probability of the false alarm increases, the threshold value decreases.

The variations of different values of trust at different timeslots are shown in Figures 4, 5, 6, and 7. The variation of past event trusts \( (T_{PE}) \) at different timeslots for different types of SUs is shown in Figure 4. The genuine SUs exhibit a \( T_{PE} \) variation between the upper and lower thresholds, where the upper threshold indicates that the respective SU is 100% genuine (having all sensing outputs correct in the previous time slots) and lower threshold indicates that the SU is 90% genuine (has reported one sensing result falsely). Thus, the past event trust of any SU fluctuates between the two thresholds (10.5 to 8.5) cannot be malicious. Another inference is that a selfish SU (MU) exhibits a trust variation between alternate timeslots. As a selfish SU does not participate in all the sensing rounds for a particular interval of time for saving its resources, the \( T_{PE} \) never reaches the upper threshold value. Also, the trust value \( (T_{PE}) \) for a random attacker (MU) lies at values which are much lower than the lower threshold, specifically below 8.5. Thus, just by evaluating \( T_{PE} \), the three types of SUs can be identified.

### Algorithm 2

Input: \( T(ts(j - 1)), SU_i'(ts_j), FCO(ts_j), W(i), k, F(i), w_1 \) to \( w_4 \)

Output: Cumulative trust calculation and inference about SU

(1) Calculate the past events trust using equation (10)
(2) Calculate the participation trust using equation (11)
(3) Calculate the requisite trust using equation (12)
(4) Calculate the reliability trust using equation (13)
(5) Find the cumulative Trust \( (T_{tot}) \) using equation (14)
(6) If \( T_{tot} > \tau \), then SU \( i = \) Genuine else SU \( i = \) Random malicious attacker

### Table 2: Simulation parameters.

| Parameter                  | Depiction                  |
|----------------------------|----------------------------|
| No. of SUs                 | 10                         |
| Timing window              | \((t_{s0}, \ldots, t_{s9})\)|
| Participation count \((K)\)| 10                         |
| Percentage of false reports| 0.1 to 0.9                 |
| Weights for cumulative trust| \(w_1 = 0.1, w_2 = 0.2, w_3 = 0.3, w_4 = 0.4\) |
The identification of selfish users is also based on the calculation of the requisite trust and registry trust. Figure 5 shows the variation of the requisite trust ($T_{RQ}$) as a function of time for a genuine SU and a selfish SU. $T_{RQ}$ increases consistently with respect to time. However, the $T_{RQ}$ of selfish users does not yield a consistent increase. Furthermore, there is a dip of about 10% in the value of the $T_{RQ}$ compared with the genuine SU response. Figure 6 shows the variation of the registry trust ($T_{RG}$) with the time slot. As time increases, the $T_{RG}$ value for the genuine SU stays at a constant value, but for

### Table 3: Evaluation of all types of trusts with malicious behaviour of SU.

| Sl. No | Percentage of malicious behaviour | Past event trust | Registry trust | Requisite trust | Reliability trust | Cumulative trust |
|--------|----------------------------------|------------------|----------------|----------------|------------------|------------------|
| 1.     | 10%                              | 8.5              | 1              | 0.9            | 0.90             | 1.676            |
| 2.     | 20%                              | 6.5              | 1              | 0.8            | 0.86             | 1.434            |
| 3.     | 30%                              | 4.5              | 1              | 0.7            | 0.84             | 1.196            |
| 4.     | 40%                              | 2.5              | 1              | 0.6            | 0.83             | 0.958            |
| 5.     | 50%                              | 0.5              | 1              | 0.5            | 0.83             | 0.716            |
| 6.     | 60%                              | -1.5             | 1              | 0.4            | 0.83             | 0.502            |
| 7.     | 70%                              | -3.5             | 1              | 0.3            | 0.84             | 0.176            |
| 8.     | 80%                              | -5.5             | 1              | 0.2            | 0.86             | -0.046           |
| 9.     | 90%                              | -7.5             | 1              | 0.1            | 0.90             | -0.264           |

Figure 2: Plot of cumulative trust with respect to malicious behaviour of SU. The dots represent the value of cumulative trust for 10 to 70% variation in malicious behaviour.

