Investigating the Effectiveness of Spectrum Sensing Data Falsification Attacks Defense Mechanisms in Cognitive Radio Ad Hoc Networks

Sekgoari Mapunya(✉), Bokang Makgolane, and Mthulisi Velempini

Department of Computer Science, University of Limpopo, Polokwane, South Africa
{sekgoari.mapunya,mthulisi.velempini}@ul.ac.za

Abstract. Cognitive Radio Networks (CRN) was proposed to improve the utilization of wireless spectrum resources. However, it is susceptible to various security attacks like any other wireless network. CRN technology allows secondary users (SU) to opportunistically utilize the idle spectrum while avoiding interfering with primary users (PU). Spectrum sensing is a key characteristic of this technology and it is the main enabling functionality in facilitating the utilization of free channels by PUs and SUs. Unfortunately, malicious users can interfere with either the PUs or SUs. Spectrum Sensing Data Falsification (SSDF) attack is one of the major attacks in CRN which result in incorrect wrong spectrum access decisions being made which result in interference. There is therefore a need to investigate this attack and design robust SSDF mitigation schemes. In this study, we investigate different approaches to prevent or mitigate SSDF attack and evaluate comparative results of two best mitigation schemes in literature and make recommendations for future research. Three metrics were used for evaluation. These are: missed detection, success and false alarm probabilities which were used to evaluate the performance of the schemes. It is shown though MATLAB simulation results that extreme studentized cooperative consensus spectrum sensing performs better compared to the reputation-based and majority ruling scheme.

Keywords: Spectrum Sensing Data Falsification · Cognitive Radio Ad hoc Network

1 Introduction

The advancement in wireless technology resulted in spectrum congestion due to ever increasing demand for the wireless spectrum [1]. Joseph Mitola proposed cognitive radio network (CRN) as a solution to the problem of spectrum congestions [2]. This is achieved by allowing Unlicensed users/secondary users (SUs) to opportunistically utilize the licensed spectrum band. The Federal Communications Commission (FCC) in 2008 [3] followed by the office of communication in 2010 [4] made a decision to avail the licensed spectrum to unlicensed users. The SUs scan the radio environment to check for the

W. Bao et al. (Eds.): ADHOCNETS 2021/TridentCom 2021, LNICST 428, pp. 72–80, 2022.
https://doi.org/10.1007/978-3-030-98005-4_6

availability of the spectrum bands and utilize them opportunistically. They are expected to vacate them when the signals of the Primary User (PU) are detected. SUs cooperate in using the idle spectrum. Therefore, security is a critical aspect of this technology. Hence, in this paper we focus on Spectrum Sensing Data Falsification (SSDF) also known as the byzantine attack. The attack impacts negatively on the success of CRN since it interferes with spectrum sensing phase which is significant for spectrum access decision making. This attack shares false spectrum occupancy data with its neighbours which results in incorrect spectrum access decisions being made.

The study investigated different types of SSDF attacks, which can be categorized according to their signatures [5]. Greedy SSDF attack is an attacker which reports that a spectrum is occupied by PU yet it's not. This result in an attacker monopolizing a specific band by deceiving other legitimate nodes in assuming that the spectrum is occupied. Malicious SSDF attack is where the attacker's main objective is to cause disruption on the network. A malicious user may send the wrong sensing results to the Fusion Centre (FC) or other nodes. This causes other nodes to assume that there exists a PU which is active in the spectrum when it is not, or it may cause the other nodes to assume that there is no PU occupying the spectrum when the spectrum is not idle. This causes the legitimate users to vacate the spectrum band in the first case and causes interference to the PU in the second case.

Furthermore, the paper compered two best schemes in literature designed to mitigate the SSDF attack. The evaluated schemes are the Reputation-based and Majority ruling scheme [6] and Extreme Studentized Cooperative Consensus Spectrum Sensing (ESCCSS) scheme [7]. The schemes utilize energy detection, which means that the received energy is a proportion of a specific part of the spectrum. The detector compares the computed energy to a threshold value to decide when the channel is free [8].

The rest of this paper is organized as follows: The related work is presented in Section 2. In Section 3, we describe the schemes to be analysed. We present the methodology in Section 4. The comparative results are presented in Section 5. Finally, we conclude and recommend future research direction in Section 6.

2 Related Work

There are a number of studies which sought to address SSDF attack in literature and this section reviews some related works.

