Evaluating the Effects of Primary User Emulation Attacks on Cognitive Radio Networks

Nomfundo Favourate Manyisa and Mthulisi Velempini

Abstract A Cognitive Radio Network (CRN) is a solution to wireless technology which solves the spectrum scarcity challenge. CRN addresses the underutilization of the spectrum by enabling unlicensed users to coexist with the network's licensed users (primary users). The secondary users are expected to utilize the spectrum only when the primary user is idle. Unfortunately, cognitive radio network is vulnerable to security threats. This study focuses on one of the threats known as the Primary User Emulation Attack (PUEA). A number of mitigation schemes have been designed to combat the PUEA. This study evaluates the Neyman-Pearson Hypothesis Test (NPCHT) and Wald's Sequential Probability Ratio Test (WSPRT) through network simulations. The results show that the NPCHT only outperformed the WSPRT in the probability of false alarm results when the malicious nodes are high. However, the remaining scenarios also yield poor results.

Keywords Cognitive radio network · Primary user emulation attack · Security threats

1 Introduction

The advancement of wireless communication technology increases the need for more bandwidth and spectrum which results in spectrum scarcity. However, Cognitive Radio introduced by Mitola [1] is a new technology which is regarded as the solution to the overcrowding of unlicensed spectrum and the underutilization of licensed spectrum. Unfortunately, the technology is susceptible to security attacks. This chapter focused on Primary User Emulation Attacks (PUEA). This attack degrades the performance of CRNs. Hence there is a need for mitigation techniques to be deployed to improve the performance of CRNs and to counter the effects of PUEA. In a PUEA, malicious users can emulate the primary user and transmit using the idle channels to

N. F. Manyisa · M. Velempini (✉)
University of Limpopo, Limpopo, South Africa
e-mail: mthulisi.velempini@ul.ac.za

X.-S. Yang et al. (eds.), *Proceedings of Eighth International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 695,
https://doi.org/10.1007/978-981-99-3043-2_66

block the secondary users (SUs) or it can report an idle channel as in use to prevent SUs from using a given channel [2]. The PUEA misleads the SUs so that it can either monopolize the idle channels or prevent the SUs from using the idle channels. As a result, the goals of CRNs are not realized.

2 Related Work

The authors in [3] proposed a cooperative belief propagation procedure to detect an attacker by using Received Signal Strength (RSS) measurements and the interactions between neighbouring secondary users. To relate the received power to the distance between the transmitter and receiver, a parametric model is needed for the approach. The drawback of the belief propagation is that it uses RSS-based approximation of the primary user, which could result in fluctuations even in small environments causing obstacles and transmission imperfections. Furthermore, actual values are not used as it relies on estimated values.

In [4], the authors used the location data of the primary user and the Received Signal Strength (RSS). This scheme has three phases in which at least two of the phases must be satisfied. The phases are: (i) verification of signal characteristics, (ii) received signal energy estimation and (iii) localization of the transmitter. It locates the transmitter using RSS measurements collected by a wireless sensor network. The use of RSS is a challenge as estimates and fluctuations may be frequent in small geographical areas.

Authors in [5] proposed a public key cryptography mechanism where a PU will attach a digital signature to the data unit it transmits. The digital signature is generated using the primary user id, current time stamp and private key. The SUs sense that the primary signal (malicious or non-malicious) is transmitted in a specific channel. The digital signal part is sent to the base station through the control channel. The secondary base station with the help of a Certification Authority (CA) verifies if the signal detected is from the PU or not. The challenge of this method is that a base station is susceptible to DoS attacks when an attack continuously transmits fake signals. DoS is an attack where a stream of traffic is sent continuously to the target to overwhelm and make it unavailable to process any request other than the attack. A number of schemes designed to either detect, address or mitigate the effects of primary user emulation attacks are proposed in [6–22]. The techniques show that this attack still require further attention in CRN. In this work, we evaluate the performance of the most promising techniques.

