https://dx.doi.org/10.22161/ijaers.4.4.20 ISSN: 2349-6495(P) | 2456-1908(O)

An Empirical Estimation of CSS Cognitive Radio Network Performance under Spectrum Sensing Data Falsification Attack

Rajesh D. Kadu[1], Dr. Pravin P. Karde[2], Dr. V. M. Thakare[3]

[1] Research Scholar, SGB Amravati University, Amravati, India
[2]Department of Information Technology, Government Polytechnic, Amravati, India
[3]Department of Computer Science, SGB Amravati University, Amravati, India

Abstract**—***Cooperative spectrum sensing (CSS) significantly improves the performance of spectrum sensing process in cognitive radio networks (CRNs). Individual spectrum sensing by a cognitive radio (CR) is often inaccurate as the channel often experiences fading and shadowing effects. CSS has been shown to have many advantages in terms of spectrum use and robustness. Despite these facts, a CSS scheme also vulnerable to many security attacks from malicious users (MUs). In order to get unfair usage of spectrum band, MUs can generate false spectrum sensing reports to disturb the good secondary users (SUs) decision about presence of primary user (PU). In this paper, we consider the spectrum sensing data falsification attack (SSDF) in CSS and propose the protocol to identify and eliminate the attacker or malicious user (MU) to improve the network performance. In SSDF attack, MUs send the false spectrum sensing results to fusion center (FC) with the intension that it should make wrong decision about spectrum sensing. In this scenario, FC acts as a data collector to fuse the reports sent by SUs.*

Keywords— CR, CRNs, CSS, FC, SSDF.

I. INTRODUCTION

The fast growing smart phone users and mobile internet based applications demands for optimum utilization of spectrum. CRNs improves the efficiency of spectrum utilization under the current static spectrum allocation policy. In conventional spectrum regulation models, majority of the spectrum is allocated to PUs or licensed users for exclusive use. CRNs allows SUs or unlicensed users to use idle spectrum without causing interference with PUs.

Cognitive radio (CR) technology allows the SUs to access the spectrum in opportunistic manner when PUs are not using it. The SUs continuously carry out the sensing process to detect the white spaces available in spectrum band. The white spaces are the frequency bands which are not used by PUs. The SUs should sense the idle spectrum in order to avoid the interference with PUs. Moreover, in order to avoid the disturbance to PUs, SUs should vacate the spectrum timely if PUs appears to be using it [1].

Individual spectrum sensing by a cognitive radio (CR) is often inaccurate as the channel often experiences fading and shadowing effects. CSS significantly improves the accuracy in detection of PUs presence and helps to increase channel sensing accuracy in CRNs [2]. Moreover CSS is more accurate and have more advantages as it exploits the cooperation among many CRs or SUs.

For detection of PU in a spectrum band, good SUs mainly uses three methods. These are matched filter detection, cyclostationary feature detection, and energy detection. [3] [4]. Energy detection method of spectrum sensing has low computational and implementation complexities. Hence, it is more preferred method for spectrum sensing. Energy based detection can be carried out in both the time and frequency domains.

II. RELATED WORK

Saud Althunibat et al. [5] have proposed protocol for secured CSS. This protocol improves the improves the energy efficiency in presence of malicious users (MUs). In this approach, a Message Authentication Code (MAC) is produced by using a low-overhead symmetric cryptographic mechanism. This code is used to authenticate spectrum sensing data reports under a trade-off between energy and security. With increase in number of MUs, achievable energy efficiency decreases without using security algorithm. The proposed secure CSS greatly improves the energy efficiency compared to the conventional insecure CSS.

Chowdhury Sayeed Hyder et al. [6] proposed adaptive reputation based clustering algorithm as a countermeasure against SSDF attack. The algorithm does not consider the past information of attacker distribution or full identification of MU. The performance evaluation of the proposed algorithm is carried out with respect to independent and collaborative SSDF attacks. The proposed algorithm considerably reduces error rate with compare to

https://dx.doi.org/10.22161/ijaers.4.4.20 *ISSN: 2349-6495(P) | 2456-1908(O)*

existing collaborative sensing schemes and improves the spectrum utilization.

