SACJ 31(2) December 2019
Research Article

The design and implementation of a robust scheme to combat the effect of malicious nodes in cognitive radio ad hoc networks

Sekgoari Semaka Mapunya, Mthulisi Velempini

Department of Computer Science, University of Limpopo, Sovenga, South Africa

ABSTRACT
A cognitive radio network, which enables dynamic spectrum access, addresses the scarcity of radio spectrum caused by ever-increasing demand for spectrum. Cognitive radio technology ensures the efficient utilisation of underutilised licenced spectrum by secondary users (SUs). SUs sense the radio environment before utilising the available spectrum to avoid signal interference. The SUs cooperatively sense the spectrum to ensure a global view of the network. Unfortunately, cooperative sensing is vulnerable to Byzantine attacks whereby SUs falsify the spectrum reports for selfish reasons. Hence, this study proposes the implementation of a scheme to combat the effects of Byzantine attack in cognitive radio networks. The proposed scheme, known as the extreme studentized cooperative consensus spectrum sensing (ESCCSS), was implemented in an ad hoc cognitive radio network environment where the use of a data fusion centre (DFC) is not required. Cognitive radio nodes perform their own data fusion before making spectrum access decisions. They fuse their own reports with reports from neighbouring nodes. To evaluate the performance of our scheme and its effectiveness in combating the effect of Byzantine attack, comparative results are presented. The comparative results show that the ESCCSS outperformed the Attack-Proof Cooperative Spectrum Sensing scheme.

Keywords: byzantine attack, cognitive radio networks, secondary users

Categories: • *Networks ~ Network security* • *Networks ~ Ad hoc networks*

Email:
Sekgoari Semaka Mapunya sekgoari.mapunya@ul.ac.za (CORRESPONDING),
Mthulisi Velempini mthulisi.velempini@ul.ac.za

Article history:
Received: 08 Jun 2019
Accepted: 24 Oct 2019
Available online: 20 Dec 2019

1 INTRODUCTION

As there are more innovations and more technologies, there is a need for more spectrum bands due to spectrum over-crowding caused by those technologies (Singh, Upadhyay, Lee, & Costa, 2019). It was observed that as unlicensed spectrum are being over-crowded, licensed spectrum bands are underutilised (Abognah & Basir, 2015; Mehdaw, Riley, Paulson, Fanan, & Ammar, 2013). Given these spectrum challenges, the cognitive radio technology was proposed as a possible solution to the

Mapunya, S.S. and Velempini, M. (2019). The design and implementation of a robust scheme to combat the effect of malicious nodes in cognitive radio ad hoc networks. *South African Computer Journal 31*(2), 178–194. https://doi.org/10.18489/sacj.v31i2.713

SACJ is a publication of the South African Institute of Computer Scientists and Information Technologists. ISSN 1015-7999 (print) ISSN 2313-7835 (online).

underutelization of licenced spectrum and overcrowding of unlicensed spectrum (Mitola & Maguire, 1999). However, the cogitive radio technology is a wireless technology which is susceptible to security challenges.

Security is a major challenge in wireless networks because of the openness of the communication channels. The air interface and the open wireless standard are vulnerable to security attacks (Zou, Zhu, Wang, & Hanzo, 2016). Data is transmitted through the air interface which is susceptible to man-in-the-middle attacks such as the interception of data in transit (Mirsky, Kalbo, Elovici, & Shabtai, 2019). Cognitive radio technology is also susceptible to all wireless related generic attacks. However, due to CRNs capabilities, such as spectrum sensing, spectrum decision, and spectrum data sharing, new security challenges have emerged. For example, if false spectrum sensing results are broadcasted by a malicious user (MU) or an attacker, spectrum access decisions based on false data, affect the utilisation of the spectrum (Wan, Ding, Xiong, & Zhou, 2019). This results in either interference with the Primary User (PU) or monopolisation of spectrum use by a MU.

This paper focuses on Byzantine attacks also known as the spectrum sensing data falsification attacks (SSDF). This attack has a major impact on the functionality of the cognitive radios. It interferes with the cognitive cycle of the radios which leads to interference with other cognitive radios and PUs (Mapunya & Velempini, 2018b). Malicious nodes, known as Byzantine nodes, can report false sensed data which leads to harmful spectrum access decisions. The Byzantine node can report that a spectrum is occupied while it is, in fact, idle. On the other hand, it can report an occupied channel as idle. This leads to the underutilisation of the spectrum and PU interference. Given the challenges of the Byzantine attack, the main objective of the CRNs, which is to address the underutilisation of the spectrum without causing any interference with PU, is therefore not realised (Yawada & Dong, 2019).

This paper is organised as follows. Section 2 presents related work. Section 3 discusses the design of the proposed scheme while Section 4 provides an in-depth description of the simulation environment. Section 5 then presents the graphical representation of the results and the discussion. Finally, Section 6 presents the conclusion of the study.

2 RELATED WORK

Several schemes have been proposed to address the effects of security threats associated with spectrum sensing. Most of these proposed schemes are based on a centralised model of cooperative spectrum sensing. However, gaps still exist in the infrastructure-less CRNs (Mapunya & Velempini, 2018a).

The performance of various algorithms which implement a fusion centre were evaluated in Lavanis and Jalihal (2017). The detection of the SSDF attack is a challenge in these schemes. The standard and p-nom energy detector algorithm was assessed under the assumption that a Gamma and Gaussian distribution of the test statistics was implemented. The comparative results demonstrate that the Gaussian assumption for distribution of test statistics performs better in combating the SSDF attack compared to the Gamma assumption. The experiment was carried out with the assumption that the network is populated with a very small percentage of attacking nodes. It is not guaranteed that the algorithm will perform well in a network with a higher percentage of MUs.

In Lu, Wei, and Chen (2014) an SSDF attack mitigation scheme which is based on the hard decision technique was proposed. The scheme uses the Gaussian approximation of Binomial distribution to detect and isolate MUs participating in cooperative spectrum sensing (CSS). The scheme was evaluated in a network with 50 nodes. The scheme may not function well in large networks hence its robustness may be evaluated in larger networks. In our work five different sizes of networks ranging from 10 to 100 nodes were considered.

