A Survey on Prevention of the Falsification Attacks on Cognitive Radio Networks

Pratibha¹, Sharmelee Thangjam², Naresh Kumar³, Sanjiv Kumar⁴

¹,²,³,⁴ University Institute of Engineering & Technology, Panjab University Chandigarh 160023, India

¹ singh.pratibha2901@gmail.com ² thangjam@pu.ac.in ³ naresh_uiet@yahoo.com ⁴ sanjivsam86@gmail.com

Abstract: Today is the era of intelligent cognitive radio network technology that allows the utilization of available spectrum efficiently by allocation of the spectrum dynamically to unlicensed users. The technology utilizes the free spectrum bands which are not being used by the authorized users without causing any obstruction to the existing transmission. Cognitive radio technology promises interference free spectrum access by users. However, there exist many security attacks on spectrum impacting on spectrum access probability and network services. This will result in significant degradation of the performance of a cognitive radio network. This paper discusses the several attacks on different layers, their motives and various mechanisms to prevent them. The specific threats based on issues with configurability are explored on the basis of the related work. In this paper the role of authentication mechanism to prevent the attacks for hassle free spectrum utilization and its performance in resolving the cognitive network security issues are discussed. The need for effective sensing and decision mechanisms to enhance the security of cognitive networks is demonstrated in the paper. Hence, the presented paper gives an overview of existing research efforts at first and secondly, the research challenges are identified that can address the ways to secure the cognitive radio network and lastly the countermeasures in cognitive radio network security strategies are demonstrated.

Keywords: Cognitive Network; Primary User; Secondary User; Primary User Emulation Attack; Spectrum Sensing falsification Attack; Authentication, Network security

1. Introduction

Cognitive radio technology [1-5] is the strategy applied to wireless communication to make efficient utilization of spectrum. This strategy is an intelligent way to access the spectrum as it can learn from its environment by analyzing spectrum and make decisions by adaptation of operating parameters. Due to
the dynamic access feature of cognitive radio networks the secondary users are able to access spectrum whenever the vacant spectrum is available without interference to primary users. The initial step is to sense the spectrum available. Further steps are spectrum decision making, spectrum management, and spectrum mobility[6]. The network is vulnerable to various attacks on spectrum sensing and policy protocols[7] which lead to disturb functionality of cognitive radio technology. Cognitive radio must be secure to use for an efficient working mechanism throughout so security challenges need to be addressed. Primary user emulation attack is discussed in [1][7][8] in which primary users are mitigated by malicious users which sends wrong information about spectrum to secondary users in the queue. The change in decision rule strategies is proposed as a natural defence mechanism[9][10][11]. This defence strategy makes decisions with the help of secondary users sensing reports which they gather from their neighbours. The spectrum sensing data falsification (SSDF) attack is discussed in[12] which false spectrum sensing data is transmitted to a data collector having impact on decision making. In, the defence mechanism based on public key cryptography[13] is proposed in which PU is authenticated by appending signature provided to PU signal. Authentication with tags to the primary users is a better perspective. CRN technology should provide integrity, confidentiality and authenticity to the users[14]. In this paper a survey on security attacks on basis of user’s categorization and its countermeasures for these attacks is demonstrated. The shortcomings of current security mechanisms[15] are discussed from the literature review. The detection methods and countermeasures are discussed. Challenges and future perspectives which can improve the security of cognitive radio networks are presented.

2. Cognitive radio: An Overview
Cognitive radio follows a methodology to spectrum utilization[16] in appropriate manner. The cognitive radio network works on a particular format. The figure 1 demonstrates the functions of cognitive radio and the features on which the cognitive radio network relies.

- Spectrum sensing: to sense the available spectrum in the radio frequency environment
- Spectrum management: to select the available channels on basis of signal strength, efficiency etc[17].
- Spectrum sharing: to share the spectrum bands of the licensed-band users with the unlicensed users[17].
- Spectrum mobility: to allow the cognitive-radio user to vary its feature operational frequency[18].

2.1. Categorization of users in cognitive radio network
- Primary users (PUs): the licensed users who can operate in a prescribed frequency band of spectrum accessing of the primary base station.
- Secondary users (SUs): the unlicensed users who are allowed to access when the primary user is not using its spectrum band.
2.2 Spectrum Sensing Techniques
The literature review discussed the various sensing algorithms on the basis of features. Feature Detection: Features of the spectrum are considered according to several signal parameters, cyclostationary parameters modulation parameters etc. The problem in this feature detection spectrum sensing mechanism is large delay in decision due to high complexities in signal processing. Switching detection: This is a stochastic process based on samples distribution and analysing the changes. Drawback is that false sensing information may be provided by users to the decision centre.

