ISSN: 2321-7782 (Online)
e-ISJN: A4372-3114
Impact Factor: 6.047

Volume 5, Issue 9, September 2017

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Estimating the Performance of CSS Cognitive Radio Networks by Detection and Elimination of an Attacker

Rajesh D. Kadu[1]
Research Scholar
SGB Amravati University
Amravati – India

Dr. Pravin P. Karde[2]
Information Technology Department
Government Polytechnic
Amravati – India

Dr. V. M. Thakare[3]
P. G. Department of Computer Science
SGB Amravati University
Amravati – India

Abstract: Cooperative spectrum sensing (CSS) is more reliable and accurate than individual spectrum sensing (ISS) by cognitive radio (CR). The ISS scheme often experiences the signal fading and shadowing because of low received signal strength (RSS). CR technology solves the spectrum shortage problem and improves spectrum utilization by allowing the sensing of vacant spectrum band and using it. The successful deployment of cognitive radio networks (CRNs) with meeting the quality of service can be possible if its security problems are resolved. The CRNs are more vulnerable to many attacks and threats than conventional wireless radio networks (WRNs) because of intrinsic nature of CR devices. The major attacks that degrade the performance of CRNs are primary user emulation attack (PUEA), spectrum sensing data falsification (SSDF) attack and jamming attack. The malicious users in network launch these attacks. In this paper, we estimate the performance of protocol which identifies and eliminates an attacker. The simulation results show that protocol performs better with increased network size.

Keywords: PUEA; SSDF attack; jamming attack; CSS; CR.

I. INTRODUCTION

The spectrum demand is increasing greatly due to ever growing wireless applications. The most of the spectrum in various countries is statically allocated. However, it is observed that, the allocated spectrum remains underutilized [1]. The several bodies for the regulation of spectrum such as Federal Communication Commission (FCC), Electronic Communications Committee (ECC) and ITU world radio conference (WRC) have defined several frequency bands as unlicensed bands. For example, Industrial Scientific and Medical (ISM) band of 2.4 GHz was initially given for Radio LANs use. In the same manner, U-NII systems use several unlicensed bands in the 5GHz spectrum as regulated by FCC or WRC [2]. In September 2010, FCC has agreed on new regulation which allows the unlicensed users to use spectrum allocated for wireless broadband services (300 MHz and 400 MHz) to fulfill the increasing demand of spectrum. The Cognitive Radio Networks (CRNs) technology allows using unused spectrum to solve the spectrum shortage problem [3].

If primary user (PU) does not use allocated spectrum band and remains vacant then it is a spectrum hole. The Cognitive Radio (CR) device can sense the spectrum to search the vacant band also called as spectrum holes or white spaces. The deployment of CRNs can be only successful if its security problems are resolved. The attacks and threats in CRNs are different than conventional wireless networks (WRNs) due to intrinsic nature of CR devices. There are many attacks that can be launched by malicious users (MUs) in network. These are primary user emulation attack (PUEA), spectrum sensing data falsification (SSDF) attack and jamming attack.

II. Related Work

Prior works employ different strategies to improve the security of CRNs in cooperative spectrum sensing process. In [4], authors proposed the cooperative localization method to estimate the location of primary transmitter. This approach is proposed for identification primary user emulation attacks in IEEE 802.22 networks. The nodes of the CRNs cooperate with each other and based on their measurements, the base station (BS) performs time base location estimation of primary transmitter. The proposed approach can handle only primary transmissions with known locations. In order to detect emitter positions cooperatively, Time Difference of Arrival measurements (TDoA) are used. Ozge Cepheli and Gunes Karabulut Kurt [5] used trust factor for the detection of PUEA. In this proposed approach, the trust factor is used to detect attacker and beamforming approach based solution used as a defense against attack. The spectrum sensing mechanism of the attacker is blocked using trust factor. The guard agents are used towards malicious user to generate artificial noise so that attacker will not be able to search any available spectrum.

Mohammad Javad Saber and Seyed Mohammad Sajad Sadough [6] proposed approach in which attacker's fusion center (FC) is maintained and it combines the spectrum sensing information of many smart PUEA attackers. The attackers operate based on the decision taken by this FC on the basis of collected information from attackers. The approach aims at maximizing the ratio of received power to interference and noise (CSINR) by combining sensing outcomes of different CR users at FC. In [7], authors proposed improved PUEA detection by combining energy detection and localization. The approach uses multiple thresholds for detection of received energy level. The global decision about presence or absence of PU is taken by majority of participating secondary users (SUs). The time difference of arrival (TDOA) localization approach is combined with energy detection for the detection of stationary PU.