In Sodagari, Attar, Leung, and Bilén (2012) schemes designed to counter a number of different classes of attacks which are based on the prior knowledge of the cognitive radios were proposed. The schemes detect and isolate the malicious reports. The implementation of the weighted sensing fusion mechanism in CRNs can reduce the impact of attacks in cognitive radio networks (2012). The assumption that the network has only five malicious nodes does not assess effectively the effectiveness of the scheme when the number of MUs is increased.

An extension of the generalised extreme studentized deviate test algorithm was proposed by Srinu and Mishra (2016) to address the effects of malicious SUs in cognitive radio networks. The proposed scheme can only function in a network with a fusion centre. The scheme detects MUs using the Shapiro–Wilk test and it is effective in detecting and isolating Byzantine attacks, however, it is a centralised CSS scheme. This study addresses Byzantine attacks in decentralised CRN. However, extreme studentized deviation test as the base of this work was also implemented in our scheme to address the effects of the Byzantine attack.

A novel multi-attribute, trust-based framework which facilitates dependable spectrum sensing and priority-based spectrum access allotment to support delay sensitive data transmissions was proposed in Premarathne, Khalil, and Atiquzzaman (2016). The simulation results show that the effectiveness of the scheme is 91.42%. The network was assumed to be subjected to the always-on attack only. The proposed scheme may not be reliable when different types of attacks are encountered. MATLAB was also used to evaluate the efficiency of our scheme when different types of attacks.

In Lin, Hu, Huang, Xu, and Wu (2015) a distributed CSS and cheat-proof spectrum allocation strategy was proposed. The scheme integrated the dynamic reputation model and the Vickrey-Clarke-Groves mechanism. It was proven through the analytical and simulation results that the scheme can detect and isolate SSDF attacks in cognitive radio ad-hoc networks. The performance of the scheme was evaluated against a distributed random scheme and the results show that it is superior (Luo & Roy, 2007).

A novel trust-aware, gossip-based scheme was proposed for distributed cognitive radio networks and was designed to improve the performance of the CSS in the presence of MUs (Vosoughi, Cavallaro, & Marshall, 2014). Push-sum protocol is the bases of this scheme and it is a novel consensus-based scheme (Kempe, Alin, & Johannes, 2003). Using gossip, the average values stored by each node are calculated and these values are stored using the push-sum protocol. Gossip protocols are distributed algorithms where every node transmits its own value to a random node at a given time step. The trust score was incorporated into the original push-sum algorithm to make it more resilient to SSDF attack.

The goal of every node is to assess its neighbours trustworthiness and ignore the report from untrustworthy neighbours. Furthermore, the study showed that consensus-based systems are more vulnerable to SSDF attacks. It is evident that the proposed scheme improves significantly the detection rate of the network in the presence of malicious nodes. However, it might cause delays due to the slow convergence. The proposed scheme was simulated in a scenerio with a single PU. This work also assumed the availability of one PU in all the scenerios.

Two block outlier detection methods based on Tietjen-Moore (TM) and Shapiro-Wilk (SW) tests were proposed in Srinu and Mishra (2016) to mitigate the effects of the MUs in CSS. The box plot and median absolute deviation (MAD) tests were compared to the proposed mitigation scheme. The robustness of TM and SW in comparison to statistical and random attack performed better than the box plot and MAD tests. A new type of attack was observed, called the cooperative SSDF attack, which involves cooperating MUs. Monte Carlo simulations were used to show that the largest gap and clustering method fail to estimate accurately the number of outliers in cooperative attack. To address this shortcoming, a modified largest gap method which can estimate accurately the number of outliers under cooperative attack was proposed.

3 SYSTEM MODEL

We investigated a number of Byzantine attack countermeasures and evaluated their weaknesses and strengths in the previous section. In this section, we discuss the proposed Extreme Studentized Cooperative Consensus Spectrum Sensing (ESCCSS). It incorporates the extreme studentized deviate test which makes the scheme more robust. The scheme was evaluated and its performance was compared to the Attack-Proof Cooperative Spectrum Sensing (APSCC).

Our proposed scheme is based on a cooperative spectrum sensing and sharing whereby each node in the network is responsible for observing and constructing information about its neighbourhood, and then sharing it with the rest of the nodes through a common control channel.

A consensus algorithm assists in the sharing of data and in decision making regarding the availability of the spectrum band. ESCCSS is a cooperative spectrum sensing and a consensus-based scheme. Distributed spectrum sensing was proposed to address the problem of link and node failure.

SUs share spectrum observations with their neighbours and the spectrum access decision is made by each SU based on both global and local observations through the use of the consensus algorithm.

SUs cooperate in sensing the spectrum to ensure that all the nodes have a global view of the network / environment and to ensure accuracy without the use of a fusion centre. Spectrum observations are shared amongst SUs with each SU making a final spectrum access decision based on the final converged value obtained from the fusion of the received observations from neighbouring nodes through the use of the consensus algorithm. The proposed scheme can be summarised as follows:

1. At time $t = 0$, we initialise $k = 0$, each SU initially transmits its local observation to its neighbours during this step resulting in vector $[b_1(k)\dots, b_m(k)]$.