The defense scheme proposed by Hong Du, Shuang Fu and Hongna Chu [7] use the credit value with each CR user and this value is updated if sensing result is consistence with final decision. In this approach, if reputation value is greater than minimum credit threshold then CR user can take part in next round of sensing. Otherwise, it is identified as MU. The proposed schemes based on credibility weighting and excluded MUs results in higher probability of collaborative detection. Furthermore, sensing performance of the proposed scheme has been further improved. Probability of false alarm remains constant with increase in number of malicious users.

The Majority-based Assessment approach identifies and eliminate the attackers. The Delivery-based Assessment approach evaluates the local decisions on the basis of delivery of the transmitted data by scheduled cognitive user (CU) . For the identified unused spectrum, CU gets scheduled for transmission of data. As a result, based on the success of delivering the transmitted data, the real spectrum status can be appropriately defined at the BS, and then used to evaluate the local decisions. Due to removal of attackers detection, probability improves and probability of false alarm reduces. In presence of the proposed punishment policy, individual energy efficiency of the honest CU improves and of attacker reduces with increase in attack-removal threshold [8].

Insistent Spectrum Sensing Data Falsification (ISSDF) attack is addressed by Aida Vosoughi et al. [9] . This attack is different from traditional SSDF attack. In this attack, MU falsifies its sensing data and sends the same falsified value in every iteration of consensus to all the nodes. In this approach, each CR node is associated with some trust value. If trust management not executed, then error rates increase quickly with more consensus iterations. The trust-aware schemes converge to much lower error rates compared to oblivious schemes within only a small number of consensus iterations. The misdetection probability and false alarm probability improves with more number of consensus iterations in presence of ISSDF nodes in network.

Linyuan Zhang et al. [10] proposed a defense reference scheme which in cooperation makes use of the cognitive spectrum sensing process and spectrum access in closed loop manner. This approach gives feedback to SUs about extended sensing result because of PU presence or transmission success or failure outcome to reassess the sensors local sensing performance. The proposed reference scheme improves the global sensing performance with increase in attack population with compare to other approaches such as no defense, ideal abandoning, optimal fusion, global filtering, soft fusion and trusted node. The global performance is deteriorated with increase in attack probability. If attack probability varies then performance changes in this approach.

Ji Wang et al. [11] proposed a trust-based data fusion rules which decouple erroneous reports as a result of low sensing abilities from false reports because of attacks in distributed CNNs. An individual, majority voting, and capability-weighted majority voting approaches are used to compare with the proposed approach. The parameters used for this comparison are individual success rate, or the probability of successfully detecting the actual status of the channel. The proposed trust-based data fusion scheme outperforms traditional data fusion rules and can distinguish MUs carrying out data falsification attacks through their low trust scores in the long run.

CAO Long et al.[12] proposed the symmetric cryptographic approach which use message authentication code to authenticate the sensing results of SUs as a solution over SSDF attack. The proposed approach maximize the energy efficiency of the SUs. Sasa Maric et al. [13] proposed modified belief propagation algorithm which use reputation as weighted scalar in distributed spectrum sensing scheme. In this approach, honest users are rewarded with increase in reputation while untruthful users are penalized with decrease in their reputation. the honest users with high reputation have high impact on final decision about channel is vacant or occupied.

Abbas Ali Sharifi and Mir Javad Musevi Niya [14] proposed attack proof CSS scheme which estimates attack strength. The attack strength is considered as the probability that a given user is MU. In this approach, attack strength is used in k out of N rule to find the best value of k that reduces the Bays risk. Saud Althunibat et al. [15] considered the infrastructure based CRN in which policy is proposed to identify the attackers. Once the attackers are identified, their sensing result reports are ignored. The other proposed policy punish the attacker by redistributing the transmission opportunities among users based on their local performance.

The remaining paper is organized as follows. Section III presents overview of SSDF attack in CSS. Section IV gives proposed protocol. In section V, simulation environment and result analysis is given. Section VI concludes the paper.