2.3 Functionalities of Cognitive Radio Network
The functionalities of various layers of cognitive radio network are discussed in literature. Figure 2 represents functionalities of main layers of cognitive radio network.

![FIGURE 2. Functionalities of Layers of Cognitive Radio](image)

3. Cognitive Radio Network Attacks
Huge demand of wireless network services has increased difficulties in its security aspect. Although due to the nature of CRN and its critical applications, it is vulnerable to most of the security threats. Specific threats based on issues with configurability such as attack on the data due to malicious node presence, attacks on networks affecting functioning of network, attacks by inducing malicious software and having access to data, attacks on services e.g. flooding, jamming of spectrum etc., attacks on user’s identity by emulating as users to get access of spectrum e.g. PUEA, SSDF. The need to address the security issues in cognitive radio networks is necessary to make the network efficient. Attacks are threats to the security that disrupt the efficiency of the spectrum and affect the users in many ways.

3.1 Primary User Emulation Attack
In primary user emulation attack the secondary users are misguided by attackers that mimic as primary user and it prevent them to access the vacant channels with the false sensing information [7][16] leading to wrong decisions and SUs left the access to the channel. PUE attacks are to be considered as it affects greatly the spectrum sensing process[19].
3.2. Spectrum Sensing Data Falsification Attack (SSDF)

In this type of attack the malicious users affects the fusion centre decision making process by sending false information regarding spectrum and it results in rise of false alarm probability which will decrease the throughput of an honest secondary user. This is important attack strategy need to be addressed to achieve right decision policy. It is basically a belief manipulation attack as it is caused by manipulation of parameters by malicious users degrades the decision ability of the decision centre. SSDF attack is further classified according to behaviour of malicious users[20]. The attacks are investigated in view of secondary user’s reliability on the basis of threshold choices. Security in the context of functionalities of various layers is the measure, intended to protect information and information systems by ensuring their availability, integrity and confidentiality. The SSDF attacks impact on availability and integrity of cognitive radio networks. Layer based security mechanism is a more effective way. The measurement of the authenticity of SU’s on the basis of evidence theory significantly reduces the collaboration[11][14]. The effective SSDF attack defence mechanism depends on the balance between equipment cost and proposition applied, authentication, and non-repudiation. The system must authenticate the identity, permissions, integrity of any entity. The malicious users identified with delivery based schemes improving the decision making capability of decision making. Security breaches also greatly increase with load of services. The detection of attacks improves with the development of frameworks. The cluster based mechanism is less complex for detecting malicious users in each cluster [14][18]. The reliable cluster is found and authentication of users is done. The goal of attackers is analysed from the behaviour with which it approaches helps in avoiding the other factors and easily judge the intention of users. Trust based framework makes easy implementation of security mechanisms[11][20][21]. The trust values of the users a key for evaluation of trustworthiness[8]. The approach is based on periodic scanning of the network that monitors and observes the malicious users. The reliability value is measured of the users with an optimal threshold consideration in case of Spectrum flooding to prevent jamming[14]. The learning techniques can be used to make intelligent security systems for cognitive radio. Cryptography effectively utilized for authentication of primary and secondary users ensures confidentiality of cognitive radio[16]. The fingerprinting and game theory also utilized for authentication[13]. Table 1 and 2 shows the layer based categorization of security attacks.