2. The received local observations are then sorted in ascending order.

3. Each node estimates the number of falsified data denoted by u, at $k = 0$.
4. Each node computes the mean $\bar{x}$ and standard deviation s of the received observations from its neighbours and its own observation.
5. Then compute

$$R_j = \max_i \frac{|x_i - \bar{x}|}{s} \qquad j = 1, 2 \ldots, u \tag{1}$$

   where x_i is energy detected value from the sorted vector.
6. After computing R_j, find the value of x_i that maximises $|x_i - \bar{x}|$, this is flagged as an outlier.
7. Isolate outlier x_i from the sorted local observations and repeat steps 2 to 6 with estimated outliers $j = u$ and $k = 1, \ldots, K$
8. exclude isolated data from participating in step 9 after classifying them ($x_i's$) as suspicious data
9. Subsequent to isolating false data at each successive time step ($0 < k < K$), each SU fuses these observations together with the received observations from past time steps, through a mixing function which generates a new observation $b(k)$ (Seif, ElBatt, & Karim, 2016). This new observation is transmitted to the neighbouring nodes at the current step k. This can be mathematically expressed as follows:

$$b(k) = F(b(n), n = 0, \ldots, k-1), \qquad 0 < k < K \tag{2}$$

   where $F(.)$ is the combining function.
10. When ($k = K$) the consensus algorithm terminates, at this point each SU makes a final decision individually regarding the availability of the spectrum. The $b(K)$ function is compared to a threshold value. This can be expressed as:

$$G = \begin{cases} 0 & b(K) < \alpha \\ 1 & \text{otherwise} \end{cases} \tag{3}$$

   where α, a threshold value of 3.5, is regarded as the middle value of possible energy detected values. The energy values range from zero to seven. At this stage, SUs can make a correct decision to access the available spectrum. If the final decision is 0, it means that the spectrum is available otherwise it is unavailable.

Figure 1 presents the flow chart of the spectrum access decision which guides the cognitive radios. Cognitive radios start by sensing the radio environment to locate spectrum holes. As the spectrum observation information is shared amongst cognitive radios, the proposed scheme is activated. The falsified information is detected and isolated when the consensus algorithm combines all the information received by each cognitive radio enabling all the SUs to converge. Finally, the converged information is compared to a threshold value resulting in a cooperative spectrum availability decision being made. If the spectrum is available the SUs can transmit in the available band otherwise, the spectrum sensing restarts.

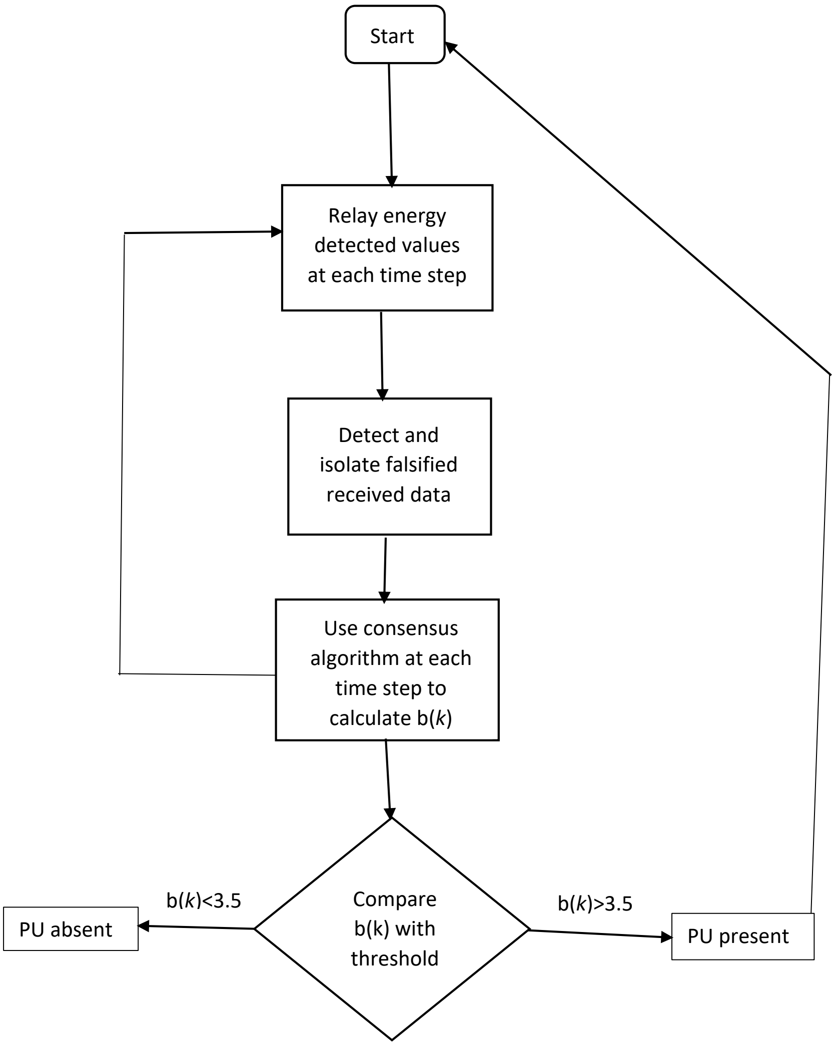
Start
Relay energy detected values at each time step
Detect and isolate falsified received data
Use consensus algorithm at each time step to calculate b(*k*)
Compare b(k) with threshold
b(*k*)<3.5
PU absent
b(*k*)>3.5
PU present

Figure 1: Spectrum access decision making in the presence of malicious users

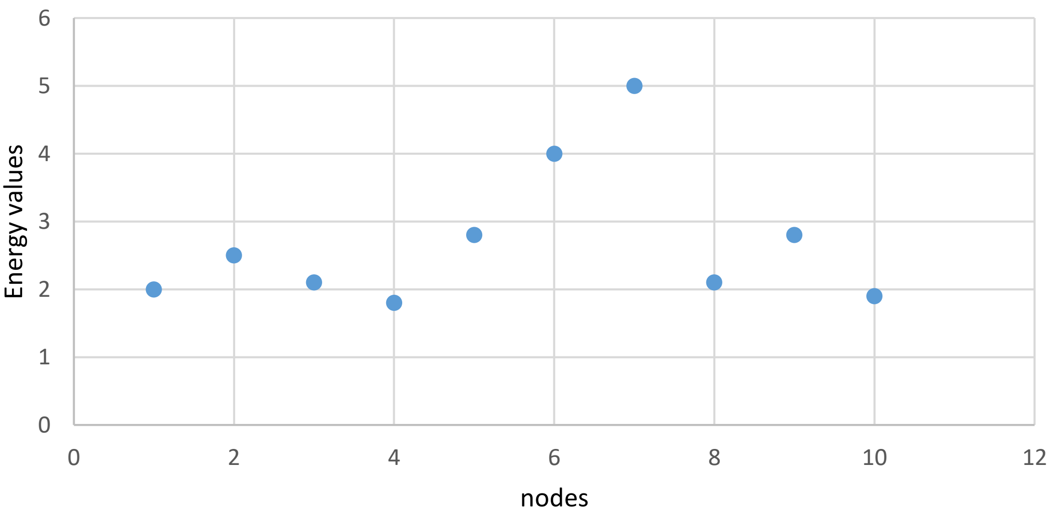

Figure 2: Energy detected values by nodes at time $t = 0$ where 10% of those nodes attacking

