IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, April 2022
Impact Factor: 6.252

A Safe Cognitive Radio Spectrum Handoff Method Using Coordinating Cognitive User

Mrs. T. G. Dhaarani1, Chandru D.[2], Harini V.G.[3], Madhumitha G. S.[4]
Assistant Professor, Department of Electronics and Communication Engineering[1]
Final Year Students, Department of Electronics and Communication Engineering[2,3,4]
Nandha Engineering College, Erode, Tamil Nadu, India

Abstract: *A new cognitive user emulation attack (CUEA) in a cognitive radio network (CRN), which could be utilized by intruders during spectrum handoffis introduced. The need for more efficient spectrum utilization in our increasingly digitalized society is becoming more important. This has given raise to the variety of new security threats. A safe handoff mechanism that could successfully counter such an attack by introducing a coordinating cognitive user that computes the level of trust of each cognitive user based on its behavioral characteristics is proposed. Malicious users could be effectively identified by the coordinating cognitive user by looking up the trust values. The activity of the proposed mechanism is validated using MATLAB simulation. The simulation executed describes the utilization of the proposed mechanism by correctly identifying the probability of false detection, detection rate, incorrect detection shown as it decreases the data transmission time or increases the transmission rates of primary user's signals.*

Keywords: Cognitive User Emulation Attack

I. INTRODUCTION

Bandwidth consumption and spectrum usagehave increased significantly in the development of Internet-connected devices and services. Therefore,the available spectrum must be used more efficientlyto meet the growing demand for bandwidth. One such approach is the use of cognitive radio (CR) technology to facilitate spectrum use. Specifically, CRs allow unlicensed or cognitive users (CUs) to use free channels/scopes from basic/licensed users (PUs). The main functions performed by a CR to usethe free spectrum of a PU are spectrum identification, spectrum decision-making, spectrum sharing (access), and spectrum handover (or spectrum mobility).

The first three main features (i.e., Sensing,Decision and Sharing) CUs do not feel the middle, recognize idle channel channels and selects the idle channel among simple bands. The CU avoids interference in the PU and generates a transport channel to the selected strip. The latest key function(i.e., Handoff / Mobility) must switch the current transport channel to another available channel during data transfer and remember the first three main functions. In addition, packet transport, spectrum detection, and PU receipts can also enter additional delays during spectrum transmission.Thus, during spectrum transmission, even amalicious user (MU) can use this delay and simulatelegitimate CU transmission (HCU) to degrade network performance.

Existing handoff mechanisms can be broadly classified into proactive and reactive strategies or engaged and not engaged spectrumstrategies. The engaged spectrum handoff schemes assume that fewer frequency channels are engaged for the PU. Conversely, a handoff scheme without an occupied spectrum assumes that all frequency channels are occupied by at least one PU. Traditional handoff mechanisms, such as those present in all CUs, are expected to be serviceable and reliable in the Cognitive Radio Network Cell (CRNC) environment. However, in practice, a CUs can be compromised by an attacker to carry out a malicious attacks.

Thus, a legitimate CU or new user (NU) compromised by an attacker can act like a MU in CRNC. Therefore, if the MU repeatedly spoofs the signal of the serving PU, legitimate CUs may be blocked from accessing the channel It also degrades system performance and handoff security. Therefore, it is necessary to distinguish between HCUs and MUs to achieve reliable spectral transmission. Achieving spectral security in cognitive radio networks (CRNs), despite its importance, is an area that has not been well studied.In addition, the types and characteristics of potential attacks among spectrum sensing, sharing and Handoff mechanisms are evolving. Therefore, this starts with a new security threat in CRN during handover

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, April 2022
Impact Factor: 6.252

called Cognitive User Emulation Attack (CUEA). Next, we describe how the Coordinating Cognitive User (CCU) mitigates this attack by calculating the CU's Trust Factor/Value (TF/TV). The CCU is the control node of the HCU or CRNC that is responsible for verifying the legitimacy of new users entering the system. The behavior of each CU is also regularly analyzed and monitored by the CCU during handover mechanisms to detect malicious or anomalous behavior.

II. Related Work

The finding and knowing of the preceding subsection are verified by slightly analyzing their behavioral characteristics for various moments as different values of the attack strength, false detection possibilities, and SNR at Cognitive User receiver. As spectrum handoff is an integral function of the CRN, designing a handoff mechanism is a subject of ongoing interest. Although there are several primary user emulation attack (PUEA) methods countering and spectrum handoff mechanisms, ensuring security during spectrum handoff is still not well investigated.

