Investigating Spectrum Sensing Security Threats in Cognitive Radio Networks

Sekgoari Mapunya(✉) and Mthulisi Velempini

Department of Computer Science, University of Limpopo, Polokwane, South Africa
sekgoarimapunya@gmail.com, mthulisi.velempini@ul.ac.za

Abstract. Cognitive Radio Networks (CRN) technology was proposed as a solution to the challenges of overcrowding and underutilization of spectrum bands. CRN is a subset of wireless networks and as such, is susceptible to traditional wireless networks security attacks. In addition, it is also vulnerable to new security attacks such as cooperative sensing related attacks. CRN has an ability to dynamically adapt to the radio environment and thereafter make decisions to access spectrum holes opportunistically.

In this paper, we evaluate spectrum sensing security attacks in CRN. Spectrum sensing is fundamental phase of the cognitive cycle of the CRN however, when compromised; it impacts negatively on the functionality of the cognitive network. Spectrum Sensing Data Falsification (SSDF) attack is one of the security challenges of the CRN and it occurs largely in CRN implementing cooperative spectrum sensing (CSS). CSS is a sensing strategy which increases the detection rate of primary users when secondary users share the sensing data. The SSDF attack degrades the performance of the CRN resulting in the poor utilization of the free spectrum. The study therefore evaluates the Cooperative Neighbouring Cognitive Radio Nodes (COOPON) and the pinokio schemes in a simulated environment. The results show that the COOPON scheme is effective in the mitigation of the effects of malicious users.

Keywords: Cognitive Radio Networks
Cooperative neighbouring cognitive radio nodes
Spectrum Sensing Data Falsification · Pinokio

1 Introduction

The ever-increasing number of wireless devices which utilize free spectrum bands has led to overcrowding of the spectrum while the licensed spectrum is underutilized [1]. The Cognitive Radio Networks (CRN) technology was proposed to address the challenge of spectrum overcrowding and underutilization, where cognitive or secondary users (SU) opportunistically utilize idle spectrum bands licensed to primary users (PU). Spectrum sensing is the most fundamental and vulnerable phase of the cognitive cycle, when cooperative sensing is implemented [2]. CRN is susceptible to both traditional and new security attacks due to its ability to dynamically sense, share, and access the spectrum. This paper focuses on cooperative spectrum sensing (CSS) related security attacks.

Y. Zhou and T. Kunz (Eds.): AdHocNets 2017, LNICST 223, pp. 60–68, 2018.
https://doi.org/10.1007/978-3-319-74439-1_6

In CSS, multiple SUs cooperate in spectrum sensing which makes the network vulnerable to spectrum sensing data falsification attack (SSDF). If spectrum sensing is compromised, it may lead to poor utilization of the spectrum and missed opportunities caused by malicious nodes [3]. The sharing of incorrect spectrum data by malicious nodes is called the SSDF attack which causes interference to both licensed and unlicensed users in CRN [4]. The SSDF attack enables greedy nodes to monopolize the use of the spectrum holes while starving the rest of the nodes. The study investigates spectrum sensing security attacks, the countermeasures and presents the comparative results of security schemes. The study then proposes a security framework for CRN.

2 Related Work

A number of schemes designed to address the effects of the SSDF have been proposed. Most of the schemes implement the data fusion techniques. In [5], a Conditional Frequency Check (CFC) technique based on a Markov Spectrum Model is proposed to mitigate the effects of the Byzantine attacks – the SSDF attacks. With one trusted user, the technique can achieve high detection accuracy of a malicious node without prior knowledge. The assumption of the availability of one trusted node has been adopted in literature. However, when such a trusted node is not available, an additional clustering procedure is required, in attempt to detect the malicious node when the number of non-malicious nodes are more than the malicious ones. The detention window should be wide enough for the scheme to be effective.

In [6], schemes implementing a fusion center (FC) are evaluated. Unfortunately, the schemes are not designed to counter the effects of the SSDF attack. The comparative analysis indicates that the Gaussian assumption is suitable where the SSDF attack is assumed as compared to the Gamma assumption. It was also assumed that the percentage of malicious users (MU) was less than the number of non-malicious users. The algorithm may not perform well as expected if more MUs are considered.

In [7], an extension of the generalized extreme studentised deviation (EGESD) test was proposed to detect selfish nodes in the network. The EGESD was designed to address the limitation of generalized extreme studentised deviation test and it subjects the validity of updates to the Shapiro–Wilk test.

