NIJEC

NUML International Journal of Engineering and Computing

Volume: 2 Issue: 2

https://numl.edu.pk/journals/nijec
Print ISSN: 2788-9629
E-ISSN: 2791-3465
DOI:https://doi.org/10.52015/nijec.v2i2.57

Detection of Emulation Attacks in Cognitive Radio Networks using Heuristic Techniques

Jabbar Mahmood[a,*], Rahim Ali Qamar [a] and Shahzad Latif [b]

[a] *School of Engineering and Applied Sciences (SEAS), Isra University Islamabad (jabbarmahmood@hotmail.com)*
[b] *Department of Computer Science, Szabist, Islamabad (shahzadlatif97@gmail.com)*

Submitted	Revised	Published
24-Jan-2024	17-Feb-2024	21-Feb-2024

Abstract

This paper discusses the issue of primary user emulation attacks (PUEAs) in cognitive radio networks (CRNs). These attackers imitate the signal characteristics of primary users (PUs), preventing secondary users (SUs) from accessing their assigned spectrum. The research focuses on detecting PUEAs using the time difference of arrivals (TDOA) to detect the attacker and reduce detection errors using heuristic techniques. Differential evolution (DE) and cuckoo search (CS) algorithms are utilized to optimize detection accuracy. Through the enhancement of user diversity, the CS algorithm exhibits a notable improvement of 35%, while the DE algorithm demonstrates a more substantial enhancement, reaching a 47% improvement in comparison to the reference algorithm. Furthermore, augmenting the iteration count yields a heightened probability of accurate detection, with CS achieving a 94% correctness rate and DE attaining an impressive 98% accuracy at 200 iterations. Simulation results confirm that the proposed CS algorithm outperforms and gives better performance as compared to the DE algorithm.

Keywords: Cognitive Radio Networks, Primary User Emulation Attacker, Time Difference of Arrivals, Heuristic Techniques.

1. Introduction

The rapid and widespread expansion of wireless technology has led to a severe overcrowding of the existing spectrum, creating a scarcity of space for new wireless services. The CR has emerged as a revolutionary technology that confidently solves spectrum shortage issues and significantly improves channel use efficiency. This is achieved by sharing the spectrum between the PUs and SUs in a highly efficient manner, making it a game-changing technology in the field of wireless communication [1]. The CR has effectively solved the issue of spectrum scarcity in the wireless industry by enabling SUs to access the unused band of PUs [2].

Spectrum sensing is the primary operation of the CR, where a SU searches for available spectrum [3]. However, during this process, a malicious user may try to disrupt the sensing or communication processes of the CRN. It is imperative that SUs possess the capability to differentiate the genuine signal from other signals to prevent discrepancies. As soon as an SU detects the presence of a PU while monitoring the spectrum, it is mandatory that it promptly vacate that spectrum and switch to another available one.

Securing the SU from unauthorized users through spectrum detection is one of the most crucial challenges in CRNs. While wireless transmission lacks security, CRNs are susceptible to various attacks that can disrupt their operation. These attacks include spectrum data forgery, incorrect feedback, and impersonation attacks. The attacker's ultimate goal is to disrupt the communication of the SUs by impersonating the PU.

The localization techniques are crucial for estimating the position of PUEA, which helps mitigate the attacker from the network. The literature mainly utilizes three localization techniques: received signal strength indicator (RSSI), angle of arrival (AoA), and time difference of arrival (TDoA) [4]. The user's location can be estimated using the RSSI technique, which relies on the received signal strength and a well-established propagation loss model. In AoA, it estimates the reception angle of the signal and uses basic mathematical manipulations to determine the positions of the nodes. Finally, TDoA calculates the distance between two points using propagation time and signal propagation frequency.

A. Motivation

The demand for wireless devices is increasing, but the spectrum is fixed and cannot be extended. The CR effectively addresses the issue of spectrum shortage by granting users the freedom to utilize unassigned spectrum or share it to authorized users within the prescribed interference threshold. Although the CR has advantages, it also poses security risks. Attackers can mimic the properties of the PU and use the specific spectrum band or disrupt the communication of the CRN. In order to ensure smooth communication in the CRN, it is crucial to detect the PUEA successfully and block it from the network.