3 Methodology

There are several techniques used to mitigate the PUEA however in this chapter, we focus on two techniques, the Neyman-Pearson Composite Hypothesis Test (NPCHT) and the Wald's Sequential Probability Ratio Test (WSPRT). These two schemes were selected in this study as they are recommended as the best techniques by other researchers. Furthermore, they do not require the knowledge of where PU is located which requires a lot of computation. They however rely on the signal strength of the PU.

The comparative performance of the schemes was evaluated using these metrics:

- The Probability of a False Alarm (PFA)
- The Probability of Missed Detection (PMD)
- The Probability of Detection (PD)

Tools and platforms that were used:

To simulate and perform the analysis, MATLAB was used. It was installed on an HP L45 Desktop computer with 8 GB RAM. Intel®Pentium(D) CPU 2037 @3.19 GHz running on Windows 10 Operating System.

4 Results

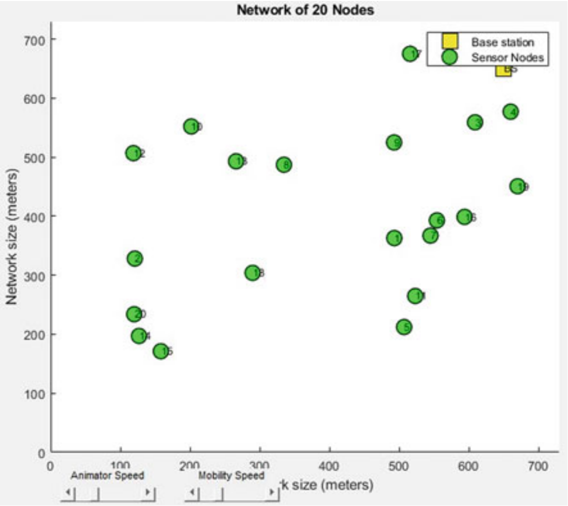
The main objective was to evaluate the efficiency of the two selected schemes in detecting the PUE attack. In this study, different network sizes were considered with 20, 50 and 70 nodes with different percentages of attacking nodes such as 15%, 25% and 35% respectively. We evaluated the performance of the schemes based on the following metrics: the PD, the PFA and the PMD. The evaluations were carried out in a grid of 700*700 square metres of network topology. The performance of the selected schemes was evaluated in a MATLAB environment.

5 Analyses of the Results

The scenario in Fig. 1 shows the simulation of the performance of the two selected schemes where both malicious users and secondary users are active in the network. For example, in a network with 20 nodes, 15% of the nodes would be malicious. The network also included a base station. The primary user is located outside the CRN.

Figure 2 results show the PFA. It shows that the WSPRT achieved the least PFA compared to the Neyman-Pearson Composite Hypothesis Test. For WSPRT, when $N = 20$, there are 3 malicious users and the results show a decreasing PFA even when the number of nodes is increased. The PFA of WSPRT is less compared to NPCHT.

Fig. 1 Cognitive radio environment.

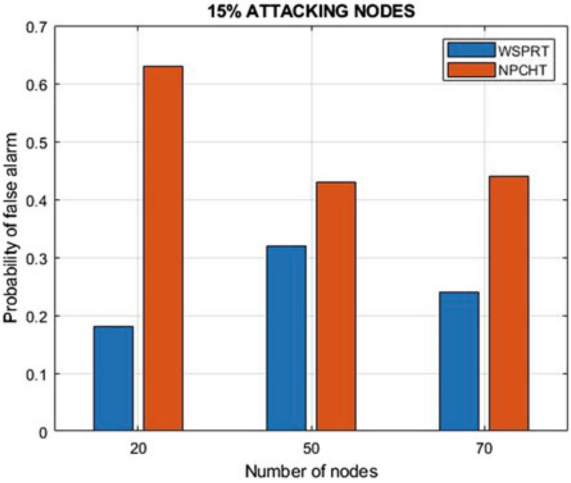


This means that the WSPRT has fewer instances of false alarms in comparison with the NPCHT which shows that it is more efficient.

