International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5737
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

Affirmed Crowd Sensor Selection based Cooperative Spectrum Sensing

[*1]D Raghunatha Rao, [2]T Jayachandra Prasad, [3]M N Giri Prasad
[*1]Assistant professor, SVR Engineering College, Ayyalur, Nandyal, Kurnool, Andhra Pradesh, JNTUA, Anantapuramu.
[*1]Email: raghudhayapule2000@gmail.com
[2]Principal, RGM College of Engineering and Technology, Nandyal, Kurnool, Andhra Pradesh, JNTUA, Anantapuramu
[2]Email: jp.talari@gmail.com
[3]Director of Admissions, JNTUA College of Engineering, Andhra Pradesh, JNTUA, Anantapuramu.
[3]Email: mahendragiri.1963@gmail.com
[*]Corresponding Author

Abstract: The Cooperative Spectrum sensing model is gaining importance among the cognitive radio network sharing groups. While the crowd-sensing model (technically the cooperative spectrum sensing) model has positive developments, one of the critical challenges plaguing the model is the false or manipulated crowd sensor data, which results in implications for the secondary user's network. Considering the efficacy of the spectrum sensing by crowd-sensing model, it is vital to address the issues of falsifications and manipulations, by focusing on the conditions of more accurate determination models. Concerning this, a method of avoiding falsified crowd sensors from the process of crowd sensors centric cooperative spectrum sensing has portrayed in this article. The proposal is a protocol that selects affirmed crowd sensor under diversified factors of the decision credibility about spectrum availability. An experimental study is a simulation approach that evincing the competency of the proposal compared to the other contemporary models available in recent literature.

Keywords: cooperative spectrum sensing, crowd sensor, cognitive radio users, error probability model, secondary users.

1 Introduction

Spectrum sensing is a key function of cognitive radio to prevent the harmful interference with licensed users and identify the available spectrum for improving the spectrum's utilization. However, detection performance in practice is often compromised with multipath fading, shadowing and receiver uncertainty issues. To mitigate the impact of these issues, cooperative spectrum sensing has been shown to be an effective method to improve the detection performance by exploiting spatial diversity. While cooperative gain such as improved detection performance and relaxed sensitivity requirement can be obtained, cooperative sensing can incur cooperation overhead. The overhead refers to any extra sensing time, delay, energy, and operations devoted to cooperative sensing and any performance degradation caused by cooperative sensing.

Increasing the consumption of wireless services is leading to more dense consumption of the spectrum space. Currently, across many global locations, there are stringent regulations of the spectrum utilization by the telecommunication departments, resulting in regulated usage of licensed spectrum for specific services by the primary users. Hardly there is any provision for the unlicensed services or secondary user services category.

Licensed spectrum is generally under-utilized in terms of temporal and spatial conditions. For addressing the conditions, the cognitive radio was proposed in the earlier studies as a solution to support the secondary users with utilization and license sharing scope [1]-[5]. While there is a distinct form of spectrum sensing models discussed in the literature, the model in terms of cooperative spectrum sensing [6]-[8] has depicted significant performance towards improving the ability and the scope of spectrum utilization.

The cooperative spectrum sensing model is profoundly abutting the secondary user identifying the spectrum bands available for sharing. The information about the available spectrum bands is provided by the cognitive radio users who have technically seen as the source of crowd sensors. The model of crowd sensor is about how a set of cognitive radio users collaborate and share the results of sensors among the secondary users, which will help the users take inform decisions about the spectrum band availability and usage. Every similarly low device in the crowd might contribute anomalous data, whether due to system failures or arbitrary malicious activity. This means that the present protection techniques outlined above are useless because of this. For example, if the "onion-peeling" technique inside this sensor filtering techniques is employed for dynamic spectrum access with crowd sensors, most of sensors would've been

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5737
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

filtered away and eventually few may survive. Although most sensors of the spectrum might supply anomalous data at any given time, it's possible that they'll all be given the same sensor rating if reputation is utilized in the sensor weighting methods.

Such modus operandi has potential scope for malicious practices among the compromised crowd sensors and manipulated sensing reports, thus resulting in authenticated data from the secondary user network or the affirmation from the primary users. The other key challenge that can be attributed to the conditions is the identification of the sensing reports that are forged, and the detection must be executed among the uncompromised sensing report conditions only.

Profoundly, the user's networks tend to avoid the cooperative neighbors as part of the crowd sensors, as usually, such neighbors provide false information regarding the availability of spectrum space for sharing.

1.1 Motivation

According to the Federal Communications Commission, the majority of assigned spectrum is inefficiently used by authorized primary users [9]. To maximize spectrum usage, unregistered secondary users should be granted opportunistic access to the spectrum [10]. Cognitive radio is a new technology that enables a unregistered secondary user (SU) to detect and efficiently utilise any valid spectrum that is available with authorized primary users (PU) at any given time. Cooperative spectrum sensing has recently attracted a great attention as a viable method for improving detection performance by leveraging spatial diversity via observations of spatially distributed secondary users [8]. Secondary users can collaborate to pool their sensing data and make a more accurate decision [11].

1.2 Problem Statement

However, Cooperative spectrum sensing assumes that secondary user's technically the low end personal spectrum sensors (such as smartphones, tablets, and in-vehicle sensors) cooperation is always fair enough, and thus leads to falsified final decision about spectrum allocation [12].

Cooperative spectrum sensing, on the other hand, presupposes that secondary users' collaboration with reduced initial spectrum sensors (such as smartphones, tablets, and in-vehicle sensors) is always fair, resulting in a false final spectrum allocation decision [12].

Fortunately, trust mechanisms can inhibit this erroneous spectrum allocation, and numerous efforts have been devoted to diversified trust mechanism studies [13-18]. When generating a final conclusion, they evaluate whether a secondary user is honest or not based on his prior actions and provide minimal weights to the data from unreliable secondary users. Attackers frequently adapt their techniques to escape detection of trust mechanisms. Each secondary user in cooperative spectrum sensing has two roles: one as a spectrum status seeker who uses sensing data and another as a spectrum status provider who contributes sensing data. Currently, seeker feedback on the spectrum condition of PUs after cooperative spectrum sensing is regarded as reliable. In this situation, attackers might first provide false feedback data to disrupt the trust process, then counterfeit sensing data with maximum sensing trust. As a result, the fair exchange of spectrum availability information by secondary users acting as spectrum status providers and the fair exchange of provider reputation by secondary users acting as spectrum status seekers is critical.

This paper addressed the problem of forged crowd sensor cooperation (FCCS) in cooperative spectrum sensing and tainted secondary user feedback (CFSU) to crowd sensors, and proposed an Affirmed Crowd Sensor Selection based Cooperative Spectrum Sensing that defends both FCCS and CFSU practises in cooperative spectrum sensing. The following are the paper's main contributions:

- The Review of related research portrayed an in-depth investigation on cooperative spectrum sensing, scope of FCCS and CFSU, and contemporary defense mechanisms
- The model has portrayed a set of metrics to defend FCCS and CFSU to improve fair cooperation of crowd sensors towards cooperative spectrum sensing as well as to achieve fair feedback exchange by secondary users.