D. Teguig et al. [8] proposed quantized three-bit combination scheme for data fusion at FC in CSS process. The authors compared the performance of soft, hard and quantized fusion schemes. Although the soft fusion scheme does better than hard fusion scheme, it requires more bandwidth for control channel. The detection performance of hard fusion is lower than soft fusion and requires less bandwidth. The proposed quantized fusion scheme takes the advantages of both hard and soft fusion schemes. Saud Althunibat et al. [9] proposed punishment policy for the SSDF attackers based on majority based assessment and delivery based assessment. The policy eliminates the attackers and scheduling priority is assigned to SUs. If data is successfully delivered then based on delivery, FC takes the correct decision about spectrum availability due to sensing of SU.

. Ji Wang et al. [10] proposed data fusion scheme against SSDF attack based on trust which identifies the erroneous reports of spectrum sensing due to low sensing capabilities of SUs. These reports then decoupled from false reports due to attackers. Linyuan Zhang et al. [11] proposed the novel and reliable defense reference against SSDF attack. This scheme takes the advantage in combination of both the cognitive process of spectrum sensing and its access in closed loop manner. The proposed reference is reliable and performs better. In [12], Roberto Di Pietro and Gabriele Oligeri proposed anti-jamming approach which is suitable in broadcast communication. The proposed approach dynamically pairs the nodes in network to forward the message just like unicast communication. This communication appears to be like delayed broadcast. In this communication, message gets delivered although one frequency band is jammed as frequency band for delivery gets changed.

In [13], authors considered multiple uncoordinated jammers and independent Rayleigh flat-fading propagations to study the jamming attack. The anti-jamming performance is analyzed by using markov model of CRN transmission. CRNs are more vulnerable to jamming attack in spectrum sensing process. In [14] authors considered the spectrum sensing and jamming detection in combined manner and modeled the problem with multiple hypothesis testing. Authors considered the scenario without knowledge of jammer's signal and noise power. For these both scenarios, correlated GLRT solution is discussed. In

[15], authors considered the database driven CRNs where secondary users (SUs) obtain white space information by submitting location based query to white space database. The jammer can carry out using this channel availability information from submitted queries. The jDefender framework is proposed to infer the probability of user being a jammer by observing jamming events and accordingly applying the anti-jamming strategies.

The remaining paper is organized as follows. Section III explains cooperative spectrum sensing, Section IV presents various attacks in CRNs. Section V Simulation Environment and Result Analysis, Section VI concludes the paper.

III. Cooperative Spectrum Sensing

In cooperative spectrum sensing (CSS) several secondary users (SUs) sense the spectrum to know it is vacant or not. If primary user (PU) is not using the spectrum then secondary user can use it. In CSS, all the SUs involved in spectrum sensing sends the results of spectrum sensing to fusion center (FC). The FC then applies the data fusion rules to take decision whether spectrum is available or not. This decision is then broadcasted to all the SUs involved in spectrum sensing. The CSS is more reliable and accurate than individual spectrum sensing (ISS) by each SU or CR user. The ISS scheme often experiences the signal fading and shadowing because of low received signal strength (RSS). Although, the CSS scheme is more preferable, it is also prone to many security threats and attacks. Primary user emulation attack (PUEA), spectrum sensing data falsification (SSDF) attack and jamming attack is more common in CRNs. If these attacks are launched by malicious user (MU) or group of MUs then it degrades performance of the CRNs. Fig. 1 shows CSS Scheme.

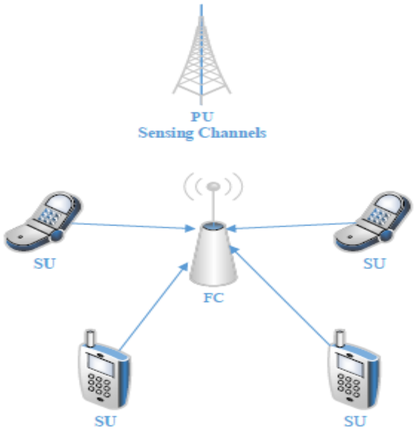

Fig. 1. Cooperative Spectrum Sensing

IV. Attacks in CSS

The CRNs are more vulnerable to attacks and threats than conventional wireless radio networks (WRNs) because of intrinsic nature of CR devices. The major attacks that can be launched in CRNs are primary user emulation attack (PUEA), spectrum sensing data falsification (SSDF) attack and jamming attack. The performance of the CRNs gets degraded in presence of these attacks. It is necessary to identify the attackers so that they can be eliminated from networks.

A. Primary User Emulation Attack (PUEA)

The PUEA is the great threat to spectrum sensing. In this attack, the attacker CR node transmits the signals similar to primary user's signals so that other good secondary users (SUs) can be forced to believe that it is genuine PUs signals. Hence, good SUs may vacate the spectrum which then can be used by attackers. There are two types of PUEA that can be launched by attackers. In selfish PUEA, attackers aim is to use the vacant spectrum bands preventing the other good SUs to use it. In malicious PUEA, attackers aim is to block the other good SUs from using the spectrum so that there will be denial of service for them.