Figure 3: Plot of threshold with respect to probability of false alarm. The dots represent the value of threshold for 0.1 to 0.5 variation of $P_{fa}$. 
the selfish SU, the TRG varies with a maximum dip of about 33% from the constant value of genuine SU.

Reliability measures the consistency of a node. Figure 7 shows the variation of the reliability trust ($T_{RL}$) as a function of time. For the MU, the TRL never reaches the value of unity, but for genuine SU, the value stays at a constant value for most of the time. Specifically, the $T_{RL}$ value for genuine SU never falls below 90%, but for MU, the maximum value is only 86%. Thus, by comparing $T_{RL}$, the genuine SU and MU can be identified.

6.2. Complexity Analysis. This section investigates the appropriateness of the proposed SETM algorithm in terms of message, storage, time, and computational complexities.

(i) Message complexity (MC): defined as the number of spectrum sensing outputs required by the FC to formulate the final decision. The majority rule is used by the FC to calculate the final output. The number of SUs considered for the timeslot $t_{s0}, \cdots, t_{s9}$ is “S.” Therefore, the message complexity would be

$$MC = S$$

(ii) Storage complexity (SC): defined as the amount of memory needed for the storage of the trust value. Let “r” be the size of the register in the register table of the FC for storing the trust value. With regard to

![Figure 4: Plot of variation of past event trust for genuine SU and selfish SU and MU with time.](image)

![Figure 5: Plot of requisite trust with respect to time for genuine and selfish SU.](image)
the SETM algorithm, only the trust values of random MU, selfish MU, and genuine SU, need to be stored. Thus, the total storage complexity would be \((S - M) (r)\), where \(M\) is the number of malicious users filtered in the first phase of the SETM algorithm

\[
SC = (S - M)(r)
\]  

(16)

(ii) Time complexity (TC): the timeslots needed by the FC to receive the spectrum sensed output of the SUs. Let \(t_{sam}\) be the predefined sampling period needed by the FC

\[
TC = t_{sam}
\]  

(17)

(iii) Computational complexity (CC): it is a measure that evaluates the maximum number of times the SETM is executed for the identification of malicious users. SETM has two phases: the first phase has a complexity of \(4 \times O(S) \sim O(S)\). The second phase also has a complexity of \(O(S)\), where \(S\) is the total number of SUs. \(O(S)\) represents the linear complexity

\[
CC = O(S)
\]  

(18)

Tables 4 and 5 give the parameters and complexity measured for the SETM algorithm. The message complexity is the same as the number of SUs.

The storage complexity is needed only for the genuine and random attacker SU, and not for other types of MU’s.
Institutions declare no competing interests.

extended by considering more than one PU.

overhead. As future work, the analysis of trusts can be
random attackers only need to be stored, thus lowering the
based system. Additionally, the trust values for genuine and
SUs. Thus, our method eliminates the need to evaluate the
This study are available within the article.

rithm evaluates the trust to di
algorithm was proposed to combat
SSDF attacks based on the identi
In this study, the SETM algorithm was proposed to combat
radio networks, “Wireless Personal Communications,” vol. 97, no. 2, pp. 2523–2540, 2017.

Thus, the storage requirement and overhead are minimised.
Further, the time complexity purely depends on the sampling
period of CR (few milliseconds). Also, the computation
complexity is the least complexity of any algorithm that is linear
complexity [14]. Thus, as the computational complexity is
minimum, the SETM algorithm proves to be a low-
reckoning trust management system.

7. Conclusion

In this study, the SETM algorithm was proposed to combat
SSDF attacks based on the identification of all types of mali-
cious users that contribute to these attacks. In the first phase,
the four types of SSDF attackers (always yes, always no, selfish,
and alternator) were determined without the need to
evaluate all the trusts. The second phase of the SETM algo-
rithm evaluates the trust to differentiate random and genuine
SUs. Thus, our method eliminates the need to evaluate the
trusts for all SUs, thereby providing a low-reckoning trust-
based system. Additionally, the trust values for genuine and
random attackers only need to be stored, thus lowering the
overhead. As future work, the analysis of trusts can be
extended by considering more than one PU.