Figure 3 results show how the two schemes performed when the number of attacking nodes was increased with the number of nodes being constant. The results show that WSPRT has been consistent in reducing the PFA compared to NPCHT which fluctuates between the three scenarios. The WSPRT outperformed the NPCHT as shown in Fig. 3. We also observed that the PFA increases as the attacking nodes are increased.

Figure 4 shows the results with 35% of attacking nodes. We observed that there was an increase in the PFA in WSPRT as the environment was smaller with a higher

Fig. 2 Probability of false alarm with 15% attacking node.



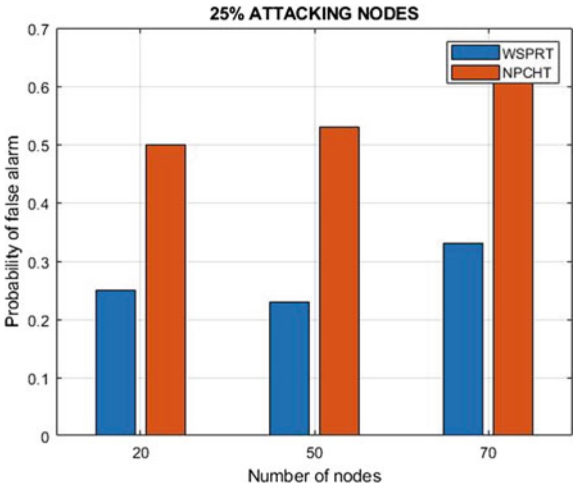


Fig. 3 Probability of false alarm with 25% attacking nodes.

number of attacking nodes. In this scenario, the number of attacking nodes was increased to 35%. The NPCHT performed better than WSPRT in this instance which shows that it is effective in addressing the effects of malicious nodes when more malicious nodes are considered. The results also show how the scheme performs in scenarios where the number of malicious nodes is increasing.

Figure 5 shows that WSPRT reduced the PMD more than the NPCHT scheme. We observed that NPCHT's PMD is much higher which shows that the scheme is unable to reduce the PFA. We also observed that the PFA remains consistent as the number of nodes in the network increases. The performance of WSPRT keeps on reducing the PFA regardless of the change in the number of malicious nodes in a network.

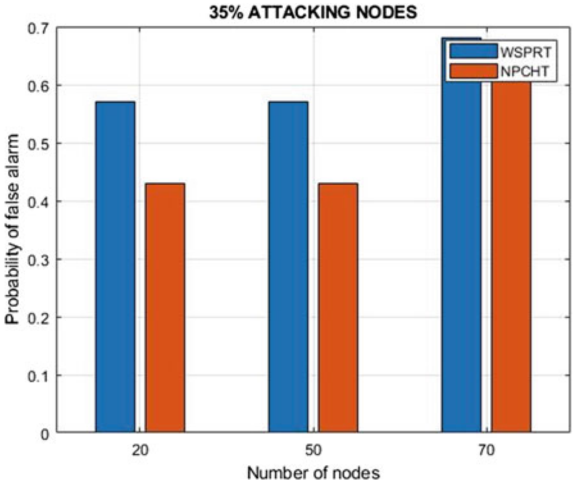
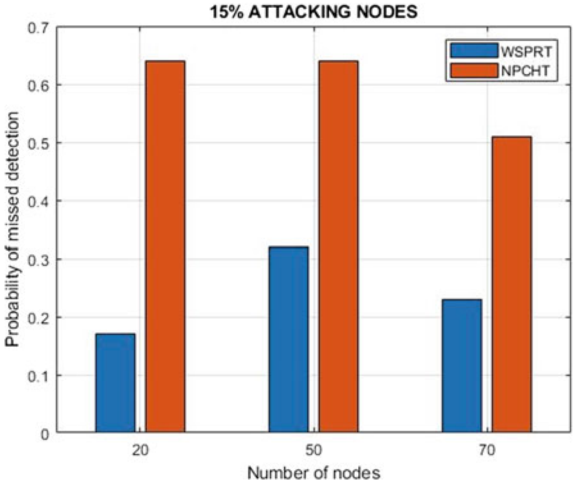


Fig. 4 Probability of false alarm with 35% attacking node.

