International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS)
(Volume 30, Issue: Special), October 2018
An Indexed and Referred Journal with Impact Factor: 2.75
ISSN (Online): 2347-601X
www.ijemhs.com

A Study on Data Falsification Lenient Secure Spectrum User Reliability Verification

[1]Gyanendra Kumar Rout
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India
[2]Sambit Parida
Black Diamond College of Engineering & Technology, Jharsuguda, Odisha, India

Abstract

Cognitive radio network's primary challenge is sensing of primary user signal and efficiently handling the spectrum availability. Spectrum sensing is the way ahead and vital for Dynamic Spectrum Access, where malicious users deploy Spectrum Sensing Data Falsification (SSDF) attacks. This paper discusses the technique to calculate the importance of using nodes for primary as well as secondary users. It prevents spectrum problems to primary users from Spectrum Sensing Data Falsification by secondary users and also shields secondary users from unauthorized primary users. Simulation runs of the novel approach using usual network conditions and SSDF attacks greatly bought down the error rate of spectrum decision and at the same time improved the detection rate of malicious cognitive nodes.

Keywords: *Cognitive Radio, Cooperative Spectrum Sensing, Data falsification attack, Malicious User Detection, Spectrum sensing*

I. INTRODUCTION

Till date, predetermined spectrum bands are being allotted to service providers. This approach resulted in unproductive spectrum consumption and as an alternative cognitive radio networks was introduced. The network will allow cognitive radios, labeled secondary unlicensed users (SUs) to choose the foremost licensed users or primary users (PUs) bands when these bands are unoccupied by PUs. However the SUs should vacate the band promptly following a Licensed User begins transmission in the affiliated band [1]. Thus the main function of a cognitive radio is spectrum sensing.

Spectrum sensing methods are mainly energy detection, cyclostationary feature detection, and matched filter detection [2-4]. The functioning of spectrum sensing is evaluated using probability of detection and probability of false alarm. Probability of detection is the probability of confirming the occupancy of spectrum while the licensed user is found. Probability of false alarm is the probability of confirming the occupancy of spectrum while the licensed user has no broadcast. Among various spectrum sensing strategies for easily determining the licensed spectrum reputation, the energy detector method incurs quite a lower execution cost and as such is broadly utilized. It serves as the optimum strategy to identify the signal carried by a primary user whose place is obscure and also to realize the power of the obtained transmission [6]. The trouble with this technique is that the obtained transmission power may be significantly diminished at a specific geographic area because of multipath fading as well as shadowing consequences [7]. In these conditions, it is complicated for a secluded sensing device to differentiate around an idle band and faded one. To conquer this issue, cooperative spectrum sensing techniques have been projected [5, 8, 9]. Anyhow, in cooperative sensing, because of imperfect network between a licensed user and a secondary user (SU) or dishonest tendencies of a SU, a customer could transmit false sensing outcome to the fusion hub. Thus, the efficiency of the method degrades significantly. To conquer this concern, protected spectrum sensing become suggested.

II. RELATED WORK

The concept of utilizing Beta Reputation System as reputation assessment system projected in [10] is that a node's capability in its spectrum sensing reputation is exploited as a primary factor for computation of spectrum reports. The assumption being made is that the Licensed User's transmission range is sufficient to be obtained by every node in the cognitive radio network (CRN) and the Secondary User base station (SUBS), the controlling station of the CRN. It further assumes that the Licensed User could interact with SUBS subjective to error reporting to the secondary user base station about any impedance resulting from CRN procedure. As this services considers that the Licensed User can't sell its unallocated spectrum bands, hence generally there is no compensation for it to interact with the CRN. This conversation could cost a Licensed User, extra hardware and/or system complexity, merely just to notify the CRN about its communication interferences.