2 Related Work

Many studies have focused on the process of improving the spectrum sensing accuracy by focusing on distinct solutions of cooperative spectrum sensing. Irrespective of the developments, there are certain challenges in the system wherein the multiple secondary users can detect the decisions by reporting any compromised sensing or unreliable data reported by the network users' sensors. Considering such implications, it is essential to focus on designing a robust and cooperative sensing scheme in defending the malicious users.

Many of the studies have focused on such modalities [19] – [26]. The authors of the study [19] have proposed the solution as a reputation-based mechanism, wherein the issues of falsification of data based on the weightage of the sensing reports are the structure. Authors of a research study [20] have discussed the conditions of outlier detection schemes

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5737
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

that rely on filtering out the values which are extreme, whilst sensing the data. The other model proposed in [21] is about the conversion of the areas of interest into a grid form for identification and discarding of the outlier conditions. Another contemporary model [22] has discussed the option of abnormality detection as a scope, and in [23], the abnormality detection model has emphasized with a model of path-loss exponent over the signal propagation. The machine learning center approach for detection of the falsification is proposed in [24], wherein the initial trusted set of data has used for developing a classifier that has a subsequent impact on the detection of integrity and violations. In [25], the other model of the consensus-based scheme has proposed for controlling the data falsification conditions, wherein the cooperative decisions among the group have attained in a distributed manner. The authors of the study in [26] have proposed the solution as the total error probability model for evaluating the spectrum sensing accuracy. Also, the model discusses the usage of a weighted sensing framework. Some of the solutions proposed in the similar format are [27], [28] wherein the public-key schemes-based models have proposed for defending the conditions of malicious users' networks. However, the compromised feedback updates by secondary users haven't been addressed in these contributions [21]-[26].

The study [29] discusses the reputation-based mechanism for recognizing the malicious users and mitigation of its relative impact by using a comparative analysis of reputation values. Ambiguity region analysis in terms of double threshold energy detection constituting a hard combination process is observed in [30] wherein the emphasis is limited to improving the performance of spectrum sensing by avoiding malicious users. However the model is reactively analyzing the users towards their malicious practices. The other contemporary model is the usage of joint and instantaneous trustworthiness detection model deployment among the mobile detectors as soft combinations based on the reputation values to achieve secured crowd-sensing for cooperative spectrum [31]. Like the above model, in [32], a contemporary model of user clustering is proposed for the detection of malicious or compromised users. In [33], a novel-reputation centric cooperative spectrum sensing model, wherein the results of energy detection across participants have assessed using the combination of data available from secondary users in the network. In [34], another model has proposed wherein an innovative test constituting logical operator and majority voting rules for cooperative sensing is proposed for enhancing the performance of spectrum sensing. Nevertheless, the trustworthiness of the users performing the reputation updates of the cooperative secondary users is overlooked in these contributions [29], [31-33], which is critical constraint of the reputation based cooperative spectrum sensing mechanism. In [35], the authors developed a list of reliable users for mitigating the usage from malicious users, based on the statistics of true or false decision analysis. But such works contribute towards the detection of malicious users and towards improvising the performance of the spectrum sensing, based on hard or soft combination conditions.

2.1 Trust Mechanism

Many application scenarios, such as e-commerce [36], peer-to-peer file-sharing [37], crowd sensing [38], social networks [39], [40], [41] are becoming more reliant on the trust mechanism. The trust-mechanism furthermore plays a key role in CSS, such as 1) assisting FC in making reliable decisions, 2) encouraging honest behavior, and 3) discouraging attackers from participating. The following are some examples of trust mechanism studies: The authors of [13] suggested a trust-aware hybrid spectrum-sensing system that utilizes the beta reputation to build sensing trust. Zeng et al. suggested a credible CSS strategy for mitigating attacks those falsifies spectrum sensing with the help of trusted providers (secondary users) [14], and divide each provider's trustworthiness into three states. The authors of [15] quantify the reliability of providers in CSS throughout the cognition process and integrate this into the fusion of the sensing data in order to reduce the impact of assailants on final decision of spectrum sensing [16] updates the provider trust level based on his CSS behavior and uses it in the sensed allocation of spectrum. The authors of [17] use trust as a key attribute to penalize attackers who try to gain access across any unoccupied PU spectrum. In [18], the author suggested a trust management strategy to improve the evaluation of sensing trust by incorporating multiple decision factors, including 1) a history-based trust factor, which is a provider's trust level during spectrum sensing periods; 2) an active factor, which reflects a provider's level of activity in the spectrum sensing process; and 3) a leverage factor that is used as a reward for honest providers and also serves as Currently, the assessment of sensing trust is the focus of all these contemporary trust mechanism strategies.

The common feature is that a provider's sensing trust is determined by secondary user's past practices of data exchange about spectrums, and sensing data is given low weights for less honest providers when making a final decision.

To extract these current trust mechanism strategies for the common factor, a basic model of trust mechanism is described. Because CSU sensing data can be regarded as a

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5737
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

binary indicator, which can easily be classified as true or false sensing results. In this case, FC can use two indexes to set the CSUs' sensing trust value representing as the count of true sensing and the count of false sensing. The function, which uses binary input to evaluate trustworthiness, has recently become one of conventional strategies. It counts the true and false sensing of the user has engaged in before using probability functions to calculate the trusted sensing value [42], [43]. [44]

Reviewing the related works, the complexities pertaining to accuracy in the crowdsourcing schemes are evident, and despite that, some of the existing frameworks or solutions are addressing certain issues. Still, there is scope for improvisation inaccuracy of falsification detection and degree of agreement among the cognitive radio users network as crowd sensor group for cooperative spectrum sharing.

The contemporary model privacy-preserving truth discovery scheme in crowd sensing systems [45], [46], [47] is a competent model to discover the truth from the information shared by the crowd sensors. The portrayed method is generalized version, which can be adopted to perform cooperative spectrum sensing by crowd sensors. However, the method is evincing the accuracy towards truth identification from the information shared by the crowd sensors, the critical constraint evinced that the set of sensors compromised to enable the Credibility Entangling and Contrived Credibility.

To address these issues, the proposal of this manuscript endeavored to define an Affirmed Crowd Sensor Selection based Cooperative Spectrum Sensing, which proactively discards the crowd-sensor or crowd-sensor pool having malevolent crowd-sensors prone to share the falsified spectrum band information.

3 Methods and Materials

As stated in the block diagram of Affirmed Crowd Sensor Selection (ACSS) based Cooperative Spectrum Sensing shown in Figure 1, the model ACSS focus on various metrics to obtain reliable cooperation from crowd sensor about spectrum band status in cooperative spectrum sensing. The broad objective of the proposal is to adopt crowd sensors based on their fair cooperation index (fci) to perform spectrum sensing by secondary users. In this context, a secondary user seeks cooperation from crowd sensors to adopt an adequate spectrum band under the spectrum sensing process. After completion of the transmissions over the spectrum band that chose under cooperative spectrum sensing, the respective secondary user updates the fair cooperation index of the crowd sensor(s), which can be either positive, negative, or neutral. The overall framework critically handles two significant concerns about the cooperative spectrum sensing process. One is to avoid crowd-sensors (cognitive radio devices/users), who compromised and sharing falsified spectrum band sensing information. The other objective is selective acceptance of the updates to the fair-cooperation-index fci of corresponding crowd sensor(s). In contrast to these contemporary methods, the proposed model avoids the selective acceptance of updated fair cooperation index. To this, the proposal relies on the camouflage publishing strategy. Following are descriptions of the notations in Table 1.