Cryptographic techniques can be used to secure the spectrum handoff process. A new spectrum handoff technique that can achieve security without high overheads is needed. Therefore, we proposed a trust-based spectrum handoff mechanism that can both efficiently and effectively mitigate the discussed security attack.

The handoff mechanism has been designed in order to provide accurate channel sensing by reducing the handoff delay, transmission delay and energy consumption. By the way, to analyze the trust-based security under various transmission delays, probability of attack strength, and the probability of error during CU mobility, a probabilistic system model is used.

As the reason for choosing the scheme was that both the mechanisms use probability-based strategies to ensure security in the CRN environment and have significant performance improvement for throughput and transmission delay as compared to other cryptographic schemes. The recital of the proposed mechanism is compared, in order to depict the effectiveness of the proposed trust-based security mechanism and the gain of the mechanism since the trust-based security scheme validates each handoff CU before allowing it to resume its transmission process on another vacant channel, there is no security method. So that there is an increase in transmission delay and attack probability.

Table 1: Nomenclature

Symbol	Description
AFDRW	Average Packet Delivery Ratio of the New Node
CCU	Coordinating Cognitive User
CRN	Cognitive Radio Network
CRNC	Cognitive Radio Network Cell
CU	Cognitive User
CUEA	Cognitive User Emulation Attack
DDR	Data Delivery Ratio
HCU	Handoff Cognitive User
ID	Identity
MU	Malicious User
NBMNN	Network Broadcasts Messages of the New Node
NU	New User
OTPH	Optimal Transmission Proactive Spectrum Handoff
PU	Primary User
ROC	Receiver Operating Curve
ST	Survival Time
TF/TV	Trust Factor/Trust Value
n	Number of CUs
M	Total Number of Samples
$x_{i,j}$	j-th Sample of i-th CU
E_i	Energy sensing technique of ith CU
$H_{x,x}$	Hypothetical combinations of CUs as $s0$, $s1$, $s2$ and $s3$ CUs probability of legitimate and malicious

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, April 2022
Impact Factor: 6.252

	Probability of error Predefined threshold Value

III. Proposed Secure Handoff Mechanism

During the Handoff Mechanism, the recognition and security of each Cognitive User is given by a Coordinating Cognitive User. Coordinating Cognitive User is identifying and computing their Trust Values based on their communication behavior for analyzing and regulating the activities of Cognitive Users.

This Security Mechanism aims to detect and resolve the handoff threats which is mainly depends on the liveliness of the Cognitive User in the network, data delivery ratio of intermediate nodes, and the number of nodes present in the network.

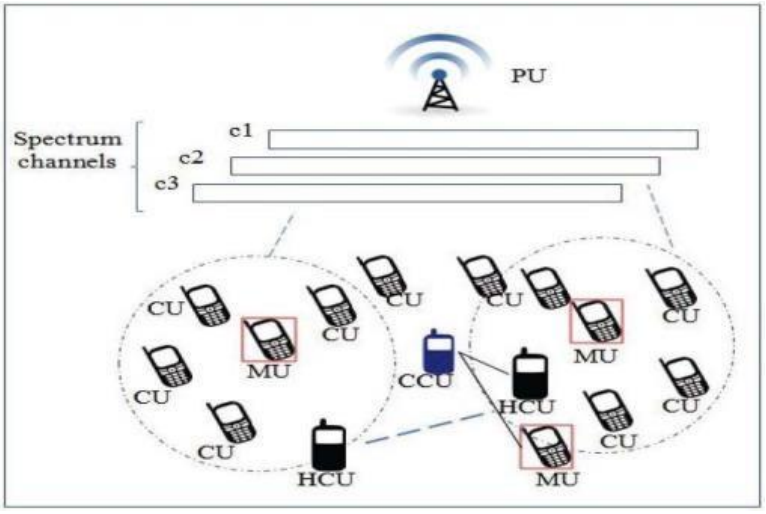


Figure 1: A typical CU handoff mechanism for CRNC

Fig.1. is the CU (Cognitive Users) handoff mechanism for a cognitive radio network cell. A promising Cognitive Radio (CR) technology has been pioneered in the field of wireless transmission, which enables the Cognitive Users (CUs) or unlicensed users to exploit the unused bands/channels of the Primary Users (PU)/licensed users.

Spectrum handoff is the previous major function (i.e., spectrum sensing, spectrum decision, and spectrum sharing) whenever the CU wants to switch the current transmission to another accessible channel upon arrival of the PU through packet transmission is started.