Spectrum sensing reports only in Licensed User's coverage area should be considered for spectrum decisions, and only those SUs prominence scores will be updated. Moreover, the FCC stipulates, the CRN might use empty spectrum bands in a non-interfering perspective eliminating the requirement of changes in Licensed User. The work also does away with any mobility by SUs or PUs and proposes a collaborative spectrum sensing strategy [11] taking into consideration Location Reliability and Malicious Intent as reliability criteria. The Dempster-Shafer concept of validation to analyze reliability of revealing secondary user nodes is used in this work. The projected strategy assigns reliability values to various cells in each network that can acquire exceptional stages of Licensed User's signal because of the consequence of multi-path, signal diminishing and additional considerations in the radio environment. Spectrum sensing reports from SUs using Equal Gain Combining and trust values assigned to their cells are both given equal importance for data aggregation.

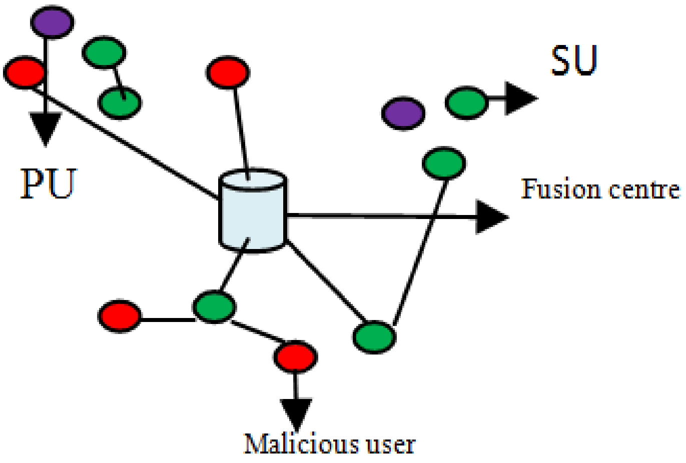

Figure 1 Adhoc CRN with Malicious Nodes

This strategy is based upon the factor that Licensed User's interaction range is hugely adequate to be obtained by the whole CRN and utilizes the spectrum sensing assessments of every CRN nodes to achieve the ultimate spectrum decision. Authors in [12] and [13] base their strategy on the factor that the transmitting range of Licensed User is significant adequately to be obtained in the whole CRN [12] and offer pre-filtering all reports to eliminate drastic spectrum sensing reports and a simple strategy to compute spectrum sensing decisions. [13] presents the spectrum sensing issue as an M-ary hypotheses screening difficulty and proposes a cluster- based CRN where cluster heads acquire, process raw spectrum sensing information and send it to the fusion center.

Concluding the basis of both the approaches is on the fact that PUs transmission range is large enough for every node in the network to access; both approaches have no practical application for a CRN having a Licensed User with smaller transmission range than the size of the CRN.

III. DATA FALSIFICATION LENIENT SECURE SPECTRUM SENSING BY NODE RELIABILITY VERIFICATION

The reliability of spectrum sensing (CSS) can be severely degraded by the falsified spectrum sensing reports provided by malicious secondary users (SUs). In regard to this a novel prominence state verification strategy (PSV) was introduced in our earlier work. It is proven to be significant to identify the reliable neighbor nodes towards spectrum sensing. The constraint of that model is that it verifies only the reliability of the responders (neighbor nodes involved in spectrum sensing) by assuming that the supplicant (secondary user that is initiating spectrum sensing) nodes are not malicious, but in reality this is not true. A node can attempt to seek the spectrum under malicious intention that it can infer the utilization of the spectrum by primary user. This practice of attack on supplicant side would lead to severe interference towards spectrum usage. The model devised here is intended to avoid the malicious and selfish nodes from the act of spectrum sensing. A secondary user of CRN can seek the response from its neighbor nodes under a malicious or selfish intention.

The possible attacks would be

- By knowing the busy state of the spectrum, can attempt for an interference attack (malicious intention).
- By knowing the idle state of the spectrum, can engage that spectrum for future usage (selfish intention)

The model devised in our earlier work verifies the reputation of the respondents only. This verification is being enhanced such that any neighbor node verifies the reputation state of the supplicant.