Figure 2 presents details of the proposed scheme. In a network populated with 10 nodes and 10% of those nodes being malicious, it can be seen that two of the nodes report data which is out of the range. The purpose of the scheme is to identify such reports and exclude them from the final spectrum occupancy decision making. If the falsified data are not isolated, the spectrum may be underutilized or monopolized by selfish MUs and the potential of cognitive radio networks won't be realized. The falsified data leads to wrong overall spectrum availability decision making.

4 SIMULATION MODEL

The network size and the number of malicious nodes in the network were varied in different simulation scenerios to effectively evaluate the efficiency of the scheme. The evaluation was done using different network sizes which ranged from a small-sized network to a large-sized network. This was done by varying the number of the malicious nodes from 10% to 15% and then to 25%. The simulation parameters used in the evaluation are presented in Table 1.

The proposed scheme was simulated in the MATLAB environment because it is widely used in this research area. Therefore, It is an effective tool to simulate the proposed scheme.

The spectrum sensing can be conducted in one of the two ways, either cooperatively or non-cooperatively. Cooperatively is where the SUs sense the spectrum band and share the information with each other before making the final transmission decision.

Non-cooperatively is where a SU senses the spectrum band and makes the spectrum access decision without cooperating with neighbouring nodes. In this research, cooperative spectrum sensing was considered because it is more effective than non-cooperative spectrum sensing.

Table 1: List of parameters

Parameters	**Settings**
Antenna type	OmniAntenna
MAC protocol	IEEE 802.11 with extension to support CR networks
Data channels	8
Common control channel	1
Channel data rate	11 Mbit/s
Number of SUs	10, 15, 25, 50, 100
Number of selfish SU	10%, 15%, 25%
Propagation model	TwoRayGround
Grid size	1000m x 1000m
Primary user detection type	Energy detection
Mobility type	Random waypoint model
Sensing type	Cooperative spectrum sensing
Threshold α	3.5
Performance metrics	false alarm probability, missed detection probability, success probability

5 RESULTS AND DISCUSSION

We evaluate the performance of the proposed Byzantine attack mitigation scheme, the ESCCSS and compare it to the APSCC (Liu, Gao, Guo, & Liu, 2010). APSCC is closely related to our work however in our proposed scheme we used the generalised studentized deviate test. The APSCC makes use of the consensus algorithm and it is optimised to work in an ad hoc cognitive radio network environment. According to literature, the APSCC is the best performing scheme (Liu et al., 2010). This is the basis for the selection of the APSCC and comparison to the ESCCSS scheme.

A number of simulation scenarios were considered in this evaluation. The size of the networks and the percentage of attacking nodes ranged from 10 to 100 nodes and 10% to 25% attacking nodes respectively. We evaluated the performance of the two schemes based on the following metrics: probability of false alarm (FAP), missed detection (MD), and success probability.

The performance of the ESCCSS in addressing the different types of Byzantine attacks in different sized network scenarios was examined. Figure 3 presents the FAP where there is 10% of MUs in the network ranging from 10 to 100 nodes.

The false alarm probability results in Figure 3 show that in all the considered scenarios, our proposed scheme significantly reduced FAP compared to APCSS. In a scenario with 10 nodes and only one malicious node, ESCCSS achieved a good FAP which is below 0.2 while the APCSS's FAP is above 0.6. In Figure 4, where there was 15% of the nodes being malicious, the ESCCSS scheme also achieved good results. The ESCCSS scheme managed to isolate most of the data from MUs in the final decision making.

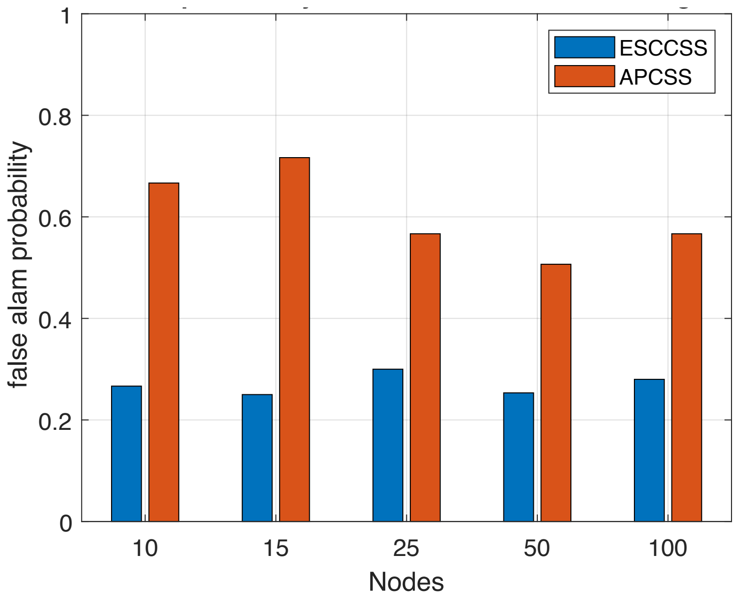

Figure 3: False alarm probability with 10% attacking nodes

The APCSS isolates falsified data based on the following expression $(\mu_i(k)-\gamma_c)(\mu_i'-\gamma_c)<0$ which sometimes fails to make a correct decision. If the difference between $\mu_i(k)$ and μ_i' is large enough, then $(\mu_i(k)-\gamma_c)(\mu_i'-\gamma_c)<0$ becomes greater than 0, therefore concluding that the tested data is correct which might not be the case. This ultimately results in the failure to reduce the FAP.