Table 1: Descriptions of the notations and expressions used

(dfc)	Degree-of-fair-cooperation
$(dfcu)$	Degree-of-fair-cooperation-update
$(fcus)$	Fair-cooperation update support
$(ddfcu)$	Degree of Diversity in Fair-cooperation update
cs	Crowd-sensor
τ	Threshold
$cspc$	Count of the crowd sensor pools
ulu	Unique list of users
csp	Crowd sensor pools
$r\,csc$	Count of responses by crowd-sensor
(dsr)	Degree-of-spectrum-realization
(ftf)	Frequency-of-Transmission-Failures
$(dtfi)$	Degree-of-Transmission-Failure-Impact
$edfc$	Encoded version of the new Degree-of-fair-cooperation

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5737
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

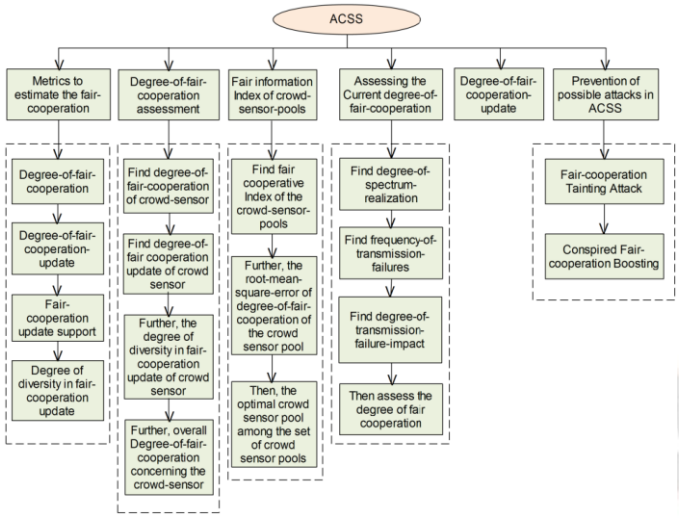

Figure 1: Block diagram representation of ACSS

3.1 Metrics to Estimate the Fair-cooperation

- Degree-of-fair-cooperation (dfc): The Degree-of-fair-cooperation of the crowd-sensor shall consider in the cooperative spectrum sensing process, which is neutral, negative, or positive that updates by the secondary user upon completion of the spectrum sensing carried under the recommendations of the corresponding crowd-sensor. Such an update performed by aggregating -1 for negative feedback, 1 for positive feedback, or 0 for neutral to the present Degree-of-fair-cooperation of the target crowd-sensor.
- Degree-of-fair-cooperation-update $(dfcu)$: It indicates the Degree-of-fair-cooperation-update that has taken place for a crowd-sensor, which indicates the number of times the Degree-of-fair-cooperation of the crowd-sensor has been updated during a period.
- Fair-cooperation update support $(fcus)$: This metric denotes the ratio of the Degree-of-fair-cooperation against the count of responses observed for the corresponding crowd-sensor.
- Degree of Diversity in Fair-cooperation update $(ddfcu)$: This metric denotes the ratio of unique crowd-sensors involved in Degree-of-fair-cooperation-update against the Degree-of-fair-cooperation-update of the crowd-sensor.

3.2 Degree-of-fair-cooperation Assessment

If the secondary-user isu indulges request broadcasting to crowd-sensors to select the fair spectrum band under cooperative spectrum sensing. All of the crowd-sensors those responded to secondary-user comprise aforesaid four key factors, and they are "Degree-of-fair-cooperation (dfc)", "Degree-of-fair-cooperation-update $(dfcu)$", "Fair-cooperation update support $(fcus)$", and "Degree of Diversity in Fair-cooperation-update $(ddfcu)$". The secondary-user prefers reliable crowd sensor(s), which have a high fair cooperation index that derived from the aforesaid factors shared by the crowd-sensors. The detailed description of the crowd-sensor selection follows.

Further, the integrity of the factors shared by the crowd-sensor cs shall assess by the secondary-user. In this regard, the secondary-user defines the signature from the fair index factors shared by the corresponding crowd-sensor, which is a hash-value. Further, verifies that the resultant hash is the same as the hash that published to the other secondary-users during the last fair-cooperation update process of the corresponding crowd-sensor cs. If the mismatch observed between the signatures (hash values), then ignores the crowd-sensor cs from the cooperative spectrum sensing.

Also, the Degree-of-fair-cooperation $dfc(cs_i)$ of crowd-sensor cs_i is a simple aggregation of the varied number of times incremented by 1, 0, or -1.

The overall ratio of Degree-of-fair-cooperation $\rho(cs_i)$ shall estimate as in (Eq 1):

$$\rho(cs_i) = \frac{dfc(cs_i)}{cspc(cs_i)} \quad \text{... (Eq 1)}$$

The ratio of Degree-of-fair-cooperation concerning the temporal threshold τ is in (Eq 2),

$$\rho^{\tau}(cs_i) = \frac{dfc^{\tau}(cs_i)}{cspc(cs_i)} \quad \text{... (Eq 2)}$$

Also, the Current Degree-of-fair-cooperation of the crowd-sensor cs_i shall evaluate as in (Eq 3):

$$cdfc(cs_i) = \frac{\rho^{\tau}(cs_i)}{\rho(cs_i)} \quad \text{... (Eq 3)}$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5737
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

$$\left.\begin{array}{l} if\ \left(cdfc(cs_i)>1\right) then \\ cdfc(cs_i)=1-\dfrac{1}{cdfc(cs_i)} \end{array}\right\}$$ ..... // concluding the normal form (between 0 and 1) of the value $cdfc(cs_i)$

The Degree-of-fair-cooperation-update ($dfcu$) shall calculate as shown in (Eq 4):

$$dfcu(cs_i)=1-\frac{1}{cspc(cs_i)} \quad \text{... (Eq 4)}$$

// $cspc(cs_i)$ the count of the crowd sensor pools having the crowd-sensor cs_i

The fair-cooperation-update-support ($fcus$) of the crowd-sensor cs_i shall evaluate as in (Eq 5)

$$fcus(cs_i)=\frac{cspc(cs_i)}{r\,\mathrm{csc}(cs_i)} \quad \text{... (Eq 5)}$$

// $r\,\mathrm{csc}(cs_i)$ denotes the count of responses by crowd-sensor cs_i such that (see Eq 6)

$$cspc(cs_i)\le r\,\mathrm{csc}(cs_i) \quad \text{... (Eq 6)}$$

Further, the degree of diversity in fair-cooperation update ($ddfcu$) shall estimate as in (Eq 7)

$$ddfcu(cs_i)=\frac{|ulu(cs_i)|}{cspc(cs_i)} \quad \text{... (Eq 7)}$$

// $ulu(cs_i)$ denotes the unique list of users involved in Degree-of-fair-cooperation update of the crowd-sensor cs_i and $|ulu(cs_i)|$ is the size of the corresponding list

Further, the overall Degree-of-fair-cooperation concerning the crowd-sensor cs_i can assess as shown in (Eq 8):

$$DFC(cs_i)=1-\left[cdfc(cs_i)\otimes dfcu(cs_i)\otimes fcus(cs_i)\otimes ddfcu(cs_i)\right] \quad \text{... (Eq 8)}$$

// the normalized value v of each metric falls in the range $0<v\le 1$. Hence, the absolute product of these metrics shall lesser value than the value of any of these metrics. In this regard, to obtain the fair-cooperation update, the resultant product of these metric values shall subtract from the 1.