Reliability check technique is devoted to obtain the reliability through neighbors. It executes a particular divergence test to offer the position with almost all the processing neighbor secondary user position. Usual Deviance Test requires each and every neighbor secondary user to authenticate accumulated reliability as well as its solid reliability to attain a neighbor and avoid any oblique reliability that is isolated by a specific quality A (the divergence roof). In Exclusive Divergence Test the outcome is to obtain neighbor secondary user by focusing on the reliability of its neighbor secondary user. The reliability of the neighbor nodes is checked and is concluded as reliable if the value is greater than the threshold. This enables quick reliability checking that is essential in our evaluated circumstances during which neighbor secondary users don't get adequate time to notice the reliability of various neighbor secondary users.

Assessing the Reliability of the Neighbor Secondary Users

A cognitive secondary user *ssu,* is a spectrum supplicant and *nsu* is the number of neighbor secondary users to spectrum supplicant users *ssu*. The spectrum supplicant measures the reliability of all its neighbor secondary users as shown in figure 2

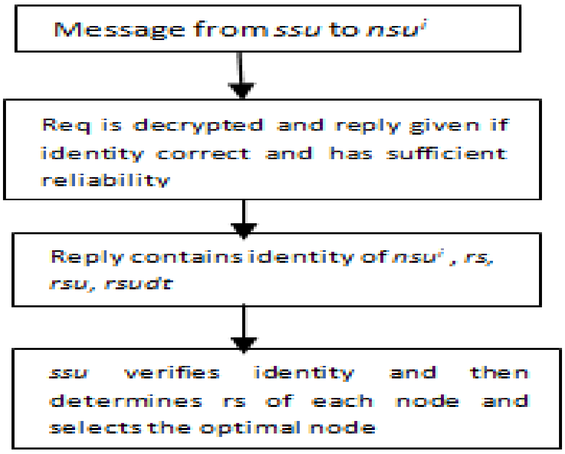
Message from *ssu* to nsu^i
Req is decrypted and reply given if identity correct and has sufficient reliability
Reply contains identity of nsu^i , *rs, rsu, rsudt*
ssu verifies identity and then determines rs of each node and selects the optimal node

Figure 2 Assessing Reliability of nodes

IV. EMPIRICAL STUDY BY SIMULATION

The aim of the simulations is to analyze the relevance of prominence state verification towards handling the Spectrum Sensing Data Falsification attacks in Spectrum state verification process. The network is considered with 200 numbers of nodes with divergent number of malicious and selfish nodes that ranges from 2% to 20%. The characteristics and attributes are illustrated in table1. The constraint that we didn't consider is the impact of location consistency of secondary user, which is assumed to be stable and consistent. The explored results are significantly confirming the advantage of the proposal. The impact of the proposal was verified by comparing with our earlier model devised.

Table1 Parameters and their values range used in simulations

Number of secondary users Range	18 to 180
scope of network region	1720 m × 540 m
Radio spectrum's least cope	258 m
Channel count	43
Radio Frequency Model(each)	7 rps
Maximal load per each transmission	0.9 KB
Load assortment range	256 to 512 kb per second
raw data transfer under physical link	2.5 Mb per second

The main purpose of this model is to analyze the relevance of Data Falsification Lenient Secure Spectrum Sensing (DFL) over the previous model which verifies the reliability of the neighbor nodes only. Parameters used are inference lenient ratio and spectrum utilization ratio.

Figure (3) shows the interference free spectrum utilization vs percentage of malicious secondary users. The results in table 2 indicate that the reliability verification of the supplicant secondary users increases the avoidance of inference during spectrum utilization by secondary users. The average covariance of the inference free spectrum utilization ratio observed is 0.12, which can conclude as the advantage of proposal towards inference lenient spectrum sensing.