III. SSDF ATTACK IN CSS

The performance of spectrum sensing process can be improved by exploiting spatial diversity called as CSS. CSS can be carried out in both centralized and distributed CRNs. In a centralized CRN, there is a data collector called as fusion center (FC) to which all the SUs reports the spectrum sensing results.. Also FC gives instructions to SUs and takes decision about presence or absence of PU

https://dx.doi.org/10.22161/ijaers.4.4.20 *ISSN: 2349-6495(P) | 2456-1908(O)*

based on received results. In a distributed CRN, there is no FC and CRs exchange the spectrum sensing results with other CRs. Hence, Each CR receiving the spectrum sensing results from other CRs plays role of FC. Although CSS scheme is more accurate and reliable, it is more vulnerable to many security threats and attacks such as jamming attack, primary user emulation attack (PUEA) and spectrum sensing data falsification attack (SSDF). In SSDF attack, MUs intentionally send fake spectrum sensing results to mislead decision making of FC.

The local spectrum sensing results of each SUs are sent to FC which makes a final decision according to fusion rule. FC then sends this decision to all the SUs. The fusion schemes used by FC are soft decision fusion and hard decision fusion. In soft decision fusion, all the SUs sends the complete local spectrum sensing results to FC. In hard decision fusion SUs send one bit information to FC regarding presence or absence of PU. Fig. 1 shows scenario in which good SU sends the honest local spectrum sensing reports to FC while attackers sends the false reports.

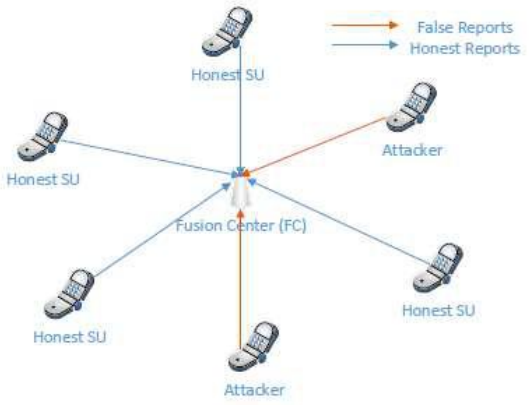

Fig. 1: SSDF attack in CSS

.

IV. PROPOSED PROTOCOL APPROACH

In proposed model of SSDF attack one PU, several SU's and FC is considered. PU transmits on communication channel and in order to detect the presence of PU, SUs sense the PU signals periodically. The SUs then sends spectrum sensing results to FC at the end of the sensing period. FC then makes the final decision about PU exist or not based on the information sent by SUs in the network. The attackers or dishonest SUs sends the false spectrum sensing results order to mislead the decision making of FC. The attacker node randomly select the available channel list and remove it from the sensed list.

After collecting the reports from all cognitive nodes in the region, FC compares the report of each device and compute its relativity between the reports. FC identifies missed active reports from all the sensed reports. False count for the corresponding node is incremented and compared with the threshold limit of the missed report. If the missed report count is greater than the threshold then corresponding device is classified as data falsification misbehavior node and eliminated from the network.

4.1 Performance of Proposed Approach

The performance of the proposed protocol is measured with various network parameters. These are packet delivery ratio (PDR), delay, control overhead, dropping ratio, average energy consumption, average residual energy, jitter and throughput. The packet delivery ratio is number of received packets by node divided by number of sent packets multiplied by 100. Delay is changes in data transmission time from source node to destination node. The total number of control packets needed to discover correct path to reach final destination is control overhead. Dropping ratio is ((number of sent packets - number of received packets)/sent)*100. Energy consumed by all nodes is total energy consumed. Total energy consumed divided by number of nodes is average energy consumption. Average residual energy is total residual energy divided by number of nodes. Throughput is number of bits delivered per second. We used traffic to measure the network performance when SSDF attacker is present with all above mentioned parameters. Traffic increases as number of senders increases.