Data Availability

The authors confirm that the data supporting the findings of
this study are available within the article.

Conflicts of Interest

The authors of this manuscript and St. Joseph’s Group of
Institutions declare no competing interests.

References

[1] J. Wang and I. Chen, “Trust-based data fusion mechanism
design in cognitive radio networks,” in 2014 IEEE Conference
on Communications and Network Security, pp. 53–59, San
Francisco, CA, 2014.

[2] J. Bennaceur, H. Idoudi, and L. A. Saidane, “A trust game
model for the cognitive radio networks,” in 2016 International
Conference on Performance Evaluation and Modeling in Wired
and Wireless Networks (PEMWN), pp. 1–5, Paris, 2016.

[3] H. Chen, X. Jin, and L. Xie, “Reputation-based collaborative
spectrum sensing algorithm in Cognitive Radio networks,” in
2009 IEEE 20th International Symposium on Personal, Indoor
and Mobile Radio Communications, pp. 582–587, Tokyo,
2009.

[4] S. Kar, S. Sethi, and R. K. Sahoo, “A Multi-factor Trust Man-
agement Scheme for Secure Spectrum Sensing in Cognitive
Radio Networks,” Wireless Personal Communications, vol. 97,
no. 2, pp. 2523–2540, 2017.

[5] J. Feng, M. Zhang, Y. Xiao, and H. Yue, “Securing Cooperative
Spectrum Sensing Against Collusive SSDF Attack using XOR
Distance Analysis in Cognitive Radio Networks,” Sensors,
vol. 18, no. 2, 2018.

[6] F. Zhao, S. Li, and J. Feng, “Securing Cooperative Spectrum
Sensing against DC-SSDF Attack Using Trust Fluctuation
Clustering Analysis in Cognitive Radio Networks,” Wireless
Communications and Mobile Computing, vol. 2019, Article
ID 3174304, 11 pages, 2019.

[7] W. N. Singh, N. Marchang, and A. Taggu, “Mitigating SSDF
attack using distance-based outlier approach in cognitive radio
networks,” International Journal of Ad Hoc and Ubiquitous
Computing (IIAUC), vol. 32, no. 2, pp. 119–132, 2019.

[8] R. Wan, L. Ding, N. Xiong, and X. Zhou, “Mitigation strategy
against spectrum-sensing data falsification attack in cognitive
radio sensor networks,” International Journal of Distributed
Sensor Networks, vol. 15, no. 9, 2019.

[9] W. Wang, H. Li, L. Sun, and Z. Han, “Securing Collaborative
Spectrum Sensing against Untrustworthy Secondary Users in
Cognitive Radio Networks,” EURASIP Journal on Advances
in Signal Processing, vol. 2010, no. 1, 2009.

[10] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, “Secure
Cooperative Sensing Techniques for Cognitive Radio Sys-
tems,” in 2008 IEEE International Conference on Communica-
tions, pp. 3406–3410, Beijing, 2008.

[11] D. Teguig, B. Scheers, and V. Le Nir, “Data fusion schemes for
cooperative spectrum sensing in cognitive radio networks,” in
2012 Military Communications and Information Systems Con-
ference (MCC), pp. 1–7, Gdansk, 2012.

[12] P. C. Sofotasios, M. Valkama, T. A. Tsiftsis, Y. A. Brychikov,
S. Freear, and G. K. Karagiannidis, “Analytic solutions to a
Marcum Q-function-based integral and application in energy
detection of unknown signals over multipath fading channels,”
in 2014 9th International Conference on Cognitive Radio Ori-
tered Wireless Networks and Communications (CROWN-
COM), pp. 260–265, Oulu, 2014.

[13] M. H. Ling, K.-L. A. Yau, and G. S. Poh, “Trust and reputation
management in cognitive radio networks: a survey,” Security
and Communication Networks, vol. 7, no. 11, pp. 2160–2179,
2014.

[14] https://introprogramming.info/english-intro-csharp-book/-
read-online/chapter-19-data-structures-and-algorithm-
complexity.