In [8], CRN was implemented in smart home energy management which is susceptible to SSDF. A multi-attribute trust based framework was proposed to facilitate dependable spectrum sensing and to prioritize delay sensitive data transmissions. The evaluation results of the scheme show that it is 91.42% reliability. However, it was assumed that the attacker would always exhibit the always-on attack and different scenarios were not considered.

In [9], a distributed cooperative spectrum sensing (DSCS) with a secure spectrum allocation strategy which is based on the dynamic reputation model and the Vickrey-Clarke-Groves (VCG) was proposed. The evaluation results show that the scheme is effective in addressing the effects of the SSDF attacks. The efficiency of the scheme was compared to the performance of the distributed random scheme in [10].

In [11], a fusion technique is proposed in which spectrum sensing reports are evaluated against a predefined threshold value to detect an attack. The spectrum is said to be occupied by the PU if the reports evaluates to a value which is greater than or equal to the threshold otherwise, it is unoccupied. The change in the value of the threshold has an effect on the results furthermore; it is not optimized for multiple attackers.

In [12], the Weighted Sequential Ration Test (WSRT) is utilized and the scheme consists of reputation maintenance and the hypothesis test. Nodes are assigned a reputation of 0 thereafter with each correct spectrum report the reputation value is incremented by one. The Sequential Probability Ratio Test (SPRT) [13] is then applied. The WSRT differs from the ordinary SPRT because it utilizes a trust-based information fusion scheme. However, there is need to evaluate the efficiency of the scheme.

In [14], a weight based fusion scheme was implemented to counter the effects of a malicious node. It uses trust based and pre-sifting procedures. Permanent malicious nodes are typically of two types, the "Always Yes" and the "Always No". The "Always Yes" malicious nodes report the presence of the PU which increases the rate of false alarms. The "Always No" advertises the absence of the PU which increases the interference rate. This approach primarily focuses on the pre-filtering of the data to detect the MU and assign the trust value to nodes.

In [15], a detection mechanism that runs in the FC is proposed. The FC detects the attacker by checking mismatches between local decisions and the aggregated decisions and then isolates outliers. The scheme is very effective against Byzantine attacks and it detects MUs within a short time-frame. Unfortunately, the scheme is FC based and infrastructure based.

In [16], a Bayesian detection mechanism that requires the knowledge of prior probabilities of the local spectrum sensing results and the knowledge of prior conditional probabilities of the previous sensing results is proposed. There are a few combination cases that exist between these two cases leading to mismatch in the assignments of the costs. The overall cost is the sum of every cost weighted by the probabilities of the corresponding cases. The scheme cannot detect an SSDF attacker without prior knowledge.

In [17], the Neyman-Pearson Test is proposed that does not require the prior probabilities of final sensing results or any cost associated with each decision case. It defines either a maximum acceptable probability of false alarm or a maximum acceptable probability of missed detection. However, it requires a prior conditional probability of the local sensing.

In [18], a detection technique called pinokio is proposed. Pinokio utilizes a Misbehaviour Detection System (MDS) which profiles the normal behaviour of network nodes based on the training data. The MDS detects MUs by checking the bit rate behavior of nodes. The bit rate has to change occasionally. Nodes not exhibiting the normal expected behavior are classified as outliers. The challenge with the proposed scheme is the assumption that mobile nodes move at a low speed. Higher mobility speeds may impact negatively the performance of the scheme.

COOPON, a simple and efficient detection scheme designed to detect selfish nodes in CRAHN known as SSDF attack is proposed in [19]. The scheme detects the availability of selfish MUs through the help of neighboring nodes. The target SU and its neighbors exchange observed radio environment data, which is evaluated by all SUs to

detect selfish malicious nodes. Then, each SU compares the reported data and if there is any difference, a given node is classified as the outlier.

3 Simulation Model

In the section, comparative performance results of the COOPON and Pinokio are presented. The two schemes are designed to counter the effects of the SSDF attacks. The schemes were simulated using the network simulator 2.31 (NS 2.31). Table 1 presents the simulation parameters used in the simulation.

Table 1. Simulation parameters.

Parameter	Values
Antenna type	OmniAntenna
Propagation model	TwoRayGround
Simulation area	500 m * 500 m
Mobility model	Random Waypoint
Node speed	20 m/s
Routing protocol	Ad hoc on-demand multipath distance vector routing
MAC protocol	IEEE 802.11b with extension to support CR networks
Data channel	8
Common control channel	1
Channel data rate	11 M bits/s
Number of SUs	50, 100, 150
Percentage of selfish SU	2%, 10%, 50%, 75%

Table 1 shows the parameters that were used in the modeling of the simulation environment. The simulation time was set to 300 simulation seconds. The cognitive radio network was assumed to be having a transmission radius of 500 m. We considered CRN with eight data channels and one common control channel for the exchanging of control packets between the SUs. The data channel rate was set to 11 Mb/s. It was also assumed that SUs can have at least two neighbors and a maximum of five neighbors.