V. SIMULATION ENVIRONMENT AND RESULT ANALYSIS

NS-2 environment is used to test the proposed protocol. The proposed protocol detects SSDF attacker and eliminates it from the network. Each node estimate its energy level to extend the network lifetime. Energy threshold is maintained and total number of nodes considered in network are 50. The total simulation time is set as 200 seconds. the data packet size considered for the simulation is 512 byte. Initial energy is 100 Jules. By considering the all optimum parameters, following results are obtained after simulation. Fig.2 shows PDR and dropping ratio results for varying traffic. The PDR does not affected much more and hence dropping ratio with increase in traffic. PDR improves due to minimum drop of packets. Protocol reduces flooding and hence collisions not occurred.

.

https://dx.doi.org/10.22161/ijaers.4.4.20 ISSN: 2349-6495(P) | 2456-1908(O)

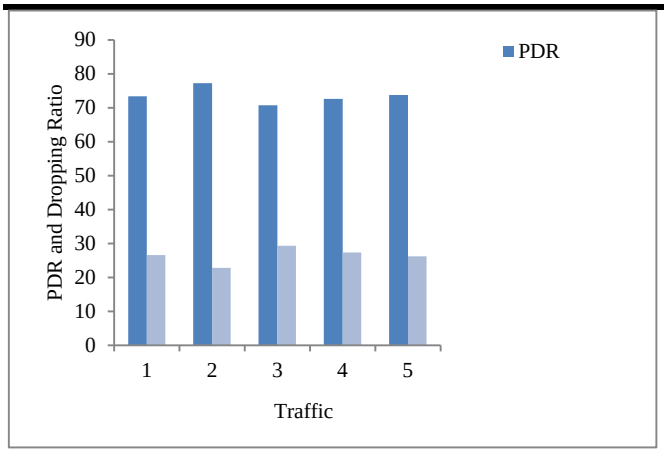

Fig. 2: Traffic vs. PDR and Droping ratio

Fig.3 shows the number of control packets that are used to find correct path to reach final destination for increasing traffic in network. With increase in traffic, less number of control packets are required. It shows good performance of the network due to identification and elimination of SSDF attacker.

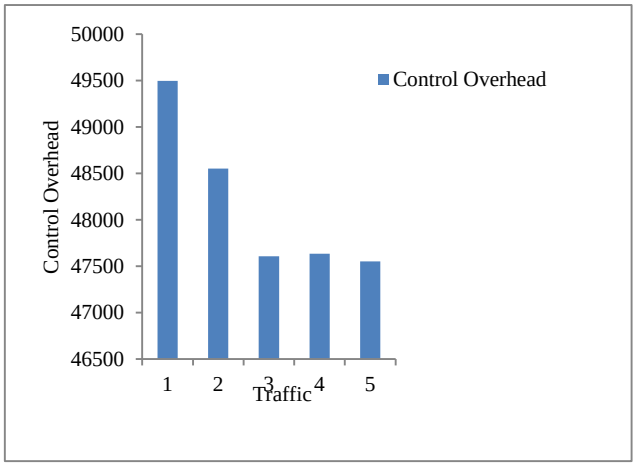

Fig. 3: Traffic vs. Control Overhead

In Fig. 4 delay is shown which is changes in data transmission time from source to destination. In Fig. 5 Average energy consumption is shown with increase in traffic. It is not affected much more and hence average residual energy is showing better results. As shown in Fig.6, jitter is improved with increase in traffic and Fig. 7 shows better improvement in throughput with increased in traffic. The proposed protocol is scalable with respect to traffic. It identifies SSDF attacker and eliminates it from network thereby improving network performance.