B. Spectrum Sensing Data Falsification (SSDF) Attack

In CSS process, all the SUs involved in spectrum sensing sends results of spectrum sensing to fusion center (FC). FC then takes decision about presence or absence of PU based on these received results from SUs. For this purpose, FC executes data fusion scheme. In order to affect the decision process of FC, some of the malicious users (MUs) send false reports to FC called as SSDF attack.

C. Jamming Attack

Jamming attack blocks the channels so that communication between genuine SUs and FC can be blocked. This attack is launched by jammers or attackers by sending bogus packets over communication channels. Jamming attack can be launched at both physical and MAC layer. In MAC layer, common control channel (CCC) is blocked by jammers. The CCC is used by SUs to send control packets and it supports for finite number of users at the same time.

V. Simulation Environment and Result Analysis

The attacks discussed above degrade the performance of network. The proposed protocol detects and eliminates the attackers of above attacks. The proposed protocol is tested in NS-2 environment and its performance is measured by considering the parameters as packet delivery ratio (PDR), dropping ratio, control overhead, throughput and jitter. These parameters are tested against increasing network size. The total time used for simulation is considered as 200 seconds with packet size of 512 bytes. The number of users considered for simulation is 50 and initial energy for each node is considered as 100 Jules. By considering all other optimal parameters, following results are obtained at FC.

The results show better network performance although network is occupied with attacks like PUEA, SSDF attack and jamming attack. As protocol identifies and eliminates the attacker, more channel quality becomes available to SUs of network. Fig. 2 shows results for PDR and dropping ratio for different size of networks. The PDR is better for increasing size of network and hence dropping ratio shows the results accordingly. This is because the protocol reduces flooding thereby avoiding the collision.

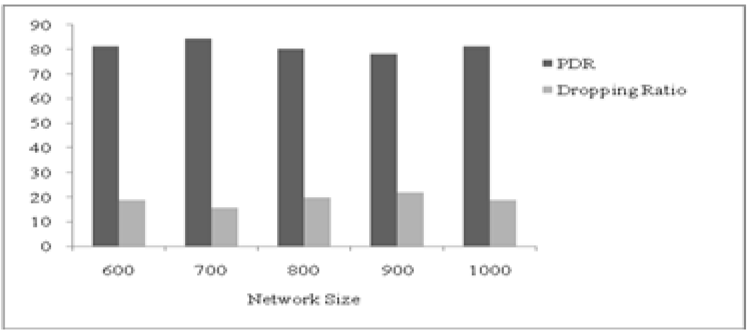

Fig. 2. PDR and Dropping ratio for increasing network size

Fig. 3 shows the number of control packets required to find correct path from source to destination. As size of network increases, the number of control packets decreases.

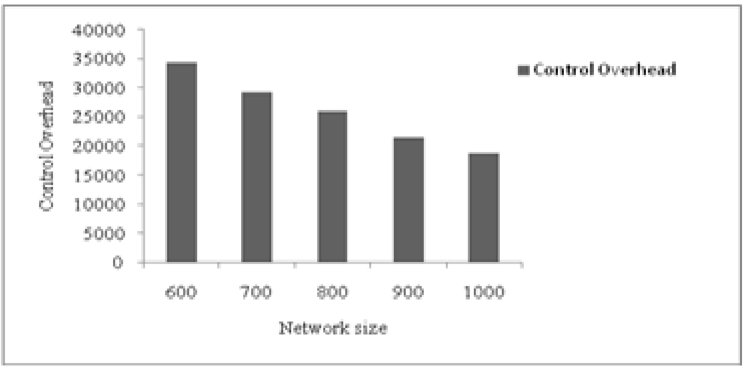

Fig. 3. Control overhead for increasing network size

Throughput is number of bits delivered per second. As shown in fig. 4, throughput does not affect much more with increasing size of network. Fig. 5 shows jitter for different network size.