The detection efficiency of the scheme was measured based on the probability of detection, which is the probability of a CR user positively detecting that a licensed user is present.

4 Results

The detection rate was considered in the evaluation of the performance of the COOPON and Pinokio schemes which were chosen based on the fact that they can be deployed in a cognitive radio ad-hoc networks. The COOPON detects MUs through the implementation of the MDS which profiles the normal behavior of nodes. The MDS detects anomaly behavior by monitoring the bit rate behavior of nodes. There must be periodic change in bit rate which is adjusted continuously by a node. For example, narrow

channels use a low bit rate. Nodes which fail to exhibit the expected behavior are classified as outliers. Figure 1 presents the detection rate of the COOPON scheme.

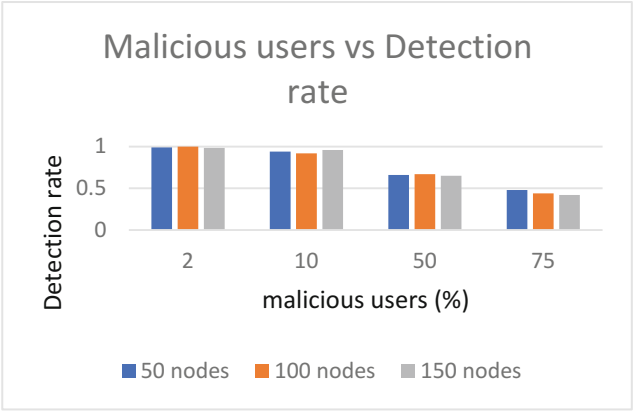

Fig. 1. Detection rate vs. malicious users in COOPON scheme.

To investigate the impact of MUs on the performance of the CRN, the evaluation was performed in network scenarios with 50, 100 and 150 SUs as shown in Fig. 1. It can be seen that the number of users in the network has an impact on the COOPON's detection rate, as the number of nodes increases in the network the detection rate decreases. Figure 2 presents the detection rate of the Pinokio scheme.

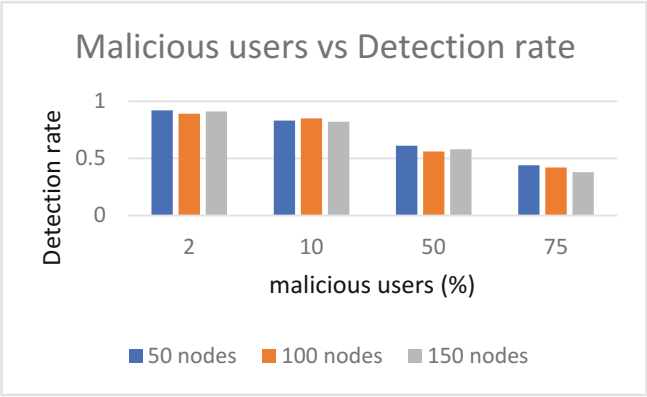

Fig. 2. Detection rate vs. malicious users in Pinokio scheme.

The impact of node density on the performance of the Pinokio was investigated in Fig. 2. The number of nodes was increased from 50 to 100, and then to 150. Figure 2 shows that the density of SUs in the network has a negative impact on the detection rate of the Pinokio scheme. The detection rate decreases as the nodes are increased in the network. In Fig. 3, the comparative results of the two schemes are presented.

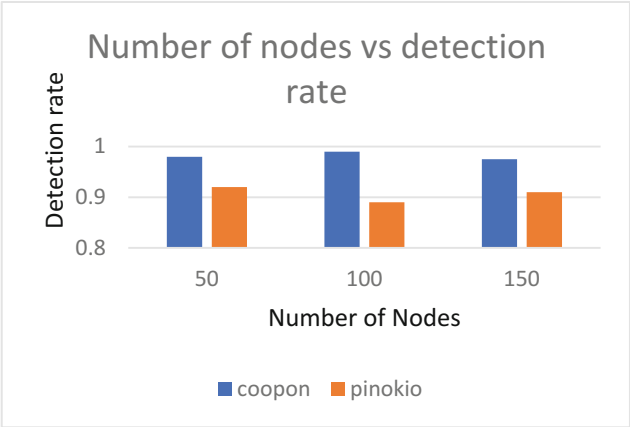

Fig. 3. Number of nodes vs. detection rate with 2% malicious nodes.