Fig. 5 Probability of missed detection with 15% attacking nodes.



In Fig. 6, through simulations, we can observe the positive results in WSPRT as it is not affected by the change in the increasing number of malicious users in the network compared to NPCHT where the missed probability is still much higher. WSPRT probability is also the same compared to the scenario when the number of attacking nodes was 15% of the total nodes. Nevertheless, the WSPRT still performed better. We then increased the number of attacking nodes from 25 to 35% of the total nodes in Fig. 7.

Figure 7 shows that WSPRT is affected by the missed probability compared to NPCHT. The results show that WSPRT is affected by the increase in malicious nodes in the network. Its performance degraded significantly compared to Fig. 6. However,

Fig. 6 Probability of missed detection with 25% attacking nodes.

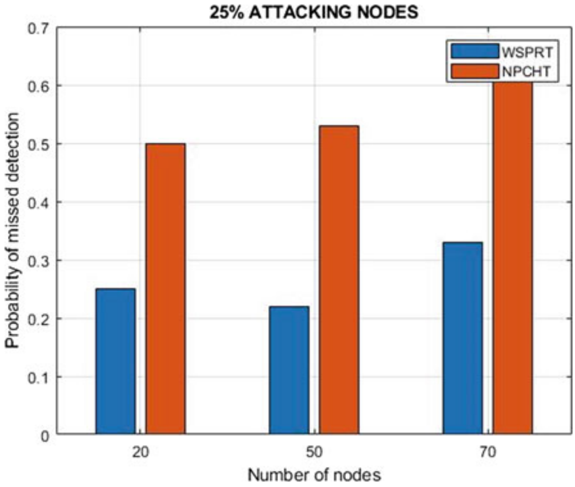
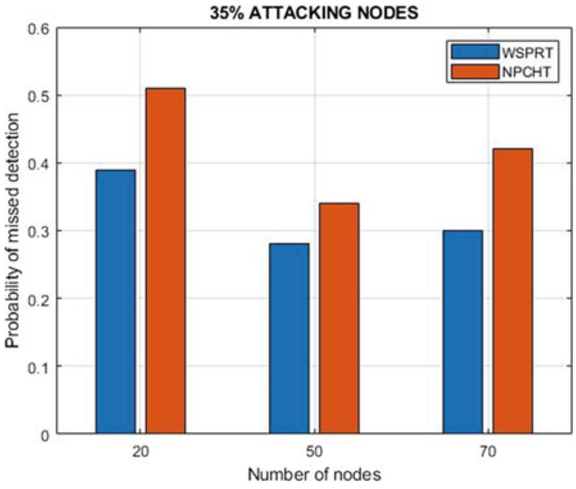


Fig. 7 Probability of missed detection with 35% attacking nodes.

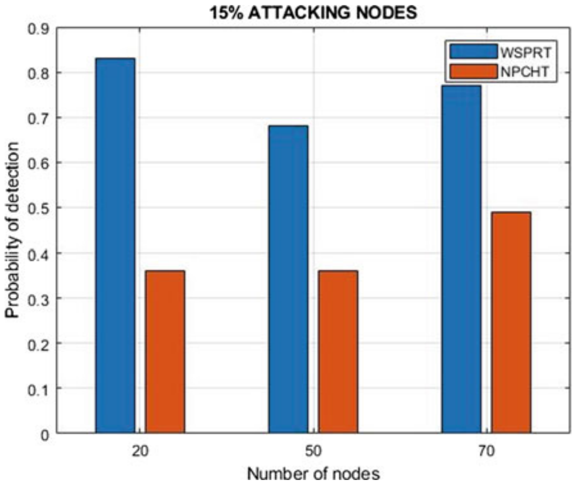


despite the higher percentage of increase in response to the increase in the number of attacks, the WSPRT still outperformed the NPCHT scheme.