3.3 Fair information Index of the crowd-Sensor-Pools

After secondary Users in CRN relies on multiple crowd sensors to seek the cooperation about spectrum band Sensing, In such case, the depicted method attains the fair cooperative Index of the crowd-sensor-pools, which has explored in this section.

For each crowd sensor pool $\{csp \exists csp \in CSP\}$ // CSP is set of crowd sensor pools found (see in Eq 9):

$$DFC(csp1)=\frac{\sum_{i=1}^{|csp|}\left\{DFC(cs_i)\exists cs_i\in\{csp\}\right\}}{|csp|} \quad \text{... (Eq 9)}$$

Further, the root-mean-square-error [42] of the Degree-of-fair-cooperation $DFC(csp)$ of the crowd sensor pool csp assesses as follows in (Eq 10):

$$edfc(csp)=\frac{1}{|csp|}\left(\sum_{i=1}^{|csp|}\sqrt{\left(DFC(csp)-DFC(cs_i)\right)^2}\right) \quad \text{... (Eq 10)}$$

// $|csp|$ denotes the count of crowd-sensors found in crowd sensor pool csp, $\{csp\}$ denotes the list of crowd-sensors used to establish the crowd sensor pool csp

In furtherance to the above process, the optimal crowd sensor pool among the set of crowd sensor pools CSP can be assessed as:

- The crowd sensor pools in CSP shall be sorted in the order of descending manner as per the $DFC(csp)$ value
- Set of crowd sensor pools that are with greater $DFC(csp)$ value than the threshold value ϖ shall be sorted
- Also, the crowd sensor pools discovered in crowd sensor pool request process that is having Degree-of-fair-cooperation $DFC(csp)$ more than the threshold value ϖ shall also be sorted

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5737
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

- Despite the fact that the degree of fair-cooperation for the crowd sensor pool is high, the deviation for the degree of fair-cooperation for crowd-sensor level has to be much lower, and thus the particular set of crowd sensor pools are again sorted in an ascending manner to their respective $edfc(csp)$.
- In the sequence, the utmost crowd sensor pool in the set of crowd sensor pools ordered in descending order of fair cooperation index shall be considered to perform optimal spectrum band sensing.

3.4 Assessing the Current Degree-of-fair-cooperation

- The metric Degree-of-spectrum-realization (dsr) represents 1,0, or -1, which is in regard to corresponding order of no transmission failures, transmission failures due to shared resources, or transmission failures due to malicious activity, terms of transmission failures due to unresponsive cognitive radio devices (users), spectrum band with shared resources, malevolent crowd-sensors, which are defined as:
- The metric Frequency-of-Transmission-Failures (ftf) denotes the values 1,0, or -1 in respective order of the ratio of egress transmissions against ingress transmissions is near to 1, less than or near to 0.5 due to shared resources, or less than 0.5 due to malevolent acts of the target crowd-sensor
- The metric Degree-of-Transmission-Failure-Impact $(dtfi)$ projected by 1,0, or -1, in respective order of events no external impact on transmission due to transmission failures, external impacts of the transmission failure observed due to shared resources, or the eternal impact of the transmission failures observed due to malevolent activity. Then the Degree-of-fair-cooperation assesses as shown in (Eq 11):

$$dfc = \begin{cases} \dfrac{dsr + ftf + dtfi}{\sqrt{(dsr + ftf + dtfi)^2}} & if\ (dsr + ftf + dtfi) \neq 0 \\ 0 & if\ (dsr + ftf + dtfi) \equiv 0 \end{cases}$$

... (Eq 11)

3.5 Degree-of-fair-cooperation-Update

The transmission process, which is finished in the selected crowd sensor pool csp_i, the secondary-user su shall update the Degree-of-fair-cooperation $dfc(cs_i) + dfc_{csp_i}(cs_i)$ (Here $dfc(cs_i)$ is actual Degree-of-fair-cooperation of the cs_i, $dfc_{csp_i}(cs_i)$ is Degree-of-fair-cooperation concluded in respective of the crowd sensor pool csp_i) of each crowd-sensor cs_i found in the corresponding crowd sensor pool. The present fair-cooperation of the crowd-sensor cs_i is incremented by 1, 0, or -1 in respective observation fair enough, not fair enough due to shared resources, or not fair enough due to suspected malicious activity. The Degree-of-fair-cooperation update is done as follows:

The secondary-user su shares the Degree-of-fair-cooperation update message $dfcu$ is encoded format to the crowd-sensor cs_i found in the current crowd sensor pool csp_i. Hence, the fair-cooperation update message cannot be viewed by crowd-sensor cs_i until it accepts the message and published it in a network. The secondary-user su frames the Degree-of-fair-cooperation-update $dfcu$ as follows in (Eq 12, 13, 14, 15):

$$\left.\begin{aligned} r\csc(cs_i) &= r\csc(cs_i) + 1 \\ cspc &= cspc(cs_i) + 1 \\ dfc(cs_i) &= dfc_{csp}(cs_i) + dfc(cs_i) \\ ulu(cs_i) &= ulu(cs_i) \bigcup su \\ dfc'(cs_i) &= dfc(cs_i)\hat{}\, s \end{aligned}\right\}$$

... (Eq 12)

$$edfc(cs_i) = e_{cp}(\{dfc'(cs_i), r\csc(cs_i), cspc(cs_i), ulu(cs_i)\})$$

... (Eq 13)

$$sig = h(id(cs_i), dfc(cs_i), r\csc(cs_i), cspc(cs_i), ulu(cs_i))$$

... (Eq 14)

$$dfcu(cs_i) = \{edfc(cs_i), sig(cs_i)\}$$

... (Eq 15)

// . $edfc(cs_i)$, is encoded version of the new Degree-of-fair-cooperation $dfc(cs_i)$ that XOR with a random token S, count of responses $rcsc(cs_i)$ by crowd-sensor cs_i, count of the crowd sensor pools $cspc(cs_i)$ having the crowd-sensor

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5737
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

CS_i, and unique list of users $ulu(cs_i)$ involved in Degree-of-fair-cooperation update of the crowd-sensor CS_i, which could be encrypted using a private key and can be decrypted by using the key that shared by secondary-user. The intermediate crowd-sensors that are available in the crowd-sensor shall decrypt and can view the values except for the new Degree-of-fair-cooperation. Also, the new signature on the crowd-sensor CS_i shall be created, with a hash value for the crowd-sensor id $id(cs_i)$, new Degree-of-fair-cooperation $\mathrm{dfc(cs_i)}, \mathrm{rcsc(cs_i)}, \mathrm{cspc(cs_i)}, \text{and } \mathrm{ulu(cs_i)}$ that are concatenated by a delimiter such as ";". The message $dfcu$ contains $edfc(cs_i)$, and $sig(cs_i)$.