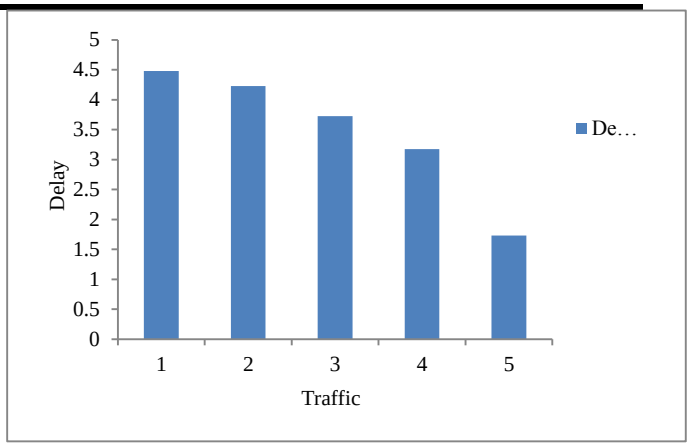

Fig. 4: Traffic vs. Delay

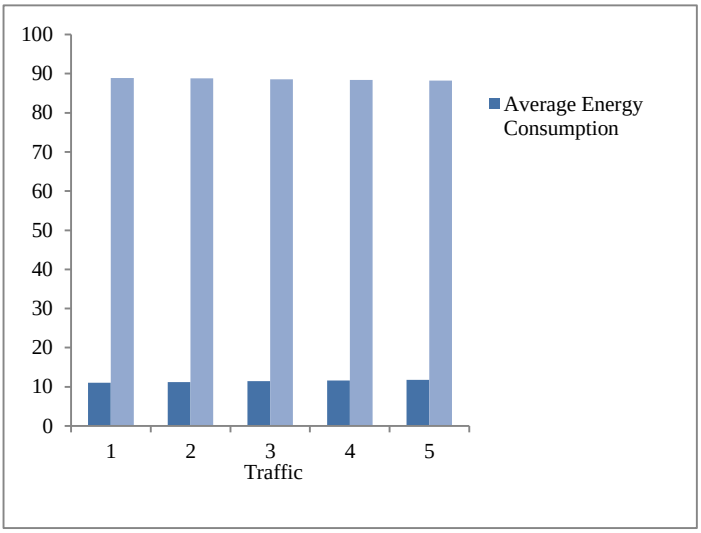

Fig. 5: Traffic vs. Average Energy consumption and Average Residual energy

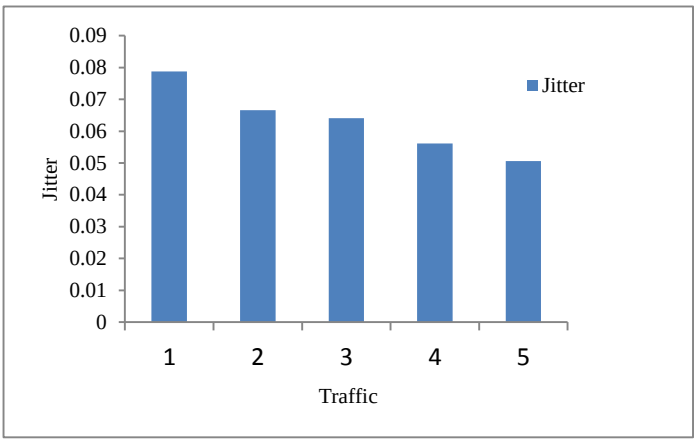

Fig. 6: Traffic vs. Jitter

https://dx.doi.org/10.22161/ijaers.4.4.20 *ISSN: 2349-6495(P) | 2456-1908(O)*

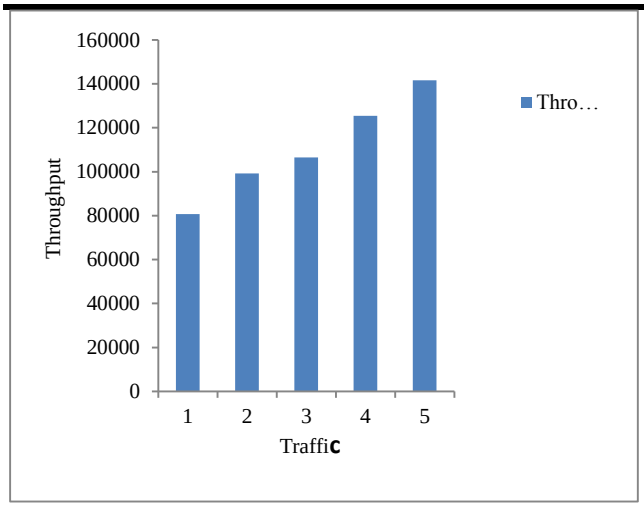

Fig. 7: Traffic vs. Throughput

VI. CONCLUSION

In this paper, we have proposed protocol which implements SSDF attack. The proposed protocol accurately detects the SSDF attacker and isolate it from the network. The proposed protocol shows better performance under the parameters considered with increase in traffic. As protocol identifies the SSDF attacker and eliminates it, network performance is not very much affected with increase in traffic.