In Fig. 8, we observed that the performance of WSPRT is degraded by the increase in the number of attacking nodes. As the percentage of malicious nodes increases, the detection results of WSPRT become poor whilst the results of the NPCHT scheme improves. This shows that the performance of NPCHT improves with the increase in the percentage of malicious nodes. This analysis pertains to how the two schemes respond to the increasing number of nodes. However, in general, the WSPRT scheme is still superior.

In Fig. 9, the WSPRT has a higher probability compared to NPCHT and its probability is somewhat constant as the number of nodes is increased. However, the

Fig. 8 Probability of detection with 15% attacking nodes.



probability of NPCHT keeps on decreasing as the number of nodes increases. This shows the effect of the increasing number of nodes in scenarios with higher percentages of malicious nodes. The NPCHT scheme was outperformed by the WSPRT scheme.

In Fig. 10, the PD of the WSPRT scheme is lower compared to Fig. 9. Its performance is marginally better than the one for the NPCHT scheme. As the percentage of malicious nodes increases, we observed that the two schemes' probabilities were increasing as the number of nodes increases. The WSPRT is still superior in all the scenarios. This shows that the WSPRT is effective in detecting PUEA.

Fig. 9 Probability of detection with 25% attacking nodes.

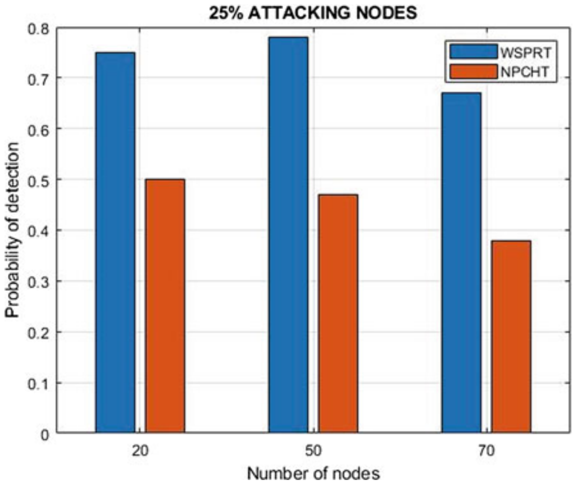
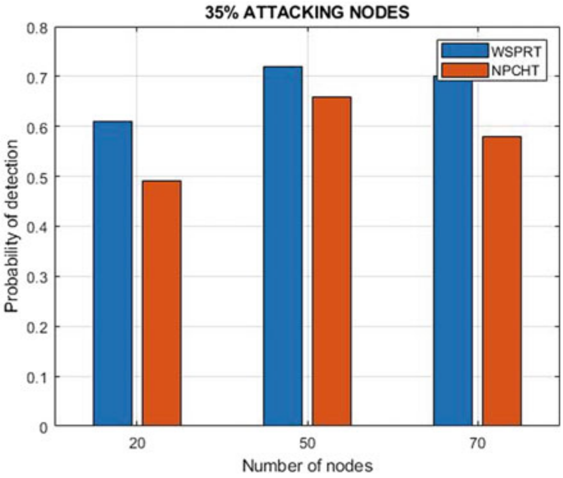


Fig. 10 Probability of detection with 35% attacking nodes.



6 Conclusion

The performance of WSPRT was compared to NPCHT, these two schemes detect and isolated malicious users. The performance results show that WSPRT is superior to NPCHT, especially when the percentage of malicious nodes is 15%. In a network where the number of malicious nodes is higher, NPCHT performs better than WSPRT in the PFA results. This happens to be the only scenario where the NPCHT performs better than WSPRT scheme.

The study can be improved by improving the two schemes. The best features of the two schemes can be integrated into a new hybrid scheme optimized for improved detection efficiency. There are also other security challenges in the cognitive radio, such as the spectrum sensing data falsification (SSDF), which require attention. The combined effects of PUEA and SSDF can be more disruptive. The DOS attacks can also scale the magnitude of the attacks in CRNs.