To ensure that the new Degree-of-fair-cooperation should accept unconditionally by crowd-sensor CS_i, the bitwise operation exclusive OR (XOR) is applied on' $dfc(cs_i)$, and a random value S. By accepting $dfcu(cs_i)$ by crowd-sensor CS_i acknowledgment is offered to secondary-user SU and by receiving this acknowledgment, SU discloses S to enable the crowd-sensor CS_i decrypts $edfc(cs_i)$ and notifies the actual fair-cooperation update $dfc(cs_i)$ by performing bitwise operation XOR between the decrypted $dfc'(cs_i)$ and the value S. Further, the crowd-sensor CS_i accepts its new fair-cooperation status by revising the values assigned to the attributes' $\mathrm{dfc(cs_i)}, \mathrm{rcsc(cs_i)}, \mathrm{cspc(cs_i)}, \text{and } \mathrm{ulu(cs_i)}$. Afterward, the signature $sig(cs_i)$ that indicates the revised fair-cooperation state of the crowd-sensor CS_i will be shared with the other crowd-sensors of the network through conditional broadcasting.

3.6 Prevention of Possible Attacks in proposed framework ACSS

- Fair-cooperation Tainting Attack: The compromised source crowd-sensors in the process often focus on polluting the Degree-of-fair-cooperation for many other crowd-sensors in the crowd sensor pool.
- Conspired Fair-cooperation Boosting: Such an attack is focused on impacting the Degree-of-fair-cooperation of individual crowd-sensors because of collusion between two crowd-sensors.

Such attacks do not have significant importance in the proposed ACSS, as this model shall be focusing on the degree of fair-cooperation for crowd-sensor by considering the varied set of "divergence of source crowd-sensors that are involved in the Degree-of-fair-cooperation update". And also, in terms of average Degree-of-fair-cooperation that is given by the crowd-sensors involved in crowd sensor pool response, and due to such impacts, the attack sequences do not have much impact on the resulting degree of fair-cooperation.

4 Experimental study

The proposed method of cooperative spectrum sensing under affirmed crowd sensor selection (ACSS) has evaluated in this section. The measures "PU interference ratio", and "spectrum fair usage ratio" have considered scaling the performance of the ACSS. Alongside, the traditional network performance assessment metrics listed as "average delay", "delivery ratio", and "transmission overhead" has also estimated. In order to scale the significance of the ACSS, the obtained results of the corresponding metrics have compared with the results obtained by the contemporary model "Privacy-Preserving Truth Discovery Scheme in Crowd Sensing Systems (PPTDS) [41] has used in cooperative spectrum sensing (CSS) to discover the truth from the recommendations given about spectrum band availability by crowd sensors, which executed on corresponding simulation environment (see Table 2).

Table 2: Simulation parameters adapted

Spectrum users	12
Crowd sensors	125
Mobility in meters/sec	1.5
Area spanned by the sensors	1500 X 1750 m^2
Simulation Span	360 Sec
MAC Specification	802.11 DCF
Each spectrum's least cope	56 m^2
Radio Frequency	16 to 23 radios per second

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5737
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

4.1 Evaluation of Performance

From the successful completion of the simulation under the circumstances that are defined above, there are significant factors and insights that are generated from the process. The divergent ratio of compromised sensors placed among the crowd-sensors considered in an experimental study that is not having any impact on ACSS. It has a significant performance when compared to the results that are generated from other models considered in the study.

The values obtained for critical performance metrics "interference ratio", and "spectrum fair usage ratio" from both proposed model ACSS and the contemporary model PPTDS have visualized in Figure 2 and Figure 3. The graph portrayed in Figure 2 evincing the interference ratio of both ACSS and PPTDS models. The interference ratio observed for ACSS is considerably very low that compared to the interference ratio observed for the contemporary model PPTDS. The increase in the ratio of compromised sensors in the simulation environment leads to proportionate raise in the interference ratio observed for contemporary model PPTDS, whereas the interference ratio observed for ACSS is low and stable against the raise in the ratio of compromised sensors.

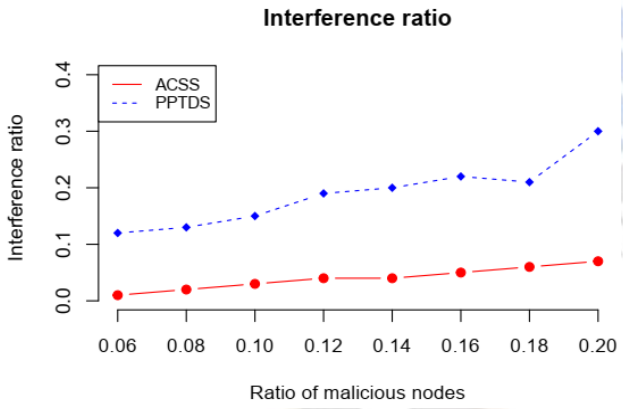

Figure 2: Interference ratio observed for ACSS and PPTDS

Similarly, the spectrum fair utilization ratio observed for cooperative spectrum sensing under ACSS is considerably high and stable that compared to the spectrum fair utilization ratio observed for cooperative spectrum sensing under contemporary model PPTDS, which is inversely proportionate to the ratio of compromised sensors in the network environment (see Figure 3).

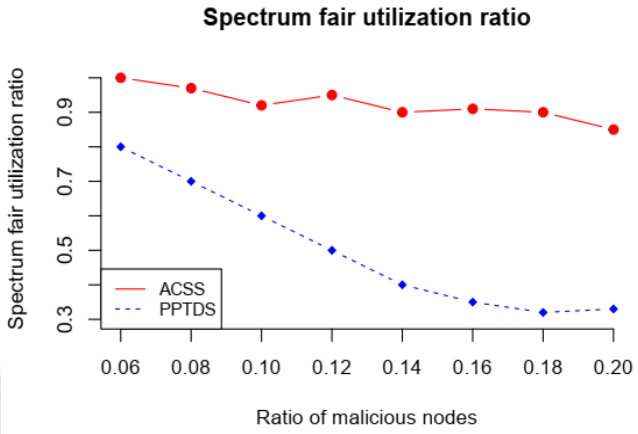

Figure 3: Spectrum fair utilization ratio observed for ACSS and PPTDS

Also, the delay ratio that is observed for ACSS has been minimal to a great extent compared to the delay ratio observed for spectrum sensing under the contemporary model PPTDS.