The authors in [9] developed a scheme called the Conjugate Prior-Based Detection scheme (CoPD) to mitigate the SSDF attacks in a cognitive radio environment. The scheme isolates false sensing reports generated by Malicious Users (MUs), so that SUs can correctly detect the activities of PUs. The scheme handles the sensing reports from SUs as random variables, then considers the probability density of the random variables through a method known as the Conjugate-Prior. The CoPD can also isolate false sensing reports received from any misbehaving SU. When a sensing report is considered to be false, the sensing report is not included in the final decision making. Therefore, when SUs are clustered, the scheme was not able to achieve the best performance in mitigating the SSDF attacks on the spectrum.

The authors in [10] proposed a Detection Bio-inspired consensus Cooperative sensing scheme. The scheme counters SSDF attacks in a distributed manner. When there is a lack of central entity in an infrastructure-less CRN, users sense the spectrum band and report their local energy data to their neighbors. From the reports gathered from all the users, each user then uses a selection-criteria to isolate reports that are likely to be from attackers. SUs exclude MUs by calculating the mean value of energy. Each node then compares its value with the ones from the neighboring nodes. The node with the most deviation is then regarded as an attacker and the remaining nodes' reports are considered in final decision making. This scheme is based on the assumption that two neighboring nodes can exchange consistently trustworthy data hence, the topology of the network stays unchanged during a given period however, in reality, Cognitive Radio Ad-Hoc Network (CRAHN) topology is dynamic and characterized with frequent topological changes.

In [11], authors proposed a Trust-aware consensus Distributed Cooperative Spectrum Sensing (DCSS) scheme to counteract SSDF attacks. The scheme requires every node to update the trust score of its neighboring nodes. The score serves as an indication of how much a node can be trusted and whether its local decision can be included in the global decision. Thus, they are able to detect the untrustworthiness of a neighbor and isolate its reports from the aggregation of reports in the next update, which helps in achieving better sensing results. This can minimize the number of attacks on a CRAHN environment. The results of the simulation show that the scheme performs well only with one attacker, which means that if attackers are more than one, the performance is degraded.

3 Evaluated Schemes

This Section presents the details of the reputation-based majority ruling and ESCCSS schemes. The two schemes were selected primarily because according to the literature, they are best performing schemes.

Reputation Based and Majority Ruling Scheme
Users sense the spectrum, share their observations and isolate MUs which are known as outliers using the reputation-based system to achieve a well-informed decision. After outliers have been excluded, the Threshold Value (TV) of 60% is used, where if a given SU behaviour exceeds it, then it is classified as an outlier which result in its reports being excluded from the final decision-making process.

The scheme penalizes outliers by incrementing their current reputation value (CRV) so that they reach the TV and risk being excluded from the CRAHN. SUs with a good reputation, will have its CRV unchanged. If malicious SUs stops misbehaving, its reputation can be restored by decrementing it by 1. This is shown in Algorithm 1.

Algorithm 1		
Step 1	:	$if\ s_i(t) < \gamma\ then$
Step 2	:	$d_i(t) = 0$
Step 3	:	$else$
Step 4	:	$d_i(t) = 1$
Step 5	:	$if\ s_i(t) \notin outlier\ then$
Step 6	:	$if\ d_i(t) == g_m(t)\ then$
Step 7	:	$r_{m_i} = r_{mi} + 0.1$
Step 8	:	$else$
Step 9	:	$if\ d_i(t) \neq g_m(t)\ then$
Step 12	:	$r_{mi} = r_{mi} - 1$

Where, m is the device-id of the assessor device.
i is the device-id of the neighbouring device.
$d_i(t)$ is the status of the primary user.
$s_i(t)$ is the value of the report from the neighbouring device i.
$g_m(t)$ is the final decision at device m.
r_{mi} is the current reputation of device i at device m
TV is the threshold value

ESCCSS Scheme

The ESCCSS scheme addresses the impact that might be caused by the greedy attacker (always yes) and the malicious attacker (always no) by isolating altered data from the final decision of the sensing user which is interested in spectrum occupancy. It uses consensus algorithm which enables users to share and arrive at a global decision without the use of a base station or fusion centre.