During the spectral handoff, the CU can be compromised by MUs that can introduce various malicious attacks into the CRNC environment. The MU leaves the current channel and captures a new unused channel during the spectral handover to take advantage of the delay required to act as a legitimate PU or CU.

The CCU analyzes the user's type (PU, HCU, or CU) by identifying their communication characteristics, and once the PU is identified, all communication is terminated. The CCU can analyze the confidence score (behavior) in 5 initial transmissions by storing each transaction in a database. After a predefined number of transmissions, the CCU validates the CU as 1 or 0.

If the TV is identified as 1, the user is a User and is permanently blocked from further communication with the network. Of the n CUs, the CCU is selected based on time to survival (ST) and power level. The trust value of each node can increase or decrease depending on the communication operation. MUs are randomly placed near the target HCU, forcing the HCU / NU to leave the occupied channel.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, April 2022
Impact Factor: 6.252

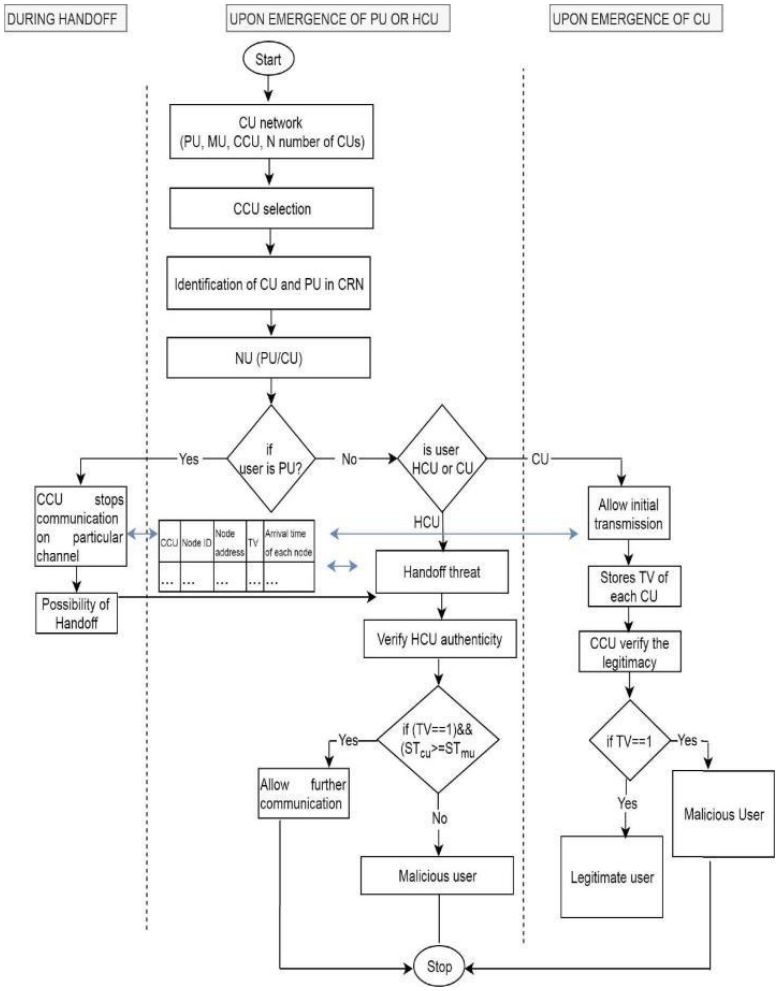
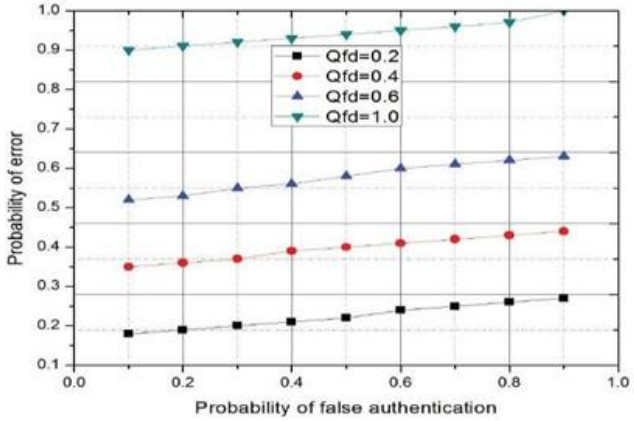


Figure 2: Flowchart of the proposed spectrum handoff of cognitive radio network cell.