Figure 3 shows the comparison of the detection rates of the two schemes when 2% of the total network nodes are malicious nodes. As shown in Fig. 3, the COOPON scheme achieved a higher detection rate than the Pinokio scheme in the three scenarios. It is therefore superior to the Pinoko scheme. Figure 4 considered a network with 10% of the nodes being malicious nodes.

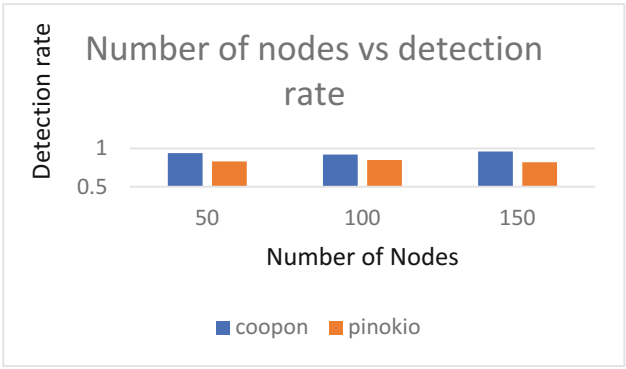

Fig. 4. Number of nodes vs. detection rate with 10% malicious nodes.

Figure 4 show that when there are 10% of malicious nodes and 90% of non-malicious nodes the COOPON scheme outperforms marginally the Pinokio scheme which suggest that the COOPON scheme was degraded severely by the increase in the number of malicious nodes. The results in Fig. 5 confirm this assertion.

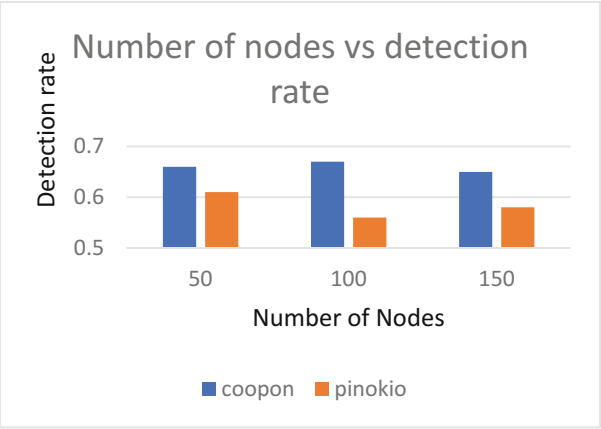

Fig. 5. Number of nodes vs. detection rate with 50% of malicious nodes.

Figure 5 shows the comparison of detection rates of the two schemes when the network consists of 50% malicious nodes. The results show that the performance of the COOPON scheme is marginally better than the performance of the Pinokio scheme as observed in Fig. 4. The degradation in the performance of the COOPON scheme in the presence of increasing number of malicious nodes is evident in Fig. 6.

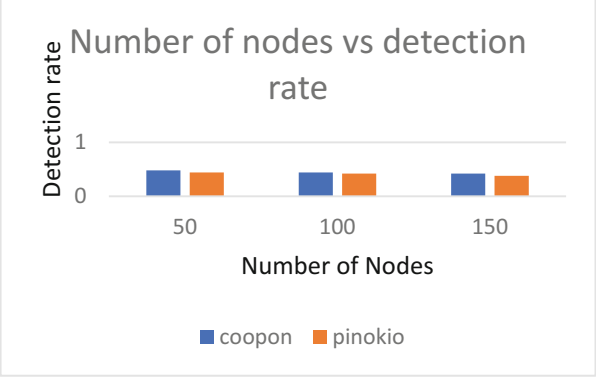

Fig. 6. Number of nodes vs. detection rate with 75% malicious nodes.

In Fig. 6, it can be noted that the performance of the two schemes are almost the same. In this case, 75% of the total nodes were malicious nodes. This proves that the COOPON scheme degrades gracefully with the increasing number of malicious nodes in the network. This indicates that, when the network has a higher percentage of malicious nodes, the COOPON scheme may be outperformed by the Pinokio scheme.

5 Future Work

There is a need to develop a new scheme optimized for the SSDF attacks in cognitive networks. The scheme should be designed to detect many malicious nodes. The scheme should be well designed to ensure that the increasing number of malicious nodes does not degrade its detection rate. We propose a new scheme which employs the extreme studentised deviation test to mitigate the SSDF attack in an ad hoc cognitive radio network. The scheme is designed to counter the effects of a number of malicious nodes. The scheme will be evaluated through numerical and analytical techniques.