Each cognitive radio computes $\mathcal{X}\mathrm{i}(n)$as the average of all the observations at each time step j after data has been shared and malicious data have been isolated and consensus algorithm has been executed. The final decision about the spectrum occupancy is done using the following equation:

$$\mathcal{X}\mathrm{i}(n) = \frac{1}{\mathcal{N}} \sum_{j=1}^{\mathcal{N}} \mathcal{Y}j(n) \tag{1}$$

Where $\mathcal{N}$ is the maximum time step at which each SU observes and records energy value, $n$and i is the node index. The computed average is compared to TV in order to make a final decision.

$$\text{Decision} = \begin{cases} 1;\ \mathcal{X}\mathrm{i}(n) > \beta \\ 0;\ otherwise \end{cases} \tag{2}$$

If the average is greater than the threshold then the spectrum is said to be in use denoted by 1, otherwise the spectrum is said to be vacant and SUs can make use of the available spectrum. The scheme is described in Algorithm 2.

Algorithm 2

Step 1 : Sort the received energy values $Y1, \ldots YN$ of N SUs at time k in ascending order. Let this sorted value be denoted by $\mathcal{X}1, \ldots \mathcal{X}N$

Step 2 : Estimate the number of outliers/malicious users U

Step 3 : Compute the mean $\bar{x}$ and s standard deviation of the received energy values $Y1, \ldots YN$

Step 4 : $$\text{Compute } \mathcal{R}j = maxi\left\{\frac{|xi - \bar{x}|}{s}\right\}, \text{j} = 1, 2, \ldots \text{U}$$

Step 5 : After computing $\mathcal{R}j$, Put xi aside that has maximized $|xi - \bar{x}|$

Step 6 : Repeat step 1 to step 5 with estimated outliers been removed, up until j= U

Step 7 : Declare isolated xi's as suspicious data and they are excluded from participating when consensus algorithm is run.

ESCCSS is activated after suspicious data is disregarded from the final decision making. Consensus algorithm is applied by the nodes so that they have the same global view of the network. Thereafter, the average of the consensus value is compared to TV to determine whether the spectrum is available or not.

4 Simulation Model

MATLAB simulation tool installed in Windows 10 operating system was used to simulate the two schemes. The network size was kept constant throughout simulations with 25 nodes. We set the population size of MUs to the following scenarios: 10%, 15% and to 25% of the total nodes in the network. The simulation parameters are listed in Table 1.

Table 1. Simulation parameters.

Parameter	Settings
Simulation time	200 s
Environment	CRAHN
Sus	25
Grid size	1000 m * 1000 m
Propagation model	Tworay ground
Fusion time	.5 s
Mus	10%, 15%, 25%
Sensing type	Energy detection

Table 1 presents simulation parameters which where considered in the simulation of the two mitigation schemes. Energy detection was the sensing type chosen by the authors because the simulated schemes where designed using the same sensing type. The simulated time was set to 200 s.

For the purpose of this research, spectrum sensing is done cooperatively, which implies that SUs sense the spectrum band and then share their observations with neighboring nodes prior to making a final decision about whether the spectrum is occupied or not. Both schemes utilized cooperative spectrum sensing, and are also affected by noise uncertainty, fading and shadowing [12].

5 Results

To evaluate the performance of the schemes effectively, we used different types of metrics. These are false alarm probability, success probability, and missed detection probability. The schemes were simulated in a CRAHN environment in a network with 25 nodes. In each scenario, we considered different percentages of MUs which were: 10%, 15% and 25% to have an in deep analysis of how the schemes perform under different network conditions. The missed detection Probability results are presented in Fig. 1.

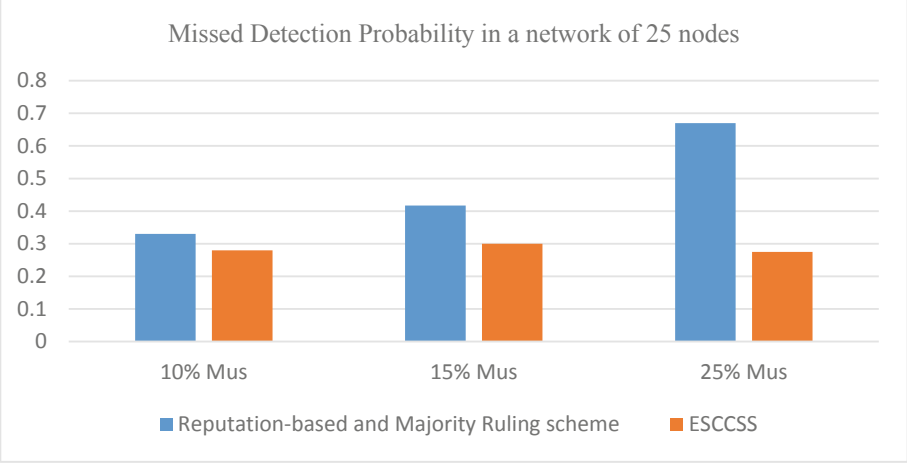

Fig. 1. Missed detection probability in a network of 25 nodes.