When 15% of the total nodes were set to be attacking nodes, it was observed that the ESCCSS significantly reduced the FAP in comparison to APCSS in all the scenarios as shown in Figure 4. The APCSS was therefore outperformed by ESCCSS as it failed to reduce FAP significantly.

The performance results of the scheme in a network with 25% malicious nodes are presented in Figure 5.

The ESCCSS scheme outperformed the APCSS scheme in these scenerios. The poor performance of APCSS can be attributed to its failure to detect and isolate all the malicious data due to the large gap between $\mu_i(k)$ and μ_i' while ESCCSS was able to detect and isolate all the incorrect data.

In the following set of results, we evaluate the perfomance of the two schmes on the bases of the MD metric. MD occurs when a PU is detected to be idle yet it is active in the given spectrum band. Figure 6 presents the MD probability of the two schemes in a network consisting of 10% malicious nodes.

A reduced MD probability is desirable for better performance. Figure 6 shows that the ESCCSS reduces the MD probability. It also outperformed the APCSS scheme. As the network size was increased, the ESCCSS scheme consistently performed better that the APCSS scheme. In a small network size (10 and 15), it was observed that the APCSS recorded a very high MD probability (0.63) while the ESCCSS reduced the MD probability by 0.45 and at least by 0.3 respectively.