The delivery ratio, which is an essential factor in the evaluation process, also has resulted in positive and noteworthy results as depicted in (See Figure 4), when compared to the delivery ratio observed under spectrum sensing by PPTDS. Also, the values obtained for the metric "process overhead" has envisaged being very positive and fair enough concerning to ACSS.

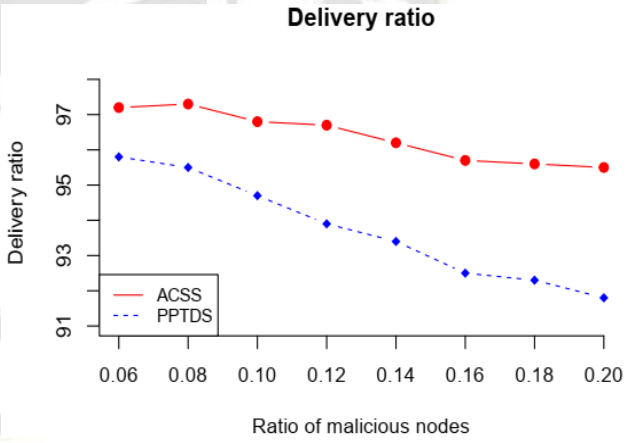

Figure 4: Delivery ratio observed for ACSS and PPTDS

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5737
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

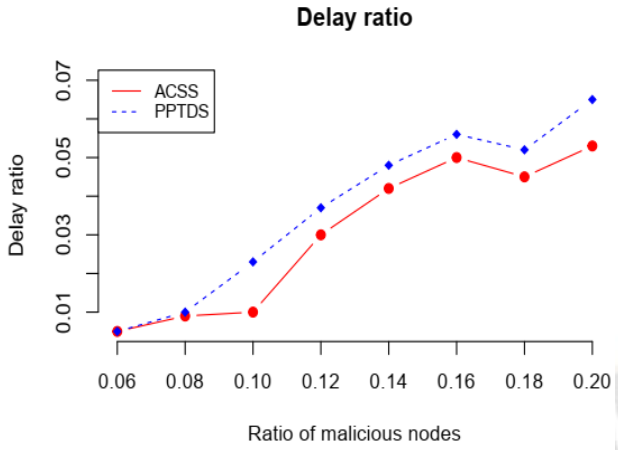

Figure 5: Delay ratio observed for ACSS and PPTDS

Under the metrics of Credibility Entangling and Contrived Credibility, Furthering is illustrated in Figure 5; the PPTDS delivery performance is downgraded. For instance, a PPTDS is performing well for compromised crowd-sensors ratios that are resulting in less than 0.08. But PPTDS has failed in terms of maintaining the same while the ratio for attacking the nodes has increased. Also, in the case of ACSS, the system conveys the linearity towards restricting the delay ratio due to resultant issues like dense ratios and compromised crowd-sensors.

The graphical representation in the above model depicts the scope and the incompetence of the PPTDS towards maintaining the optimal delivery ratio, which could take place in the conditions of the divergent ratio of attacking nodes. However, ACSS results denote the fact that the model has been successful in terms of defending the malevolent nodes with significant delivery ratio. Test results that are depicted in the process signify the method, its impact, and the related developments in an intrinsic manner.

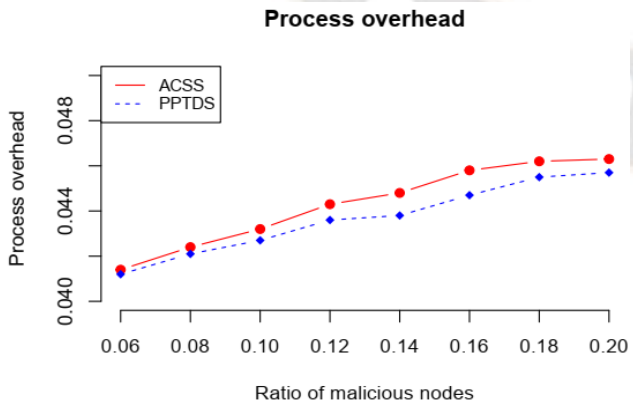

Figure 6: Results of performance of ACSS and PPTDS models for process overhead tests

The test result about how the packets are used for each data packet signifies the process overhead issues are generated from as per the inputs shown in Figure 6. From the test results, it is imperative that the process overhead that is observed for ACSS is high by a marginal extent when compared to the PPTDS model compared to the simulation. Such a rise in the count could be attributed to degree-of-reputation sharing and also some kind of publish and reveal a strategy that is adapted in the reputation update process. Unless such marginal overhead issues are addressed in trivial contexts of discovering the routes that are scalable in terms of maximal delivery ratio and minimal delay ratio factors addressing, the rise in the process overhead rates might not have much impact.

4.2 Cross Validation

This section explores the performance of the proposed model ACSS that compared to contemporary model PPTDS [41] through cross validation metrics towards truly falsified sensing data providers (truly detected compromised secondary users) and falsely falsified sensing data providers (falsely detected compromised secondary users). A plain simulation of cooperative spectrum sensing with 125 spectrum sensors as sensing data providers has been executed that discovered 67 crowd sensors as fair enough towards spectrum data sensing and 58 crowd sensors as tainted towards spectrum data sensing. The simulation with same sequence of spectrum sensing events has been repeated with proposed model ACSS and also with contemporary model PPTDS respectively in sequence. The crowd sensors discovered by these protocols as fair and compromised providers are further used to estimate the cross-validation metrics “precision, sensitivity, specificity, and accuracy. The detailed description of the performance predicted by the cross-validation model are explored following.

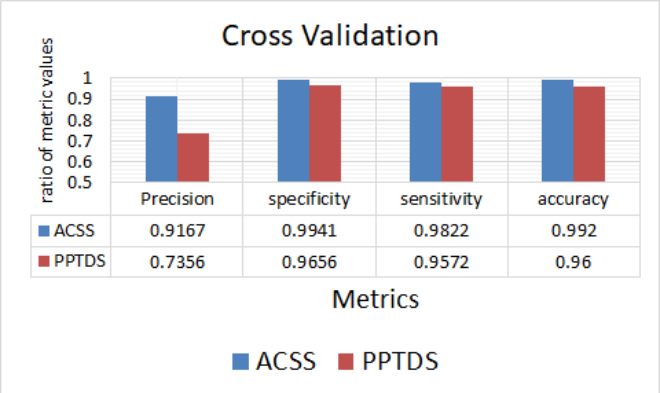

Figure 7: The related performance metric values of the models ACSS, and PPTDS discovered from cross-validation.

The crowd sensors discovered as fair by ACSS and PPTDS are 72 and 87 in respective order. The crowd sensors

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5737
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

of count 53 and 38 are discovered as compromised by the models ACSS, and PPTDS in respective order. The proposed model ACSS has discovered the count of 66 crowd sensors as truly fair crowd sensors, the count of 6 crowd sensors are detected falsely as fair crowd sensors, and the count of 56, and 1 crowd sensors truly discovered as compromised crowd sensors and falsely discovered as compromised crowd sensors respectively. Whereas, the contemporary model PPTDS discovered the count of 64, 23, 56, and 3 crowd sensors as truly detected fair crowd sensors, falsely detected fair crowd sensors, truly detected compromised crowd sensors, and falsely detected compromised crowd sensors in respective order.