Figure 1 shows that in a network with 25 nodes were the reputation-based and majority ruling scheme was used, the missed detection probability is slightly higher compared to ESCCSS when there is 10% of MUs in the network. However, as the number of MUs increased in the network, the missed detection probability of the ESCCSS decreased while the reputation-based and majority ruling scheme increased.

Figure 2 depicts the success probability results. The success probability indicates the ratio of the scheme's accuracy in sensing the SSDF attacks and MUs in a CRAHN and then mitigate the attacks by disregarding the falsified reports and use results non-malicious users. The results presented are from different network scenarios consisting of different number of nodes.

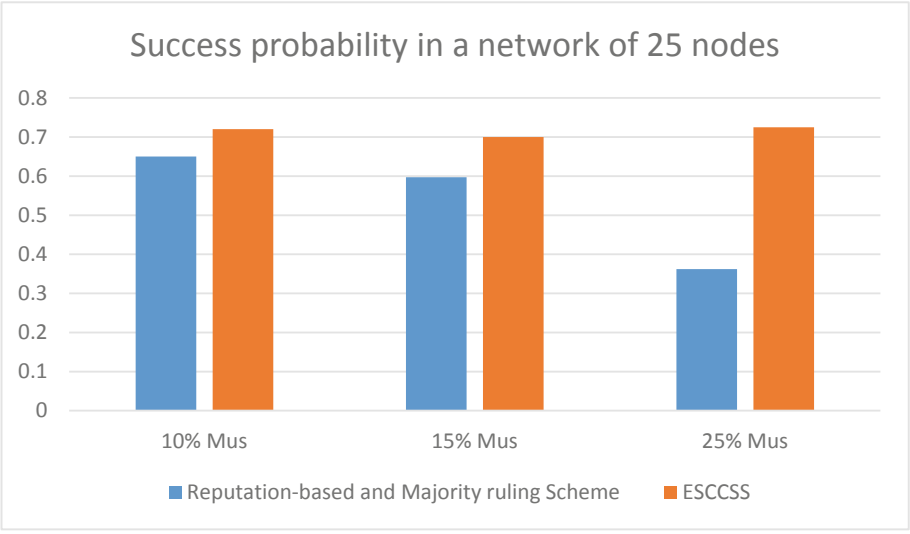

Fig. 2. Success probability in a network of 25 nodes.

In the simulation results of a network containing 25 nodes, we observed that when we have a small percentage of MUs (10%) in the network or even a high percentage (25%), the reputation-based and majority ruling scheme's performance was poor compared to ESCCSS. However, as the number of MUs increased, the success probability of the reputation-based and majority ruling scheme decreased, meaning that the scheme fails to detect accurately the SSDF attacks in CRAHN compared to ESCCSS.

The false alarm probability results are depicted in Fig. 3. We observed that as the number of MUs increased, the probability of false alarm of reputation-based and majority ruling scheme increased which shows that the scheme was not able to handle even a small percentage of MUs in the network.