REFERENCES

[1] J. Mitola and G. Maguire.: 'Cognitive radio: making software radios more personal' ,IEEE Personal Communications, Aug 1999,Mag., vol. 6, no. 4, pp. 13-18

[2] L. Li, F.W. Li, and J. Zhu. "A method to defense against cooperative SSDF attacks in Cognitive Radio Networks." IEEE International Conference on Signal Processing, Communication and Computing, pp. 1-6, 2013

[3] I. F. Akyildiz, W. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," Computer Networks, vol. 50, 2006, pp. 2127-2159.

[4] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," IEEE Communications Surveys & Tutorials, vol. 11, no. 1, 2009

[5] Saud Althunibat, Victor Sucasas, Hugo Marques, Jonathan Rodriguez, Rahim Tafazolli, and Fabrizio Granelli" On the Trade-Off Between Security and Energy Efficiency in Cooperative Spectrum Sensing for Cognitive Radio" IEEE communications letters, vol. 17, no. 8, August 2013.

[6] Chowdhury Sayeed Hyder, Brendan Grebur, and Li Xiao "Defense against Spectrum Sensing Data Falsification attacks in CR networks." Springerlink, Journal of security and privacyin computer networks. Volume 76, 2012, p.p. 154-171.

[7]] Hong Du, Shuang Fu ,Hongna Chu "A Credibility-based Defense SSDF Attacks Scheme for the Expulsion of Malicious Users in Cognitive Radio" International Journal of Hybrid Information Technology Vol.8, No.9 (2015), pp.269-280.

[8] Saud Althunibat, Birabwa J. Denise and Fabrizio Granelli "A Punishment Policy for Spectrum Sensing Data Falsification Attackers in Cognitive Radio Networks' IEEE 80th Vehicular Technology Conference (VTC Fall) ,14-17 Sept. 2014.

[9] Aida Vosoughi, Joseph R. Cavallaro, Alan Marshall "Robust Consensus-based Cooperative Spectrum Sensing under Insistent Spectrum Sensing Data Falsification Attacks" IEEE Global Communications Conference (GLOBECOM) , 6-10 Dec. 2015.

[10] Linyuan Zhang, Guoru Ding, Fei Song, Qiao Su "Defending Against Byzantine Attack in Cooperative Spectrum Sensing Relying on a reliable Reference" IEEE/CIC International Conference on Communications in China (ICCC), 27-29 July 2016.

[11] Ji Wang, Ing-Ray Chen, Jeffrey J.P. Tsai, Ding-Chau Wang "Trust-based Cooperative Spectrum Sensing Against SSDF Attacks in Distributed Cognitive Radio Networks" IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR 2016), 10-12 May 2016.

[12] CAO Long, ZHAO Hangsheng, ZHANG Jianzhao, LIU Yongxiang2 "Secure cooperative spectrum sensing based on energy efficiency under SSDF attack" IEEE International Wireless Symposium (IWS 2015), 30 march-1 April 2015.

[13] Sasa Maric, Sam Reisenfeld, Leonardo Goratti " A Simple and Highly Effective SSDF attacks Mitigation Method" IEEE 10th International Conference on Signal Processing and Communication Systems (ICSPCS), 19-21 December 2016.

[14] Abbas Ali Sharifi, Mir Javad Musevi Niya "Defense Against SSDF Attack in Cognitive Radio Networks: Attack-Aware Collaborative Spectrum Sensing Approach", IEEE Communications Letters, VolL. 20, N0. 1, January 2016.

[15] Saud Althunibat, Birabwa Joanitah Denise, Fabrizio Granelli " Identification and Punishment Policies for Spectrum Sensing Data Falsification Attackers Using Delivery-Based Assessment" IEEE Transactions On Vehicular Technology, Vol. 65, No. 9, September 2016.