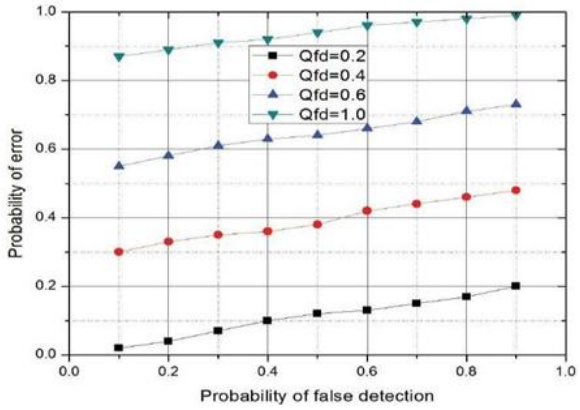
IV. Result and Analysis

A. The probability of error vs. the probability of false authentication.

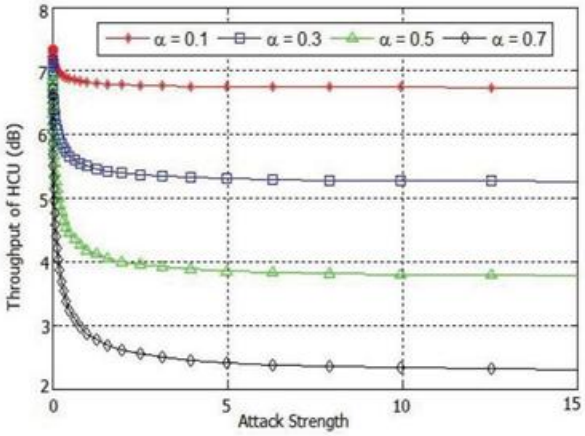


IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, April 2022
Impact Factor: 6.252

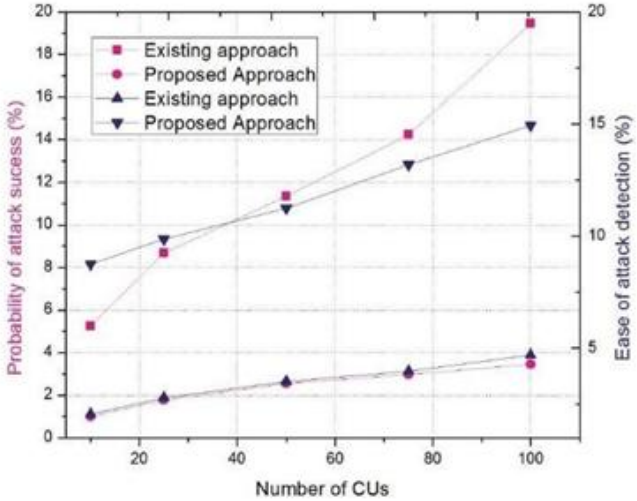
B. The probability of error vs. the probability of false detection.



C. The throughput of HCU vs. the attack strength.

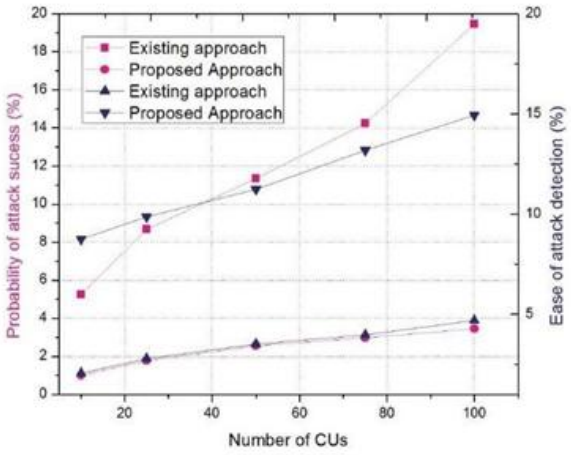


D. The throughput of HCU vs. SNR at CU receiver due to MU [α = 0.1].

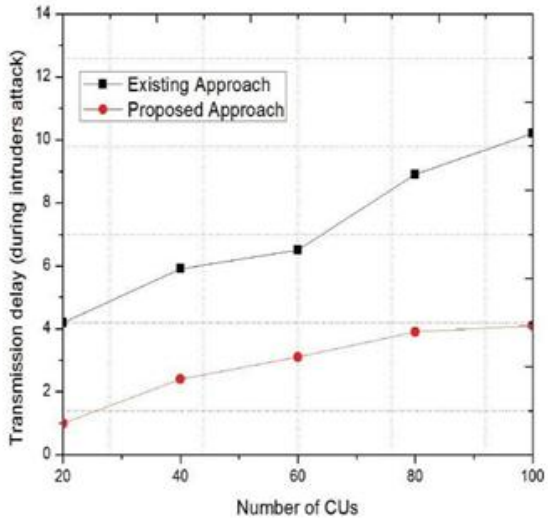


IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, April 2022
Impact Factor: 6.252