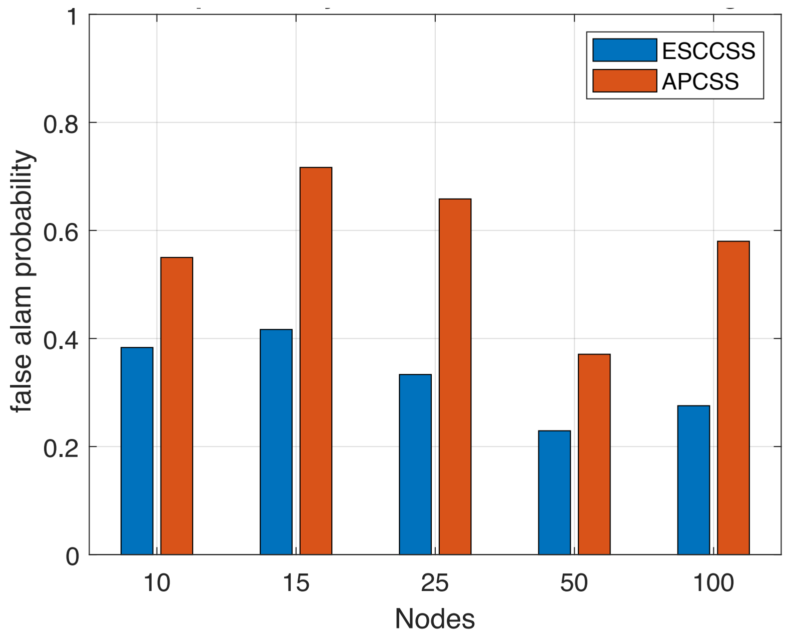

Figure 4: False alarm probability with 15% attacking nodes

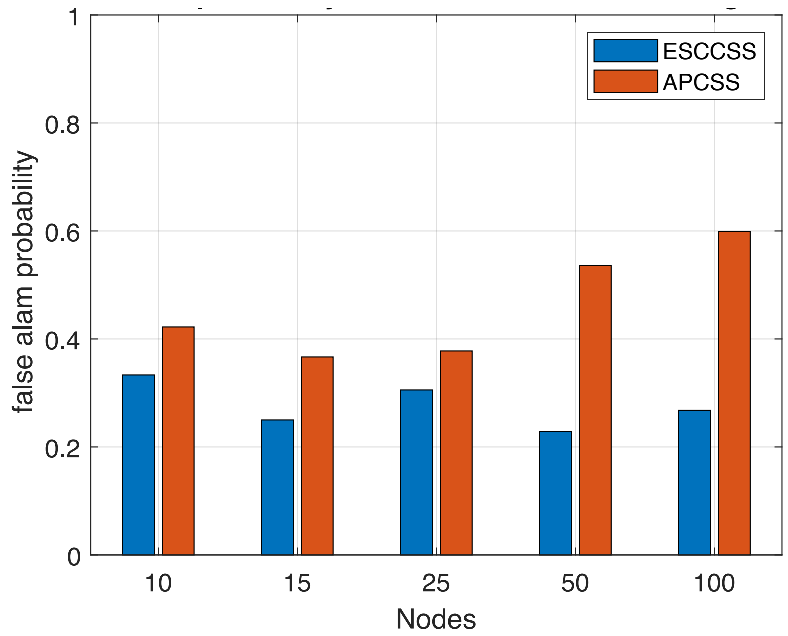

Figure 5: False alarm probability with 25% attacking nodes

https://doi.org/10.18489/sacj.v31i2.713

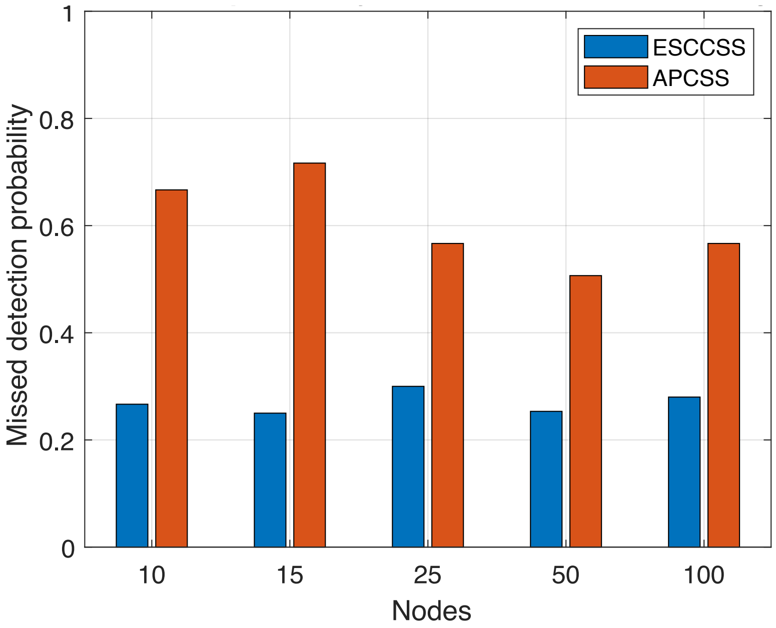

Figure 6: Missed detection probability in a network with 10% attacking nodes

https://doi.org/10.18489/sacj.v31i2.713

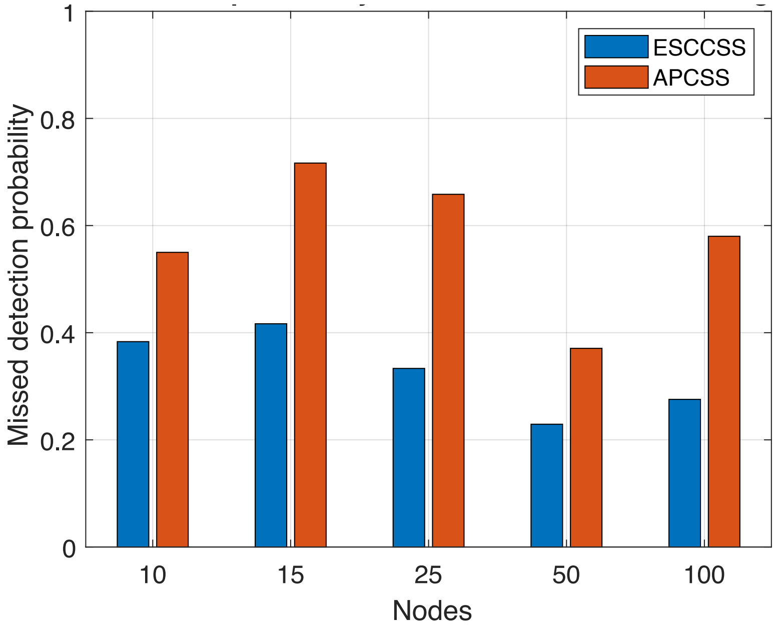

Figure 7: Missed detection probability in a network with 15% attacking nodes

Though the ESCSS posted very good results, it was not able to achieve 0% MD because the attacking nodes does not falsify all the sensed data and it also misses some false reports. Furthermore, non malicious nodes can occasionally behave like a malicious nodes due to some environmental challenges such as multipath and signal fading.

The Always Yes attack falsified the data in cases where low PU signals were sensed and the Always No attack falsified data where high PU signals were detected. The ESCSS recorded low MD probability because the extreme studentized deviate test was implemented and it managed to detect most outlying data. Figure 7 presents the MD probability simulation results of the ESCSS in comparison to APCSS results.

The results show that in a network compromised by 15% of the total nodes being malicious, the ESCSS outperformed the APCSS. It is evident that as the network size increased, ESCCSS continued to post good results as compared to the APCSS. This can be observed in all the network scenarios. The ESCCSS achieved less than 0.36 MD probability while APCSS recorded the MD Probability which is more than 0.49 in all the scenarios. The APCSS scheme failed to correctly detect and isolate all the falsified data due to this detection criterion $(\mu_i(k)-\gamma_c)(\mu_i'-\gamma_c) < 0$. When the network has 15% of attacking nodes, we can conclude that ESCCSS performed better. We then increased the number of malicious nodes in Figure 8 to 25%.

When the network size is small (10 to 25 nodes), ESCCSS achieved a marginal improvement. As the network size increased, the perfomance of ESCCSS improved. The ESCCSS is therefore more efficient in large networks with 25% attacking nodes. This is caused by the fact that at this point, the proposed scheme can still detect and isolate most of the falsified data while APCSS fails to detect even at least 50% of falsified data since there is a significant gap between $\mu_i(k)$ and μ_i' in available

https://doi.org/10.18489/sacj.v31i2.713

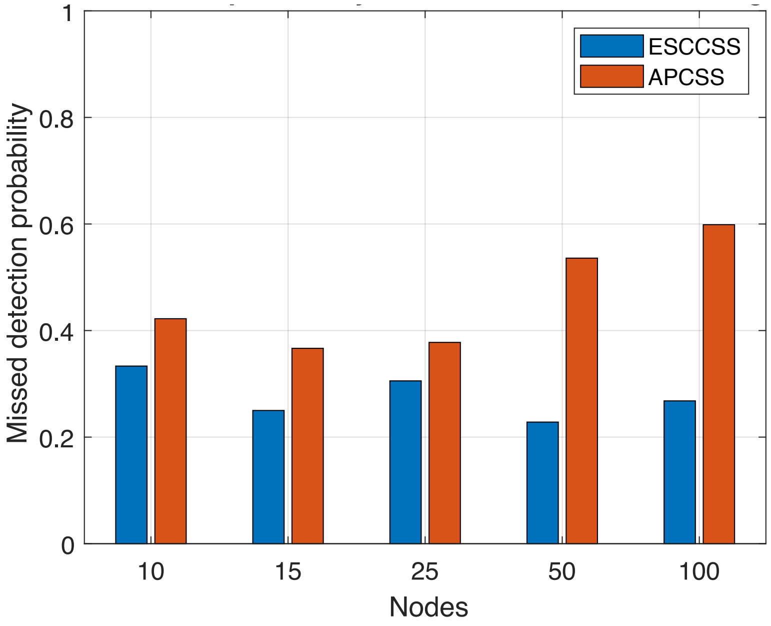

Figure 8: Missed detection probability in a network with 25% attacking nodes

data to be tested. The effects of outliers are more evident where the number of malicious nodes is high.

Figures 9–11 present the comparative success probability results of ESCCSS and APCSS schemes. Figure 9 presents the success probability results of ESCCSS in networks with varying number of nodes. However, the number of attacking nodes was kept constant.