| Sr. no. | Author’s name | Proposed algorithm | Security attacks | Authentication |
|---------|---------------|-------------------|-----------------|---------------|
| 1       | Liu et al[11] | Mechanism based on determining cognitive trust value | PUEA and SSDF attacks | User identity authentication and providing the authentic tag to the honest users |
| 2       | Chang et al[15] | Authentication of spectrum sensing results by data collector and data fusion scheme | Detection of Spectrum sensing data falsification (SSDF) | Data analysis with knowledge base approach machine learning |
| 3       | Xie et al[19] | Physical layer network coding | Primary user emulation attack (PUEA) | Hashing function to judge trustworthy senders |
| 4       | Ghaznavi et al[22] | Game theory scheme | Primary user emulation attack (PUEA) | Clustering scheme game theory implemented in every cluster to identify malicious user |
| 5       | Yadav et al[23] | Delivery based Scheme | SSDF attack | Check on sensing mechanism |
| Sr.no. | Layer          | Attack and its Effects                                                                 | Countermeasures                                                                 |
|-------|----------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| 1.    | Physical Layer | Jamming - affects sensing                                                             | Escape the denial of service, changing the spatial location[2] of legitimate user, Periodic scanning and cyclostationary parameters metrics.[24][25] |
|       |                | PU Emulation - affects PU detection                                                   | Cryptographic authentication, game theory[8], biometric techniques[14], game theory |
|       |                | Overlapping SU                                                                        | Trust approach.                                                                  |
|       |                |                                                                                       |                                                                                   |
| 2.    | Data Link layer| SSDF- affects spectrum decision                                                        | User’s authentication[7], reliability score identification of SU’s.               |
|       |                | Common Control Channel jamming                                                       | Trust node detection mechanism[14].                                              |
|       |                | Common Control Channel saturation                                                     |                                                                                   |
| 3     | Network layer  | Hello flood - affects routing                                                         | Symmetric key cryptographic approach[4]                                           |
|       |                | Tear drop- IP datagram fragmentation                                                  | Cyclostationary parameters based routing protocols[26].                           |
|       |                | Sinkhole-affects routing                                                              |                                                                                   |
|       |                | Sybil -affects host addressing                                                        |                                                                                   |
|       |                | Wormhole -affects routing                                                             |                                                                                   |
| 4     | Transport Layer| Key depletion- data, services and protocol                                             | Cryptographic algorithm[8] implementing cryptographic signature for authentication |
| 5     | Application layer | Malicious software injection- effects decisions                                       | Game theory[27] based on greedy approach build for malicious users recognition   |
|       |                | Policy attacks-effects quality of services                                            |                                                                                   |
| 6     | Cross-Layer    | Jelly fish - affects network mechanism                                                | Environment detection mechanisms [16]                                             |
|       |                | Lion attack - affects transmission control protocol                                    |                                                                                   |
|       |                | Routing information jamming                                                           |                                                                                   |
4. Future Perspectives to prevent attacks
   From the studied literature there are several countermeasures to prevent the attacks depending on the
   type of attack are summarized and shown in figure 3:
   • Implementation of authenticated protocols[6].
   • Authenticated servers, authenticating users and nodes authentication[8].
   • Periodic and sequential scanning[10].
   • Implementation of machine learning based techniques[13].
   • Intelligent decision making[14].
   • Establishing trusted framework[16].
   • Utilization of optimized spectrum sensing[20].
   • Implementing security architecture.
   • Periodic updating of software[25].
   • Considering sensing results and user behaviour in decision making[27].

   ![Security Solutions for Cognitive Radio Network](image)

   FIGURE 3. Security Solutions for Cognitive Radio Network

5. Conclusion
   The detection and prevention of attacks in an efficient manner is essential for development of secure
   mechanism for cognitive radio networks. The security at each layer is important for proper functionality
   of the network. The studied literature summarizes that security of cognitive networks helps in making
   spectrum utilization a more reliable resource. The various spectrum attacks and their effects are analysed
   and moreover their countermeasures are demonstrated. The conclusion is that the smart framework is
   needed to secure the process of cognitive radio network at every stage. Intelligent sensing and decision
   protocol to resolve the security issues can be implemented with knowledge-based approach. The reliability
   measure of users is important in security mechanisms. Authentication of users using cryptography techniques, fingerprinting and game theory are the best approaches. In future perspective
   the standardized framework for secure cognitive radio network can be implemented by experts to meet
   the security challenges of cognitive radio network and with low cost solution.
6. References

[1] Salahdine F. and Kaabouch N., 2020, Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey, *Phys. Commun.*, vol. 39, pp. 101001.

[2] Gurney D., Buchwald G., Ecklund L., Kuffner S., and Grosspietsch J., 2008, Geo-location database techniques for incumbent protection in the TV white space, *2008 IEEE Symp. New Front. Dyn. Spectr. Access Networks, DySPAN 2008*, pp. 232–240.

[3] Jianming Z., Fan L., and Quiyuan L., 2014, Data fusion based on node trust evaluation in wireless sensor networks, *J. Sensors*, vol. 2014.

[4] Sun Z., Xu Z., M. Z. Hammad, Ning X., Wang Q., and Guo L., 2019, Defending against massive SSDF attacks from a novel perspective of Honest Secondary Users, *vol. 7798, Vol. no. 2*, pp. 1–4.

[5] Feng J., Zhang Y., Lu G., and Zheng W., 2015, Securing cooperative spectrum sensing against ISSDF attack using dynamic trust evaluation in cognitive radio networks, *no. March, pp. 3157–3166*.