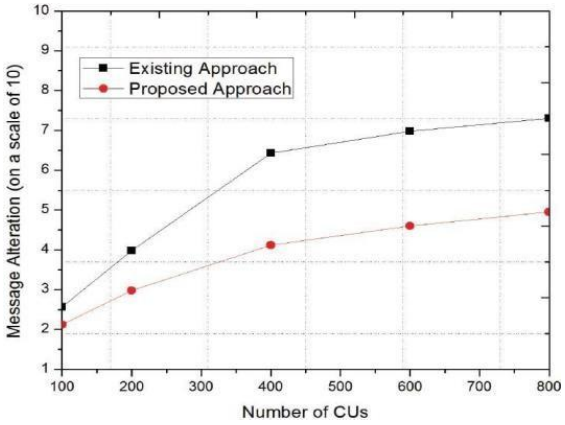
E. Number of CUs vs. probability of attack success and attack detection.



F. Number of CUs vs. probability of attack success and attack detection.



G. Number of CUs vs. message alteration



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, April 2022
Impact Factor: 6.252

V. CONCLUSION

To conclusively diminish the attack that occurs, a key that uses a CCU which exploits the behavioural characteristics of CUs is proposed. The mechanism that is used, virtually differentiates between the licensed and unlicensed CUs on verifying their trust values and analysing the probability of error by several terms that are associated with false authentication. Further, the simulation results shows that the proposed mechanism significantly shows the improvement of throughput of HCU, reduce the transmission delay, and lower attack probability under various network conditions. As a result, the proposed schemes are indeed promising for the work to consider other emerging attacks and implementing a prototype of the proposed and extended mechanism in a real-world setting.

REFERENCES

[1]. Geetanjali Rathee, Naveen Jaglan, Sahil Garg, Bong Jun Choi, Kim_Kwang Raymond Choo, "A Secure Spectrum Handoff Mechanism in Cognitive Radio Networks" IEEE transactions on cognitive Communications And Networking, Vol. 16, no. 3, 2020.

[2]. B. Zheng, M. Wen, S. Lin, W. Wu, F. Chen, S. Mumtaz, F. Ji, and H. Yu, "Design of multi-carrier lbt for laa & wifi coexistence in unlicensed spectrum," IEEE Network, 2019. doi:10.1109/MNET.2019.1900172.

[3]. B. Zheng, M. Wen, S. Lin, W. Wu, F. Chen, S. Mumtaz, F. Ji, and H. Yu, "Design of multi-carrier LBT for LAA & WiFi coexistence in unlicensed spectrum," IEEE Network, 2019. doi:10.1109/MNET.2019.1900172.

[4]. M. Kashif, Z. Ullah, M. Iqbal, L. Musavian, S. Sarwar, X. Wang, S. Mumtaz, Z. Ul-Qayyum, and H. M. Safyan, "Multiuser detection using hybrid arq with incremental redundancy in overloaded mimo systems (workshop paper)," in International Conference on Collaborative Computing: Networking, Applications and Worksharing, pp. 642–653, Springer, 2019.

[5]. P. M. Rodriguez, A. Lizeaga, M. Mendicute, and I. Val, "Spectrum handoff strategy for cognitive radiobased MAC for real-time industrial wireless sensor and actuator networks,"Comp. Netw., vol. 152, pp. 186– 198, 2019.

[6]. M. Aggarwal, T. Velmurugans, M. Karuppiah, M. M. Hassan, A. Almogren, and W. N. Ismail, "Probability-based centralized device for spectrum handoff in cognitive radio networks," IEEE Access, vol. 7, pp. 26731–26739, 2019.

[7]. Z. Zheng, T. Wang, J. Wen, S. Mumtaz, A. K. Bashir, and S. H. Chauhdary, "Differentiallyprivate highdimensional data publication in internet of things," IEEE Int. of Things Journal, 2019. doi:10.1109/JIOT.2019.2955503.

[8]. M. Patnaik, V. Kamakoti, V. Matya´s, and V. ˇ Reh ˇ ak, "PROLE- ´ Mus: A proactive learning based mac protocol against PUEA and SSDF attacks in energy constrained cognitive radio networks," IEEE Trans. on Cognitive Communication. And Network., 2019. doi:10.1109/TCCN.2019.2913397.