In a small network, the ESCCSS scheme detected a higher number of attacking nodes compared to APCSS scheme, as shown in Figure 8. As the network size was increased, the success probability of ESCCSS in general also decreased, while the APCSS's success probability increased. However, the ESCCSS outperformed the APCSS scheme in all the network scenarios. The ESCCSS detected all falsified data and isolated them from spectrum availability decision making. The success probability was also investigated in a network scenario with 15% attacking nodes. The results are presented in Figure 10 for both ESCCSS and APCSS.

Figure 10 shows that ESCCSS performed better in comparison to the APCSS. The ESCCSS recorded the highest success probability when the number of nodes in the network were 15, and 2 of those nodes were malicious. The network size was populated with a reasonable number of MUs and they were detected by ESCCSS since it is configured to detect earlier, the suspicious nodes. Figure 11 presents the results of the schemes when the percentage of malicious nodes was increased to 25%.

Figure 11 shows that as the network size increases, the success probability also increases. It can be seen that when the network size is small, the performance of the ESCCSS scheme is marginally better than the performance of the APCSS scheme. It then improves as the network size increases.

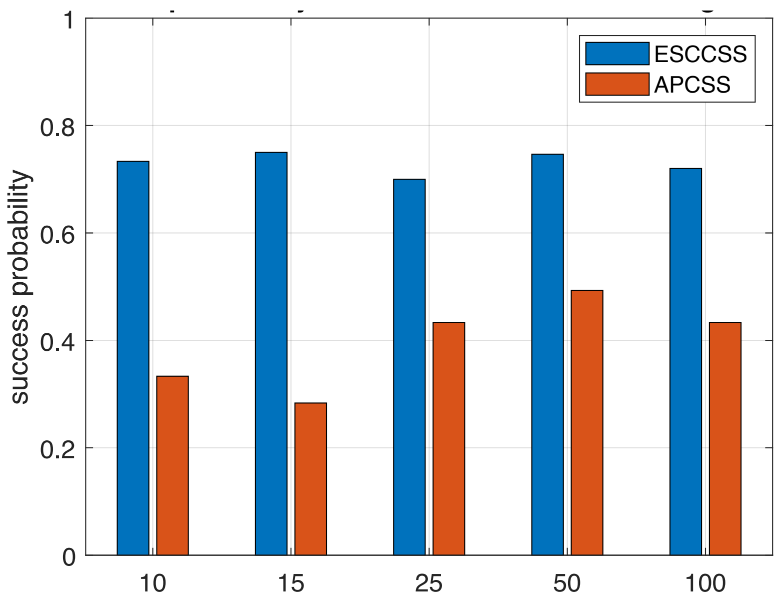

Figure 9: Success probability in a network with 10% attacking nodes

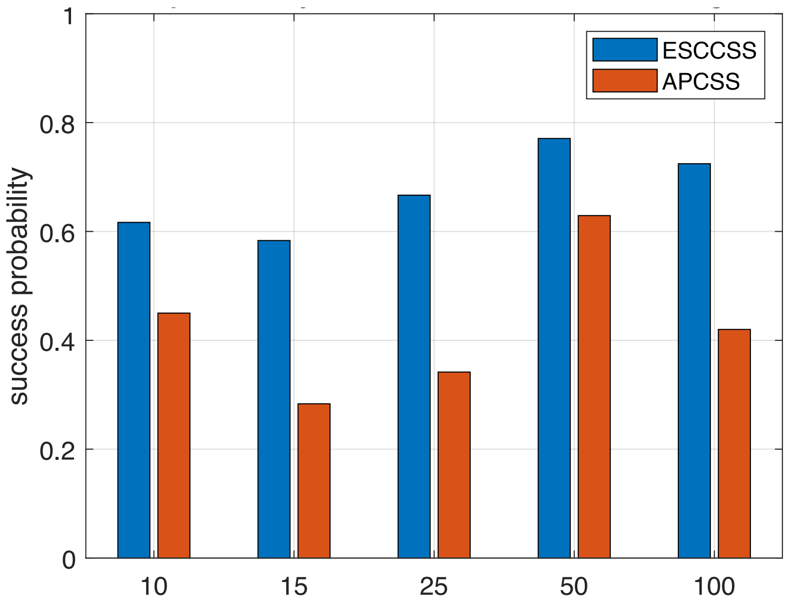

Figure 10: Success probability in a network with 15% attacking nodes

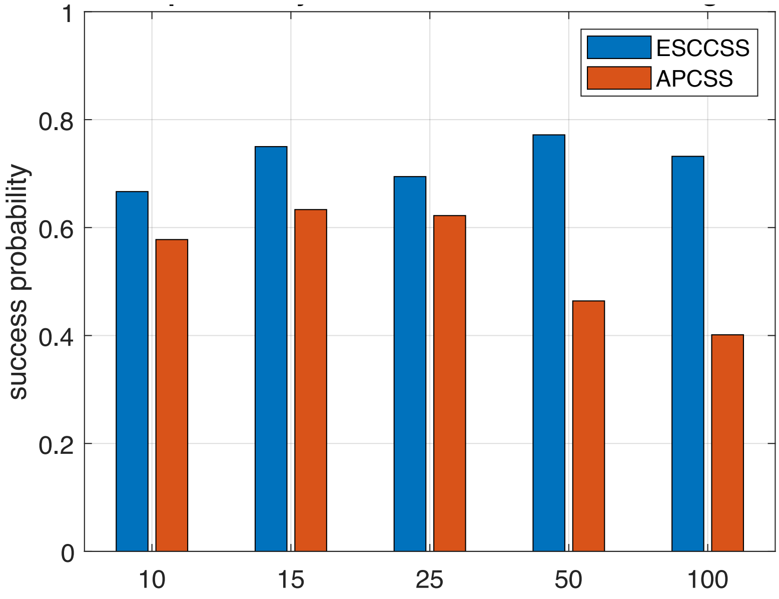

Figure 11: Success probability in a network with 25% attacking nodes

6 CONCLUSION

The main objective of this work was to design and implement a Byzantine attack mitigation scheme in cognitive radio ad hoc networks. The objective was to isolate falsified data regarding the availability of spectrum. The false data mislead SUs in spectrum access decision making. The proposed statistical approach used in isolating falsified data was integrated with the cooperative spectrum sensing technique. The results show that the extreme studentized deviate test isolated data from outliers in the shared data set from all nodes at time K. Based on the quantitative simulation results, we can conclude that the extreme studentized deviate test is an efficient scheme in combating Byzantine attacks in cognitive radio networks. The simulation results shown that ESCCSS achieved a lower FAP compared to APCSS. ESCCSS also achieved a lower MD probability compared to APCSS. The proposed scheme therefore detects successfully malicious data and it also outperforms the APCSS scheme.