It is therefore of paramount importance to address the effects of PUEA in CRNs since it negates its goals. As a result, PUEA ensures that the spectrum challenges are not addressed. The overcrowding of unlicensed spectrum and the underutilization of licensed spectrum persist in the presence of the PUEA attacks. It renders the CRN technology ineffective.

References

1. Tato A (2018) Software radio architecture: a brief introduction. 2(18)
2. Moghaddam SS (2018) Cognitive radio in 4G/5G wireless communication systems, 1st edn. In: Moghaddam SS (ed) INTECHOPEN, Thanjavur, Tamil Nadu
3. Deepa Das SD (2013) Primary user emulation attack in cognitive radio networks: a survey. IACST 3(2)
4. Sitadevi Bharatula MM (2016) An Intelligent fuzzy based energy detection approach for cooperative spectrum sensing. Circ Syst 7(6):1042–1050
5. Zhao C, Xie L, Jiang X, Huang L, Yao Y (2010) A PHY-layer authentication approach for transmitter identification. Commun Mobile Comput (CMC) 2:154–158
6. Ghanem WR, Shokair M, Desouky MI (2016) An improved primary user emulation attack detection in cognitive radio networks. In: 33rd national radio science conference (NRSC 2016), vol 2, no 12, pp 178–187
7. Yuan Z, Niyato D, Li H, Song JB, Han Z (2012) Defeating primary user emulation attacks using belief propagation in cognitive radio networks. IEE J Sel Areas Commun 30(10):1850–1860
8. Chen EAT (2008) Defense against primary user emulation attacks in cognitive radio networks. IEEE J Sel Areas Commun 26(1):25–37
9. Chen JPR (2006) Ensuring trustworthy spectrum sensing in cognitive radio networks. In: 1st IEEE workshop on networking technologies for software defined radio networks, SDR'06, vol 06, no 1, pp 110–119
10. Chen JRR (2014) Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers. J Comput Syst Sci 80(3):591–601
11. Hao KSD (2012) A differential game approach to mitigating primary user emulation attacks in cognitive radio networks. In: IEE 26th international conference on advanced information networking and applications, vol 1, no 8, pp 495–502

12. Haykin S (2013) Cognitive radio: brain empowered wireless communications. IEEE J Sel Areas Commun 23(2):201–220
13. Elgharawy SM (2018) Security in cognitive radio network: defense against primary user emulation attacks using genetic artificial bee colony (GABC) algorithm. IEEE Future Gener Comput Syst 109(2020):479–487
14. Chen R, Park JM, Reed JH (2008) Defense against primary user emulation attacks in cognitive radio networks. IEEE J Sel Areas Commun 26(1):25–37
15. Sasa Maric SR (2015) Mitigation of primary user emulation attacks in cognitive radio networks using belief propagation. Int Conf Cogn Radio Oriented Wirel Netw 156:463–476
16. Verma PK, Taluja S, Dua RL (2012) Performance analysis of energy detection, matched filter detection & cyclo stationary feature detection spectrum sensing techniques. Int J Comput Eng Res 2(5):1296–1301
17. Singh A, Sharma A (2014) A survey of various defense techniques to detect primary user emulation attacks. Int J Curr Eng Technol 4(2):900–908
18. Jiang QM, Chen HF, Xie L, Wang K (2017) On detecting primary user emulation attack using channel impulse response in the cognitive radio network. Front Inf Technol Electron Eng 18(10):1665–1676
19. Gupta A (2015) A review on software defined radio and implementation of digital communication blocks on GNU radio platform. J Comput Intell Electron Syst 4(1):10–16
20. Sarala SMSIB (2019) A novel authentication mechanism for cognitive radio network. Int J Recent Technol Eng (IJRTE) 8(4):2277–3878
21. Fragkiadakis AG, Tragos EZ, Askoxylakis IG (2013) A survey on security threats and detection techniques in cognitive radio networks. IEEE Commun Surv Tutor 15(1):428–445
22. Jin Z, Anand S, Subbalakshmi KP (2009) Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing. ACM SIGMOBILE Mobile Comput Commun Rev 13(2):964–973