The ACSS model has delivered significant performance in comparison to the other solution PPTDS, as shown in the figurative representation in figure 7.

The positive predictive value, which is the ratio of true positives to the total of true positives (truly predicted as fair crowd sensors) and false negatives (falsely predicted as compromised crowd sensors), is denoted by the metric precision. ACSS and PPTDS yielded metric precision values of 0.9167, 0.7356, respectively. These statistics has shown that the ACSS model outperforms the PPTDS model in terms of truly fair crowd sensor predictive value, as measured by precision.

The metric specificity is useful for determining the true detection rate of negative labeled crowd sensors (compromised crowd sensors), which is calculated as the ratio of true negatives (truly predicted as compromised crowd sensors) to the sum of true negatives and false positives (falsely predicted as fair crowd sensors). The specificity indicates the best way to eliminate compromised crowd sensors (having negative label). ACSS and PPTDS yielded metric specificity values of 0.9941, 0.9656, respectively. These values show that the model ACSS outperforms the PPTDS when it comes to detecting compromised crowd sensors, which is represented by specificity.

Sensitivity, which is the ratio of true positives (truly predicted as fair crowd sensors) to the sum of true positives and false negatives (falsely predicted as compromised crowd sensors), is used to calculate the true positive rate (rate of truly fair crowd sensors discovered). ACSS and PPTDS yielded metric sensitivity values of 0.9822, 0.9572, respectively. These values show that the model ACSS outperforms the PPTDS in terms of discovering truly fair crowd sensors, which is represented by sensitivity.

The ratio of the count of truly discovered fair crowd sensors, truly compromised crowd sensors, to the total count of both fair and compromised crowd sensors, is the metric accuracy used to describe the approximations of measurement towards true-value (discovering truly fair and compromised crowd sensors). ACSS and PPTDS yielded metric accuracy values of 0.992, 0.96, respectively. These values show that the model ACSS outperforms the other models in terms of discovering truly fair and compromised crowd sensors, as measured by accuracy.

5 Conclusion

Crowd sensors are playing a crucial role in decision-making systems. Cooperative spectrum sensing using crowd sensors is the buzz of cognitive radio networks in contemporary research of the corresponding domain. However, the crowd sensors based decision-making systems are highly vulnerable due to the falsified information by compromised sensors of the crowd sensors. Concerning this, a novel protocol that enables to adapt the information shared by affirmed and credible sensors is a significant need. This manuscript portrayed a novel information exchange protocol to perform cooperative spectrum sensing, which selects the affirmed and credible sensors to seek information about ideal spectrum bands to perform spectrum sensing. The proposal is a reputation based crowd sensor selection model, which is often vulnerable to "Credibility Entangling" and "Contrived Credibility Furthering". Concerning this, the proposed model has adapted a camouflaging approach to update the credibility of the corresponding sensors of the crowd-sensing approach. The contemporary model truth discovery approach has adapted to perform cooperative spectrum sensing, which is to scale the significance of the proposed model under assessment metrics "interference ratio", "utilization ratio", and other network standards "delay ratio", "delivery ratio", and process overhead. In addition the significance of the ACSS towards detecting truly fair and compromised crowd sensors has been estimated by cross validation. The values obtained for cross validation metrics from the outcomes of the ACSS, which have been compared to the values of the corresponding metrics obtained for PPDTS denoting that the ACSS is out performing PPDTS to detect truly fair and compromised crowd sensors. The experimental study portrayed that the proposed model is considerably significant compared to the contemporary model PPTDS. The future research can incorporate this Affirmed Crowd Sensor Selection approach in cooperative decision making systems of other domains such as the internet of things (IoT), software-defined networks.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5737
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

References

[1]. Buttar, Avtar Singh. "Fundamental operations of cognitive radio: A survey." 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT). IEEE, 2019, pp. 1-5.

[2]. Gao, Jing. "On the successful transmission probability of cooperative cognitive radio ad hoc networks." Ad Hoc Networks 58 (2017): 99-104.

[3]. Patil, Vilaskumar M., and Siddarama R. Patil. "A survey on spectrum sensing algorithms for cognitive radio." 2016 international conference on advances in human machine interaction (HMI). IEEE, 2016, pp. 1-5.

[4]. Homayounzadeh, Alireza, and Mehdi Mahdavi. "Performance analysis of cooperative cognitive radio networks with imperfect sensing." 2015 International Conference on Communications, Signal Processing, and their Applications (ICCSPA'15). IEEE, 2015.

[5]. Y. Zhao, M. Song, C. Xin, and M. Wadhwa, "Spectrum sensing based on three-state model to accomplish all-level fairness for co-existing multiple cognitive radio networks," in IEEE Proc. 2012 INFOCOM, pp. 1782–1790.

[6]. Jan Soliński, & Dr. Nitin Sherje. (2022). A Low Voltage Novel High-Performance Hybrid Full Adder for VLSI Circuit. Acta Energetica, (03), 09–14. Retrieved from http://actaenergetica.org/index.php/journal/article/view/471

[7]. Akyildiz, Ian F., Brandon F. Lo, and Ravikumar Balakrishnan. "Cooperative spectrum sensing in cognitive radio networks: A survey." Physical communication 4.1 (2011): 40-62.

[8]. Li, Zan, et al. "Improved cooperative spectrum sensing model based on machine learning for cognitive radio networks." IET Communications 12.19 (2018): 2485-2492.

[9]. Amrutha, V., and K. V. Karthikeyan. "Spectrum sensing methodologies in cognitive radio networks: A survey." 2017 International Conference on Innovations in Electrical, Electronics, Instrumentation and Media Technology (ICEEIMT). IEEE, 2017.

[10]. Tadeusz Chmielniak, & Nadica Stojanovic. (2022). Design of Computer Aided Design in the Field of Mechanical Engineering . Acta Energetica, (01), 08–16. Retrieved from http://actaenergetica.org/index.php/journal/article/view/460

[11]. Leibovitz, John S. "The great spectrum debate: A commentary on the fcc spectrum policy task force's report on spectrum rights and responsibilities." Yale JL & Tech. 6 (2003): 390.

[12]. Uribe, José de Jesús Rugeles, Edward Paul Guillen, and Leonardo S. Cardoso. "A technical review of wireless security for the internet of things: Software defined radio perspective." Journal of King Saud University-Computer and Information Sciences (2021).

[13]. Ali, Abdelmohsen, and Walaa Hamouda. "Advances on spectrum sensing for cognitive radio networks: Theory and applications." IEEE communications surveys & tutorials 19.2 (2016): 1277-1304.

[14]. Wang, Xiong, et al. "Millimeter wave communication: A comprehensive survey." IEEE Communications Surveys & Tutorials 20.3 (2018): 1616-1653.

[15]. T. Qin, H. Yu, C. Leung, "Towards a trust-aware cognitive radio architecture," ACM SIGMOBILE Mobile Computing and Communications Review. vol. 13, no. 2, PP. 86-95, Sept. 2009.