References

Abognah, A., & Basir, O. (2015). TV white space availability in Libya. In *CROWNCOM 2015: 10th International Conference, Doha, Qatar* (pp. 593–603). https://doi.org/10.1007/978-3-319-24540-9_49

Kempe, D., Alin, D., & Johannes, G. (2003). Gossip-based computation of aggregate information. In *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science* (pp. 1–12). https://doi.org/10.1109/SFCS.2003.1238221

Lavanis, N., & Jalihal, D. (2017). Performance of p-Norm detector in cognitive radio networks with cooperative spectrum sensing in presence of malicious users. *Wireless Communications and Mobile Computing*, *2*, 1–8. https://doi.org/10.1155/2017/4316029

Lin, H., Hu, J., Huang, C., Xu, L., & Wu, B. (2015). Secure cooperative spectrum snesing and allocation in distributed cognitive radio networks. *International Journal of Distributed Sensor Networks*, *11*(10), 1–12. https://doi.org/10.1155/2015/674591

Liu, Q., Gao, J., Guo, Y., & Liu, S. (2010). Attack-proof cooperative spectrum sensing based on consensus algorithm in cognitive radio networks. *KSII Transactions on Internet and Information Systems (TIIS)*, *4*(6), 1042–1062. https://doi.org/10.3837/tiis.2010.12.004

Lu, J., Wei, P., & Chen, Z. (2014). A scheme to counter SSDF attacks based on hard decision in cognitive radio networks. *WSEAS Transactions on Communication*, *13*, 242–248.

Luo, L., & Roy, S. (2007). Analysis of search schemes in cognitive radio. In *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*. https://doi.org/10.1109/SAHCN.2007.4292877

Mapunya, S., & Velempini, M. (2018a). Investigating spectrum sensing security threats in cognitive radio netowrks. In Y. Zhou & T. Kunz (Eds.), *Ad Hoc Networks* (pp. 60–68). https://doi.org/10.1007/978-3-319-74439-1_6

Mapunya, S., & Velempini, M. (2018b). The design of byzantine attack mitigation scheme in cognitive radio ad-hoc networks. In *Proceedings of the 2018 International Conference on Intelligent and Innovative Computing Applications*. https://doi.org/10.1109/ICONIC.2018.8601087

Mehdaw, M., Riley, N., Paulson, K., Fanan, A., & Ammar, M. (2013). Spectrum occupancy survey in HULL-UK for cognitive radio applications: Measurement and analysis. *International Journal of Scientific and Technology Research*, *2*(4), 231–236.

Mirsky, Y., Kalbo, N., Elovici, Y., & Shabtai, A. (2019). Vesper: Using echo-analysis to detect man-in-the-middle attacks on LANs. *IEEE Transactions on Information Forensics and Security*, *14*(6), 1638–1653. https://doi.org/10.1109/TIFS.2018.2883177

Mitola, J., & Maguire, G. (1999). Cognitive radio: Making software radios more personal. *IEEE Personal Communications*, *6*(4), 13–18. https://doi.org/10.1109/98.788210

Premarathne, U., Khalil, I., & Atiquzzaman, M. (2016). Trust based reliable transmissions strategies for smart home energy consumption management in cognitive radio-based smart grid. *Ad Hoc Networks*, *41*, 15–29. https://doi.org/10.1016/j.adhoc.2015.12.004

Seif, M., ElBatt, T., & Karim, S. (2016). Sparse spectrum snesing in infrastructure-less cognitive radio networks via binary consensus algorithm. In *Proceedings of 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. https://doi.org/10.1109/PIMRC.2016.7794919

Singh, V., Upadhyay, P., Lee, K.-J., & Costa, D. (2019). Cooperative and congitive hybrid satellite-terrestrial networks. In M. Rehmani & R. Dhaou (Eds.), *Cognitive Radio, Mobile Communications and Wireless Networks* (pp. 115–142). http://dx.doi.org/10.1007/978-3-319-91002-4_5

Sodagari, S., Attar, A., Leung, V., & Bilén, S. (2012). Combating channel eviction triggering denial-of-service attacks in cognitive radio networks. *Transactions on Emerging Telecommunications Technologies*, *23*(5), 454–465. https://doi.org/10.1002/ett.2502

Srinu, S., & Mishra, A. (2016). Efficient elimination of erroneous nodes in cooperative sensing for cognitive radio networks. *Computers and Electrical Engineering*, *52*, 284–292. https://doi.org/10.1016/j.compeleceng.2015.05.004

Vosoughi, A., Cavallaro, J., & Marshall, A. (2014). A cooperative spectrum sensing scheme for cognitive radio ad hoc networks based on gossip and trust. In *Proceedings of 2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*. https://doi.org/10.1109/GlobalSIP.2014.7032307

Wan, R., Ding, L., Xiong, N., & Zhou, X. (2019). Mitigation strategy against spectrum-sensing data falsification attack in cognitive radio sensor networks. *International Journal of Distributed Sensor Networks*, *15*(9), 1–12. https://doi.org/10.1177/1550147719870645

Yawada, P., & Dong, T. (2019). Intelligent process of spectrum handoff/mobility in cognitive radio networks. *Journal of Electrical and Computer Engineering*. https://doi.org/10.1155/2019/7692630

Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances and future trends. *Proceedings of the IEEE*, *104*(9), 1727–1765. https://doi.org/10.1109/JPROC.2016.2558521