[6] Akyildiz I.F., Lee W., Vuran M.C., and Mohanty S., 2008, AND N ETWORKS A Survey on Spectrum Management in Cognitive Radio Networks, *Vol. no. April, pp. 40–48*.

[7] Jain S., M. Hussain, and R. M. Garimella, 2016, Primary User Authentication in Cognitive Radio Network using Authentication Tag, *pp. 1–5*.

[8] Bhattacharjee S., Sengupta S., and Chatterjee M., 2013, Vulnerabilities in cognitive radio networks: A survey, *Comput. Commun.*, vol. 36, no. 13, pp. 1387–1398.

[9] Al-Mathehaji Y., Boussakta S., Johnston M., and Fakhrey H., 2017, Defeating SSDF Attacks With Trusted Nodes Assistance in Cognitive Radio Networks, *IEEE Sensors Lett.*, vol. 1, no. 4, pp. 1–4.

[10] Rawat A.S., Anand P., Chen H., and Varshney P.K., 2011, Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks, *vol. 59*, no. 2, pp. 774–786.

[11] Yu H., Liu S., Kot A.C., Miao C., and Leung C., 2011, Dynamic Witness Selection for Trustworthy Distributed Cooperative Sensing in Cognitive Radio Networks.

[12] Ahmadfard A., Jamshidi A., and Keshavarz-Haddad A., 2017, Probabilistic spectrum sensing data falsification attack in cognitive radio networks, *Signal Processing*, vol. 137, pp. 1–9.

[13] Thilina M. and Gamacharige K., 2015, On Spectrum Sensing, Resource Allocation, and Medium Access Control in Cognitive Radio Networks Madushan Thilina Karaputugala Gamacharige The University of Manitoba.

[14] Jianming Z., Fan L., and Quiyuan L., 2016, Retracted: Data Fusion Based on Node Trust Evaluation in Data Fusion Based on Node Trust Evaluation in Wireless Sensor Networks, *vol. 2014*.

[15] Wang H., Li Y., and Chang T.C., 2018, An enhanced cooperative spectrum sensing scheme for anti-SSDF attack based on evidence theory, *Microsyst. Technol.*, vol. 24, no. 6, pp. 2803–2811.

[16] Soto J. and Nogueira M., 2015, A framework for resilient and secure spectrum sensing on cognitive radio networks, *Comput. NETWORKS*, vol. 79, pp. 313–322.

[17] Mardini W., Khamayseh Y., and Al-Zaro S.J., 2018, Spectrum management in cognitive radio networks,” *ICIC Express Lett. Part B Appl.*, vol. 9, no. 9, pp. 887–898.

[18] In O., 2012, Spectrum Mobility in Cognitive Radio Networks, pp. 114–121.

[19] Xie X., Wang W., and. Charlotte U.N.C., 2013, Detecting Primary User Emulation Attacks in Cognitive Radio Networks via Physical Layer Network Coding, *Procedia - Procedia Comput. Sci.*, vol. 21, pp. 430–435.

[20] Parvin S., Khadeer F., and Khadeer O., 2013, Conjoint trust assessment for secure communication in cognitive radio networks, *Math. Comput. Model.*, vol. 58, no. 5–6, pp. 1340–1350.

[21] Zhao F., Li S., and Feng J., 2019, Securing Cooperative Spectrum Sensing against DC-SSDF
[22] Ghaznavi M. and Jamshidi A., 2019, A low complexity cluster based data fusion to defense against SSDF attack in cognitive radio networks, *Comput. Commun.*, vol. 138, no. February, pp. 106–114.

[23] Yadav K., Dhar S., and Sumit R., 2020, Defense Against Spectrum Sensing Data Falsification Attacker in Cognitive Radio Networks, *Wirel. Pers. Commun.*, pp. 0123456789.

[24] Magdalene A.H.S. and Thulasimani L., 2017, Analysis of Spectrum Sensing Data Falsification (SSDF) Attack in Cognitive Radio Networks: A Survey, vol. 2017, pp. 89–100.

[25] Cui J., Wang M., Luo Y., and Zhong H., 2019, DDoS detection and defense mechanism based on cognitive-inspired computing in SDN, *Futur. Gener. Comput. Syst.*, vol. 97, pp. 275–283.

[26] Omer A.E., 2015, Review of Spectrum Sensing Techniques in Cognitive Radio Networks, pp. 439–446.

[27] Spyridopoulos T., Karanikas G., Tryfonas T., and Oikonomou G., 2013, A game theoretic defence framework against DoS / DDoS cyber attacks, *Comput. Secur.*, pp. 1–12.