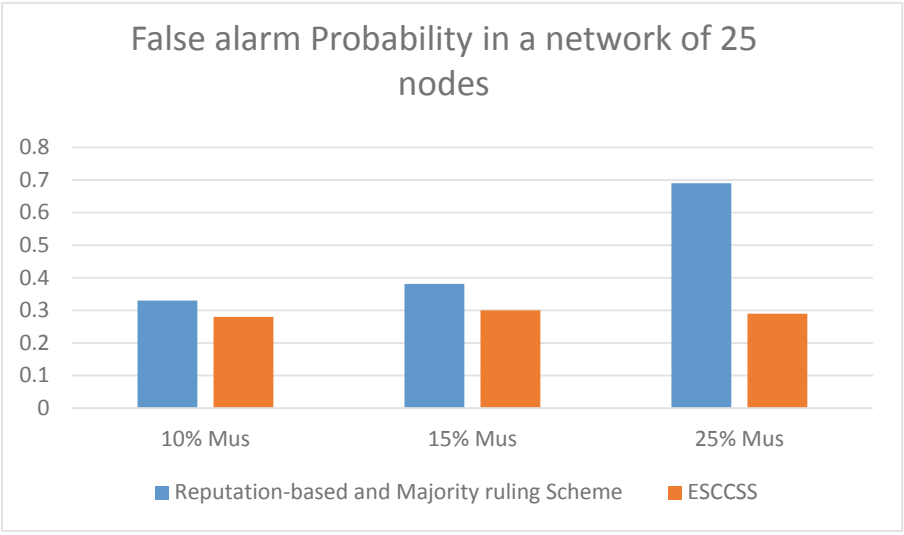

Fig. 3. False alarm probability in a network of 25 nodes

6 Conclusion

This work evaluated two types of SSDF attacks, which are the MU attack and the greedy SSDF attack. We presented comparative results of the two schemes designed to mitigate the SSDF attack. We compared the performance of the schemes with regard to the probability of missed detection, success probability and probability of false alarm.

The simulation results showed that the ESCCSS scheme is a better performing scheme in mitigating the SSDF attacks in CRAHN. Furthermore research may be conducted to evaluate the efficiency of the ESCCSS scheme in a CRAHN environment with different number of nodes and different network conditions such as cooperative or non-cooperative nodes may be considered.

7 Future Work

There is a need to develop a scheme that detects MUs earlier than ESCSS. Hence, during the simulation it was observed that both schemes starts detecting MUs after 100 s of running the simulation. We propose the use of advanced machine learning techniques in addressing the effects of this attack. The scheme may be evaluated using both a testbed and simulation techniques.

References

1. Cordeiro, C., Challapali, K., Birru, D.: IEEE 802.22: the first worldwide wireless standard based on cognitive radios. In: First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005, pp. 328–337. IEEE (2005)

2. Mitola, J.: Cognitive radio for flexible mobile multimedia communications. In: 1999 IEEE International Workshop on Mobile Multimedia Communications (MoMuC 1999) (Cat. No. 99EX384), pp. 3–10. IEEE (1999)
3. Commission, F.C.: In the Matter of Unlicensed Operation in the TV Broadcast Bands and Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3 GHz band. Second Report and Order and Memorandum Opinion and Order FCC 08-260. Washington, D.C. (2008)
4. https://stakeholders.ofcom.org.uk/binaries/consultations/cog-nitive/statement/statement.pdf
5. Fragkiadakis, A.G., Tragos, E.Z., Askoxylakis, I.G.: A survey on security threats and detection techniques in cognitive radio networks. IEEE Commun. Surv. Tutorials **15**, 428–445 (2012)
6. Ngomane, I., Velempini, M., Dlamini, V.: Detection and mitigation of the spectrum sensing data falsification attack in cognitive radio Ad Hoc networks. In: 2018 Conference on Information Communications Technology and Society (ICTAS). Durban, South Africa (2018)
7. Mapunya, S., Velempini, M.: The design of byzantine attack mitigation scheme in cognitive radio ad-hoc networks. In: 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), pp. 1–4. IEEE (2018)
8. Rawat, A.S., Anand, P., Chen, H., Varshney, P.K.: Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks. IEEE Trans. Signal Process. **59**, 774–786 (2010)
9. Chen, C., Song, M., Xin, C.: CoPD: a conjugate prior based detection scheme to countermeasure spectrum sensing data falsification attacks in cognitive radio networks. Wireless Netw. **20**(8), 2521–2528 (2014). https://doi.org/10.1007/s11276-014-0758-2
10. Chen, R., Park, J.-M., Reed, J.H.: Defense against primary user emulation attacks in cognitive radio networks. IEEE J. Sel. Areas Commun. **26**, 25–37 (2008)
11. Limbasiya, T., Das, D., Yadav, R.N.: A Reputation-based trust management model in multihop cognitive radio networks. In: Sa, P.K., Bakshi, S., Hatzilygeroudis, I.K., Sahoo, M.N. (eds.) Recent Findings in Intelligent Computing Techniques: Proceedings of the 5th ICACNI 2017, Volume 2, pp. 183–192. Springer Singapore, Singapore (2018). https://doi.org/10.1007/978-981-10-8636-6_20
12. Akyildiz, I.F., Lo, B.F., Balakrishnan, R.: Cooperative spectrum sensing in cognitive radio networks: a survey. Phys. Commun. **4**(1), 40–62 (2011)