[16]. K. Zeng, Q. H Peng, Y. X Tang, "Mitigating spectrum sensing data falsification attacks in hard-decision combining cooperative spectrum sensing," Science China, vol. 57, no. 4, pp. 1-9, April 2014.

[17]. Q. Q Pei, B. B Yuan, L. Li, H. N Li, "A sensing and etiquette reputationbased trust management for centralized cognitive radio networks," Neurocomputing, vol. 101, no. 3, pp.129-138, Feb. 2013.

[18]. H. Chen, M. Zhou, L. Xie, et al, "Joint spectrum sensing and resource allocation scheme in cognitive radio networks with spectrum sensing data falsification attack," IEEE Transactions on Vehicular Technology, vol. 65, no. 11, pp. 9181-9191, Jan. 2016.

[19]. J. Y Feng, G. Y Lu, H Chang, "Behave well: How to win a pop vacant band via cooperative spectrum sensing," KSII Transactions on Internet and Information Systems, vol. 9, no. 2, pp. 1321-1336, May 2015.

[20]. S. Kar, S. Sethi, R. K Sahoo, "A multi-factor trust management scheme for secure spectrum sensing in cognitive radio networks," Wireless Personal Communications, vol. 97, no. 2, pp. 2523-2540, June 2017.

[21]. Mourougayane, Kaliappan, et al. "A robust multistage spectrum sensing model for cognitive radio applications." AEU-International Journal of Electronics and Communications 110 (2019): 152876.

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

[23]. O. Fatemieh, R. Chandra, and C. Gunter, "Secure collaborative sensing for crowd sourcing spectrum data in white space networks," in Proc. 2010 IEEE DySPAN, pp. 1–12.

[24]. H. Li and Z. Han, "Catch me if you can: an abnormality detection approach for collaborative spectrum sensing in cognitive radio networks," IEEE Trans. Wireless Commun., vol. 9, pp. 3554–3565, 2010.

[25]. S. Liu, Y. Chen, W. Trappe, and L. Greenstein, "Aldo: an anomaly detection framework for dynamic spectrum access networks," in Proc. 2009 IEEE INFOCOM, pp. 675–683, 2009.

[26]. O. Fatemieh, A. Farhadi, R. Chandra, and C. Gunter, "Using classification to protect the integrity of spectrum

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5737
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

measurements in white space networks," Proc. NDSS, vol. 11, 2011.

[27]. 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. 2009 IEEE Military Commun. Conf., pp. 1–7.

[28]. Y. Zhao, M. Song, and C. Xin, "A weighted cooperative spectrum sensing framework for infrastructure-based cognitive radio networks," Comput. Commun., vol. 34, pp. 1510–1517, 2011.

[29]. H. Wang and Q. Li, "Efficient implementation of public key cryptosystems on MICAz and TelosB motes," College of William and Mary, Williamsburg, VA, Tech. Rep., Oct. 2005.

[30]. H. Wang, B. Sheng, C. C. Tan, and Q. Li, "WM-ECC: an elliptic curve cryptography suite on sensor motes," College of William and Mary, Williamsburg, VA, Tech. Rep., 2007.

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

[32]. D. Das and S. Deshmukh, "Ambiguity-region analysis for double threshold energy detection in cooperative spectrum sensing," 2017 9th International Conference on Communication Systems and Networks (COMSNETS), Bangalore, pp. 123-127, 2017.

[33]. R. Zhang, J. Zhang, Y. Zhang and C. Zhang, "Secure crowdsourcingbased cooperative pectrum sensing," in Proc. IEEE INFOCOM, pp. 2526-2534, 2013.

[34]. M. F. Amjad, B. Aslam and C. C. Zou, "Reputation Aware Collaborative Spectrum Sensing for Mobile Cognitive Radio Networks," MILCOM 2013 - 2013 IEEE Military Communications Conference, San Diego, CA, pp. 951-956, 2013.

[35]. O. Fatemieh, R. Chandra and C. A. Gunter, "Secure Collaborative Sensing for Crowd Sourcing Spectrum Data in White Space Networks," 2010 IEEE Symposium on New Frontiers in Dynamic Spectrum (DySPAN), Singapore, pp. 1-12, 2010.

[36]. F. Benedetto, G. Giunta, A. Tedeschi and E. Guzzon, "Performance improvements of cooperative spectrum sensing in cognitive radio networks with correlated cognitive users," 2015 38th International Conference on Telecommunications and Signal Processing (TSP), Prague, pp. 1-5, 2015.

[37]. F. Benedetto, A. Tedeschi, G. Giunta and P. Coronas, "Performance improvements of reputation-based cooperative spectrum sensing," in IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, 2016, pp. 1-6.

[38]. M. A Morid and M. Shajari, "An enhanced e-commerce trust model for community based centralized systems," Electronic Commerce Research, vol. 12, no. 4, pp. 409-427, Nov. 2012.

[39]. X. Y Li, F. Zhou and X. D Yang, "Scalable feedback aggregating (SFA) overlay for large-scale P2P trust management," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 10, pp. 1944-1957, Oct. 2012.

[40]. L. C Ma, X. F Liu, Q. Q Pei and Y. Xiang, "Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing," IEEE Transactions on Services Computing, to appear.

[41]. M. Li, Y. Xiang, B. Zhang, et al, "A trust evaluation scheme for complex links in a social network: a link strength perspective," Applied Intelligence, vol. 44, no. 4, pp. 969-987, June 2016.

[42]. Chalapathi, M. M., et al. "Ensemble Learning by High-Dimensional Acoustic Features for Emotion Recognition from Speech Audio Signal." Security and Communication Networks 2022 (2022).

[43]. Reddy, K. Uday Kumar, S. Shabbiha, and M. Rudra Kumar. "Design of high-security smart health care monitoring system using IoT." Int. J 8 (2020)

[44]. A. Jϕsang, R. Ismail, "The beta reputation system," in Proc. the 15th Bled Electronic Commence Conference, June 2002, pp.1-14.

[45]. Rudra Kumar, M., Rashmi Pathak, and Vinit Kumar Gunjan. "Machine Learning-Based Project Resource Allocation Fitment Analysis System (ML-PRAFS)." Computational Intelligence in Machine Learning. Springer, Singapore, 2022. 1-14

[46]. Suneel, Chenna Venkata, K. Prasanna, and M. Rudra Kumar. "Frequent data partitioning using parallel mining item sets and MapReduce." International Journal of Scientific Research in Computer Science, Engineering and Information Technology 2.4 (2017).

[47]. Gunjan, Vinit Kumar, and Madapuri Rudra Kumar. "Predictive Analytics for OSA Detection Using Non-Conventional Metrics." International Journal of Knowledge-Based Organizations (IJKBO) 10.4 (2020): 13-23

[48]. Miao, Chenglin, et al. "Privacy-preserving truth discovery in crowd sensing systems." ACM Transactions on Sensor Networks (TOSN) 15.1 (2019): 1-32.

[49]. Carmines, Edward G., and Richard A. Zeller. "Reliability and validity assessment". Vol. 17. Sage publications, 1979