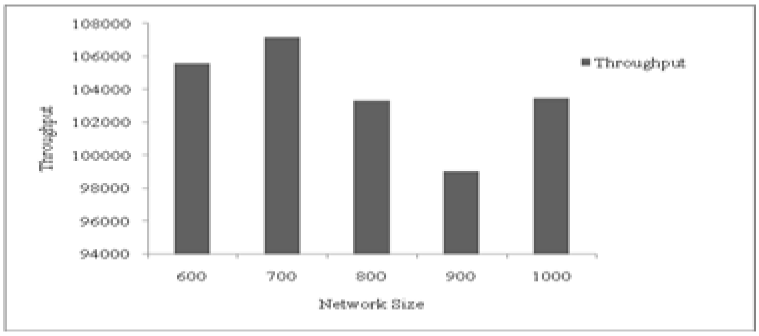

Fig. 4. Throughput for increasing network size

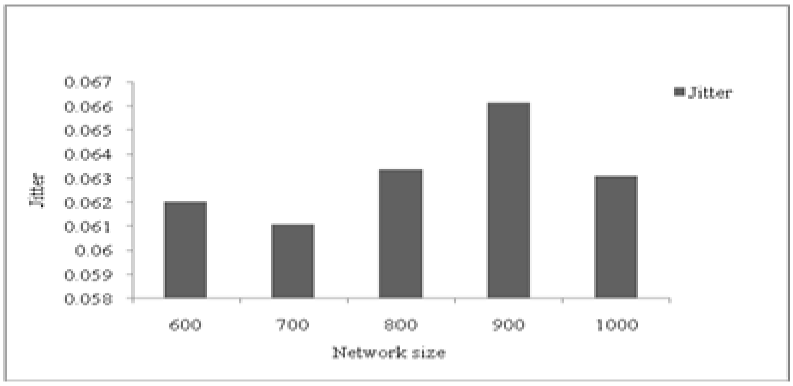

Fig. 5. Jitter for increasing network size

VI. Conclusion

In this paper, we discussed the CSS scheme and various attacks that can be launched in CRNs. Although, CSS scheme is better alternative to ISS scheme due to its accuracy and reliability, it is vulnerable to many attacks. The attacks in CRNs degrade the network performance. Hence, it is necessary to identify and eliminate the attacker. The proposed protocol identifies and eliminates the attacker and hence, improves the network performance. The simulation results show the good network performance.

References

1. Y.Liang, Y.Zeng, E.Peh and A.Hoang, “Sensing throughput trade off for cognitive radio networks”, IEEE Transactions on Wireless Communications, vol.7, issue 4, pp. 1326-1337, April 2008.

2. S. Arkoulis, L. Kazatzopoulos, C. Delakouridis and G.F. Marias “Cognitive Spectrum and its Security Issues” Proceeding of the second IEEE international conference on Next Generation Mobile Applications, Services and Technology (NGMAST’08), pp. 565-570, 16-19Sept 2008.

3. Wassim El-Hajj, Haidar Safa and Mohsen Guizani, "Survey of Security Issues in Cognitive Radio Networks" Journal of Internet Technology, vol. 12, no. 2, pp. 181–198, 2011.

4. Olga Leon, Juan Hernandez-Serrano and Miguel Soriano, “Cooperative detection of primary user emulation attacks in CRNs" Elsevier, Computer Network journal, vol. 56, issue 14, pp. 3374-3384, Sept 2012.

5. Ozge Cepheli and Gunes Karabulut Kurt "Physical Layer Security in Cognitive Radio Networks: A Beamforming Approach" IEEE 2013 First International Black Sea Conference on Communications and Networking (BlackSeaCom), 3-5 July 2013.

6. Mohammad Javad Saber and Seyed Mohammad Sajad Sadough "Robust Cooperative Spectrum Sensing in Cognitive Radio Networks under Multiple smart Primary User Emulation Attacks" 22nd Irani conference on Electrical Engineering, (ICEE 2014), 20-22 May 2014.

7. Fan Jin, Vijay Varadharajan and Udaya Tupakula, “Improved Detection of Primary User EmulationAttacks in Cognitive Radio Networks” IEEE international conference on Telecommunication Networks and Applications, Sydney, NSW, Australia, 18-20 Nov 2015.

8. D.Teguig, B.Scheers, and V.Le Nir, “Data Fusion Schemes for Cooperative Spectrum Sensing in Cognitive Radio Networks” IEEE Military Communications and Information Technology, Gdansk, Poland, 8-9 Oct 2012.

9.]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.

10. 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.

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

12. Roberto Di Pietro and Gabriele Oligeri “Jamming Mitigation in Cognitive Radio Networks” Published in: IEEE Network, vol. 27, issue 3, pp. 10-15, May-June 2013.

13. Wednel Cadeau and Xiaohua Li, “Anti-Jamming Performance of Cognitive Radio Networks under Multiple Uncoordinated Jammers in Fading Environment” IEEE 46th Annual Conference on Information Sciences and Systems (CISS 2012), Princeton, NJ, USA, 21-23 March 2012.

14. Jafar Mohammadi, Sławomir Sta´nczak and Meng Zheng “Joint Spectrum Sensing and Jamming Detection with Correlated Channels in Cognitive Radio Networks” IEEE International Conference on Communication Workshop (ICCW), 8-12 June 2015.

15. Haojin Zhu, Chenliaohui Fang, Yao Liu, Cailian Chen, Mengyuan Li, and Xuemin (Sherman) Shen “You Can Jam But You Cannot Hide: Defending Against Jamming Attacks For Geo-Location Database Driven Spectrum Sharing” IEEE Journal On Selected Areas In Communications, vol. 34, no. 10, October 2016.