[9]. S. Garg, K. Kaur, N. Kumar, G. Kaddoum, A. Y. Zomaya, and R. Ranjan, "A hybrid deep learning-based model for anomaly detection in cloud datacenter networks," IEEE Trans. on Netw and Service Management, vol. 16, no. 3, pp. 924– 935, 2019.

[10]. E. Hill and H. Sun, "Double threshold spectrum sensing methods in spectrum-scarce vehicular communications," IEEE Trans. on Indus. Info., vol. 14, no. 9, pp. 4072–4080, 2018.

[11]. S. K. Haider, A. Jiang, M. A. Jamshed, H. Pervaiz, and S. Mumtaz, "Performance enhancement in P300 ERP single trial by machine learning adaptive denoising mechanism," IEEE Netw. Letters, vol. 1, no. 1, pp. 26–29, 2018.

[12]. B. Van Nguyen, H. Jung, D. Har, and K. Kim, "Performance analysis of a cognitive radio network with an energy harvesting secondary transmitter under nakagami fading," IEEE Access, vol. 6, pp. 4135–4144, 2018.

[13]. E. Meshkova, Z. Wang, K. Rerkrai, J. Ansari, J. Nasreddine, D. Denkovski, T. Farnham, J. Riihijarvi, L. Gavrilovska, and ¨ P. Mah¨ onen, "Designing a self-optimization system for cognitive ¨ wireless home networks," IEEE Trans. on Cognitive Commun. and Netw., vol. 3, no. 4, pp. 684–702, 2017.

[14]. A. Koushik, J. D. Matyjas, F. Hu, and S. Kumar, "Channel/beam handoff control in multi- beam antenna based cognitive radio networks," IEEE Trans. on Cognitive Commun. and Netw., vol. 4, no. 1, pp. 30–42, 2017.

[15]. Y. Zhao, Z. Hong, Y. Luo, G. Wang, and L. Pu, "Prediction-based spectrum management in cognitive radio networks," IEEE Sys. Journal, vol. 12, no. 4, pp. 3303–3314, 2017.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, April 2022
Impact Factor: 6.252

[16]. M. E. Bayrakdar and A. Calhan, "Improving spectrum handoff utilization for prioritized cognitive radio users by exploiting channel bonding with starvation mitigation," AEU-Int. Journal of Elec. and Commun., vol. 71, pp. 181–191, 2017.

[17]. K. Kumar, A. Prakash, and R. Tripathi, "Spectrum handoff in cognitive radio networks: A classification and comprehensive survey," Journal of Net. and Comp. App., vol. 61, pp. 161–188,2016.

[18]. Y. Wu, F. Hu, Y. Zhu, and S. Kumar, "Optimal spectrum handoff control for CRN based onhybrid priority queuing and multiteacher apprentice learning," IEEE Trans. on Veh. Technol., vol.66, no. 3, pp. 2630–2642, 2016.

[19]. A. F. Tayel, S. I. Rabia, and Y. Abouelseoud, "An optimized hybrid approach for spectrum handoff in cognitive radio networks with non- identical channels," IEEE Trans. on commun., vol. 64, no. 11, pp. 4487– 4496, 2016.

[20]. G. Rathee, P. Thakur, G. Singh, and H. Saini, "Aspects of secure communication during spectrum handoff in cognitive radio networks," in 2016 International Conference on Signal Processing and Communication (ICSC), pp. 64–69, IEEE, 201

[21]. J. Qi, F. Hu, X. Li, A. Koushik, L. Hu, and S. Kumar, "CR based video communication testbed with robust spectrum sensing/handoff," in Info. Technol.: New Generations, pp. 59–70, Springer, 2016.

[22]. R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," IEEE Commun. Surveys & Tuts, vol. 17, no. 2, pp. 1023– 1043, 2014.

[23]. M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," IEEE Trans. on Veh. Technol., vol. 64, no. 8, pp. 3790– 3795, 2014.

[24]. C.-W. Wang and L.-C. Wang, "Analysis of reactive spectrum handoff in cognitive radio networks," IEEE Journal on selected areas in commun., vol. 30, no. 10, pp. 2016–2028, 2012.

[25]. A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Cooperative spectrum sensing in multiple antenna based cognitive radio network using an improved energy detector," IEEE Communications letters, vol. 16, no. 1, pp. 64–67, 2011.