Figure (4) maps DFL against our previous model in spectrum utilization ratio. The results indicate the maximal utilization of the spectrum by secondary users. The proposed intent inference lenient model maximized the spectrum utilization, which is due to significant avoidance of the selfish nodes as secondary users. The average improved spectrum utilization ratio observed under proposed model is 0.341.

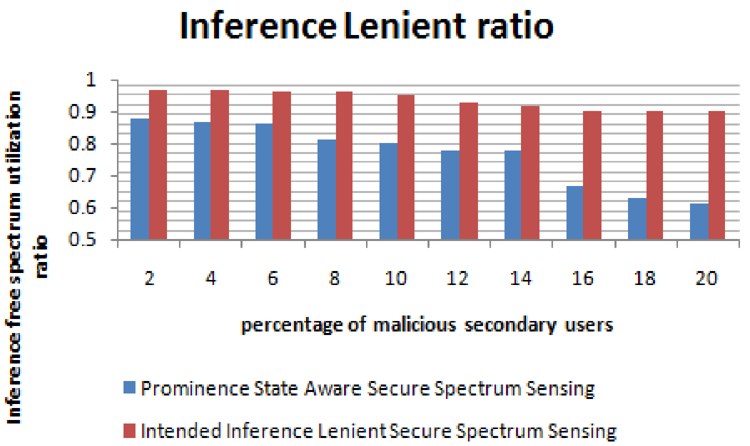

Figure 3 Interference Avoidance during Spectrum Sensing

The numerical values are tabulated in table 2.

Table 2 Comparison of PSASS and DFL with respect to Interference free spectrum utilization

Malicious Nodes %	2	4	6	8	10	14	16	20
PSASSS	0.88	0.87	0.86	0.81	0.8	0.78	0.67	0.61
DFL	0.97	0.97	0.96	0.96	0.95	0.92	0.9	0.9

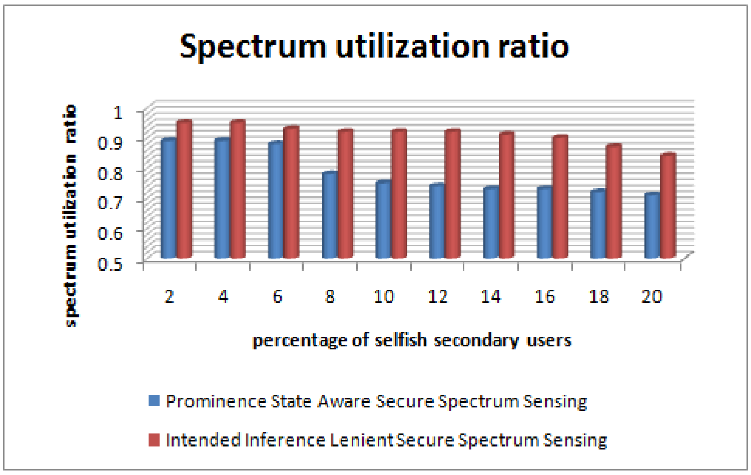

Figure 2 Spectrum Utilization Ratio

The numerical values are tabulated in table 3.

Table 3 Comparison of PSASS and DFL with respect to Spectrum utilization ratio

Selfish Nodes %	2	4	6	8	10	14	16	20
PSASSS	0.89	0.89	0.88	0.78	0.75	0.73	0.73	0.71
DFL	0.95	0.95	0.93	0.92	0.92	0.91	0.9	0.84