6 Conclusion

The comparative evaluation results of the COOPON and Pinokio SSDF attacks mitigation schemes for cognitive radio show that the SSDF countermeasures are also susceptible to the effects of SSDF. Their performance degrades gracefully as the number of the malicious nodes increase in the network. There is need for robust and more resilient SSDF security schemes for better and improved network performance. Alternatively, the current best performing scheme can be modified to enhance the performance of the CRN in the presence of malicious users.

References

1. Monika, B., Chandra, K.R., Kumar, R.R.: Spectrum sensing techniques and issues in cognitive radio. IJETT **4**(4), 695–699 (2013)
2. Dobaria, A., Sodhatar, S.: A literature survey on efficient spectrum utilization: cognitive radio technology. Int. J. Innov. Emerg. Res. Eng. **2**(1), 72–75 (2015)
3. 2015-caps-infocus, 3 December 2015. http://www.capsindia.org/2015-caps-infocus. Accessed 6 June 2016
4. Chetan, M., Subhalakshami, K.: Security issues in cognitive radio. In: Cognitive network: Towards Self-Aware Networks (2007)
5. Xiaofan, H., Huaiyu, D.: A Byzantine attack defender in cognitive radio. In: IEEE International Symposium on Information Theory, Cambridge (2012)
6. Lavanis, N., Jalihal, D.: Performance of p-norm detector in cognitive radio networks with cooperative spectrum sensing in presence of malicious users. Wirel. Commun. Mob. Comput. **2017**(2), 1–8 (2017)
7. Srinu, S., Mishra, A.K.: Efficient elimination of erroneous nodes in cooperative sensing for cognitive radio networks. Comput. Electr. Eng. **52**, 284–292 (2016)
8. Premarathne, U.S., Khalil, I., Atiquzzaman, M.: Trust based reliable transmissions strategies for smart home energy consumption management in cognitive radio based smart grid. Ad Hoc Netw. **41**, 15–29 (2016)
9. Lin, H., Hu, J., Huang, C., Xu, L., Wu, B.: Secure cooperative spectrum sensing and allocation in distributed cognitive radio networks. Int. J. Distrib. Sens. Netw. **2015**, 194–206 (2015)
10. Luo, L., Roy, S.: Analysis of search schemes in cognitive. In: Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON 2007), pp. 647–654, June 2017

11. Pandharipande, A., Kim, J.M., Mazzarese, D., Ji, B.: Wireless RANs: technology proposal package for IEEE 802.22. In: IEEE 802.22 WG on WRANs (2005)
12. Ruiliang, C., Jung-Min, P., Thomas, H.Y., Jeffrey, H.: Toward secure distributed spectrum sensing in cognitive radio networks. IEEE Commun. Mag. **46**, 50–55 (2008)
13. Shei, Y., Su, Y.T.: A sequential test based cooperative spectrum sensing scheme for cognitive radios. In: 2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, Cannes (2008)
14. Khabbazian, M., Kaligineedi, P., Bhargava, V.: Secure cooperative sensing techniques for cognitive radio systems. In: 2008 IEEE International Conference on Communications, Beijing (2008)
15. Rawat, A.S., Anand, P., Chen, H., Varshney, P.K.: Countering byzantine attacks in cognitive radio networks. In: 2010 IEEE International Conference on Acoustics, Speech and Signal Processing, Dallas, TX (2010)
16. Lu, L., Chang, S.-Y., Zhang, J., Qian, L., Wen, J., Lau, V.K.N., Cheng, R.S., Murch, R.D., Mow, W.H., Letaief, K.B.: Technology proposal clarifications for IEEE 802.22 WRAN systems. In: IEEE P802.22 Wireless RANs, May 2006
17. Hillenbrand, J., Weiss, T., Jondral, F.: Calculation of detection and false alarm probabilities in spectrum pooling systems. IEEE Commun. Lett. **9**(4), 349–351 (2005)
18. Tan, K., Jana, S., Pathak, P., Mohapatra, P.: On insider misbehavior detection in cognitive radio networks. IEEE Netw. **27**(3), 4–9 (2013)
19. Jo, M., Han, L., Kim, D., In, H.P.: Selfish attacks and detection in cognitive radio ad-hoc networks. IEEE Netw. **27**(3), 46–50 (2013)