V. CONCLUSION

The proposed Data Falsification Intended Inference Lenient Secure Spectrum Sensing strategy depends on decentralized reliability state verification of the neighbor nodes which require information regarding spectrum available and also the nodes which supply the information in cognitive radio networks. The cooperative or combined CRN spectrum sensing perspective spreads a technique to the attackers who might contradict the sensing outcomes. The determination of an attacker might be moreover selfish or malicious. Simply being selfish, an attacker may update the occurrence of the primary user if there is essentially none and abstain the cognitive users from using the spectrum. Although being malicious, an assailant may report the absence of the licensed user while there is one, hence making chaos and obstruction for primary and secondary users. In this model the Reliability based secondary user concerned Spectrum sensing technique is examined. The devised version is appreciable and exceptional to assure spectrum sensing. The quantitative analysis done through simulations indicates the devised model is scalable and robust towards handling the malicious or selfish nodes in spectrum state verification strategy. The model devised here in this paper is not considering factors such as signal fading due to urbanization, contention in spectrum sensing, which can be playing significant role to influence the nodes to send falsified spectrum sensing information. Hence in our further work these factors will be considered in respondent selection and reliability state updating strategy.

VI. REFERENCES

[1] S. Haykin, “Cognitive Radio: Brain-Empowered Wireless Communications,” IEEE Journal on Selected Areas in Communications, Vol. 23, No. 2, 2005, pp. 201-220. doi:10.1109/ JSAC.2004.839380.

[2] S. M. Kay, “Fundamentals of Statistical Signal Processing: Detection Theory, “Prentice Hall, Upper Saddle River, 1998.

[3] H. V. Poor, “An Introduction to Signal Detection and Estimation,” Springer- Verlag, New York, 1994.

[4] S. Enserink and D.Cochran, “A Cyclostationary Feature Detector,” Proceedings of the 28th Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, 31 October-2 November 1994, pp. 806-810. doi:10.1109/ACSSC.1994.471573.

[5] P. Kaligineedi, M. Khabbazian and V. K. Bhargava, “Secure Cooperative Sensing Techniques for Cognitive Radio System,” IEEE International Conference on Communications, Beijing, 19-23 May 2008, pp. 3406-3410.

[6] B. Shen and K. S. Kwak, “Soft Combination Schemes for Cooperative Spectrum Sensing in Cognitive Radio Networks,” ETRI Journal, Vol. 31, No. 3, 2009, pp. 263-270. doi:10.4218/ etrij.09.0108.0501.

[7] D. Cabric, S. M. Mishra and R. W. Brodersen, “Implementation Issues in Spectrum Sensing for Cognitive Radios,” Proceedings of 38th Asilomar Conference on Signals, Systems, Computers, Pacific Grove, 7-10 November 2004, pp. 772-776.

[8] R. L. Chen, J.-M. Park and K. G. Bian, “Robust Distributed Spectrum Sensing in Cognitive Radio Networks,” Proceedings of the 27th Annual IEEE Conference on Computer Communications, Phoenix, 13-18 April 2008, pp. 1876-1884.

[9] K. J. Peng and Z. H. Tsai, “A Distributed Spectrum Sensing Scheme Based on Credibility and Evidence Theory in Cognitive Radio,” Proceedings of the 17th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Helsinki, 11-14 September 2006, pp. 1-5. doi:10.1109/PIMRC.2006.254089.

[10] Qin, T., et al., “Towards a trust aware cognitive radio architecture,” SIGMOBILE Mobile Computational Communication Reviews 2009, pp. 86–95.

[11] Jana, S., et al., “Trusted collaborative spectrum sensing for mobile cognitive radio networks,” 32nd IEEE International Conference on Computer Communications, INFOCOM 2012.

[12] P. Kaligineedi., et al., “Secure Cooperative Sensing Techniques for Cognitive Radio Systems”, International Conference on Communications, ICC 2008.

[13] Jin Wei., et al., "Two-Tier Optimal-Cooperation Based Secure Distributed

[14] Spectrum Sensing for Wireless Cognitive Radio Networks," IEEE INFOCOM 2010.

[15] Qin, T., et al., “Towards a trust aware cognitive radio architecture,” SIGMOBILE Mobile Computational Communication Reviews 2009, pp. 86–95.

[16] http://www.ijcsit.com/docs/Volume%205/vol5issue03/ijcsit20140503453.pdf