B. Contributions of the article

This research focuses on the detection of the PUEA by using heuristic techniques. The contributions of the articles are as follows:

- The CRN systematically formulates the issue of PUEA, wherein SUs are stochastically positioned alongside the PUEA.
- The CR-BS disseminates the authentic PU location information to SUs. The Time Difference of Arrival (TDoA) method is employed to deduce the assailant's position, subsequently contrasting it with the genuine location of the Primary User.
- The proposed work offers a comprehensive comparative analysis of two heuristic algorithms, namely Differential Evolution (DE) and Cuckoo Search (CS), aimed at optimizing the TDoA.

C. Organization of the article

The article is structured in the following way: Section 2 discusses the literature review and existing research on the detection of PUEA in CRNs. The limitations of the existing literature and research gaps are also examined. Section 3 presents the problem formulation, where we formulate the PUEA problem for the CRN and propose a model. Section 4 includes simulation results that validate the performance of the proposed model. Finally, the proposed work in Section 5 is concluded, and future scopes are presented.

2. Related work

The SUs typically use energy detection techniques in spectrum sensing, which effectively thwarts the efforts of PUEA to mimic primary signal power levels. While a power-fixed attacker maintains a constant power level irrespective of the actual transmitting power or radio conditions, a power-adaptable PUEA attacker is more sophisticated and able to adjust its communication power to match the real primary user's power traits with greater accuracy [5].

In cases where PUE attacks target the CR network, the problem of dropped connections can become more severe, leading to the possible disruption of service for users. A new method called multi-level hypothesis testing (MLHT) has been developed to identify banned users on a network [6]. The decision space is partitioned into four alternatives, and the channel quality is specified using the minimal Bayes cost criterion. The MLHT approach also takes into account the practical constraints that must be considered when using this technique.

Authors in [7] present a robust model that utilizes a hash message authentication code (HMAC) to effectively detect PUEA in CRN. The proposed model establishes reliance in the PU transmission by employing HMAC. To ensure the PU signal is accurately identified and safeguarded against potential attackers, a secret key between the SU and the PU is utilized. The proposed approach has been thoroughly analyzed through both theoretical analysis and simulation, confirming its high effectiveness in detecting PUEA in CRN.

The work in [8] proposes a solution to a problem using a localization defense model based on time-difference-of-arrival measurements and a firefly optimization algorithm. The CR users work together to detect and locate the attacker, and the firefly optimization algorithm minimizes the nonlinear least squares cost function.

In [9], authors presented a method for defending against attack in CRN using a TDOA technique with PSO. The proposed approach localizes the attacker and identifies the emulated user by comparing its position with that of the PU. The proposed method utilizes a PSO algorithm with optimized inertia weight and acceleration constants, delivering unparalleled accuracy in pinpointing the attacker's location. This technique is compared with standard PSO and Taylor series estimation to demonstrate its superior performance.

The work in [10] proposed a technique that combines cross-layer learning of SUs with higher-layer authentication to identify PUEAs and PUs in mobile CRNs accurately. It establishes RF databases that classify different transmitters as either PUs or PUEAs at the Physical layer, providing higher accuracy and differentiation. This method has been confirmed effective in simulations, ensuring the safety and reliability of mobile CR networks.

In [11], the authors proposed an effective machine-learning framework for detecting attacks in CRN. They employed the Pattern Described Link-Signature method (PDLS) to differentiate between PU and attacker using various classification models. The PDLS defines a pattern that describes the structure of 52 sub-CIR in OFDM-based transceivers. To evaluate their approach, the authors tested it using a software-defined radio testbed based on the IEEE 802.11a/g/p transceiver, which comprises the physical layer. The experimental results conclusively demonstrate the framework's high effectiveness in distinguishing between legitimate and malicious users.

The authors in [12] discovered regarding the compressed signal's sparsely coded dictionary, which is dependent on the channel. This dictionary's convergence patterns are confidently utilized to differentiate between a spectrum hole, a legitimate primary user, and an emulator or jammer. The decision-making process is carried out with utmost conviction through a classification operation based on machine learning.

3. System Model

The system model being proposed involves a CRN situated at the center of a deployment area (0,0). There will be a number of randomly placed secondary users (N) within the network, and it is assumed that these users are stationary. Additionally, there will be two PUs that are TV receivers connected to a PU-BS. The network architecture is illustrated in Figure 1. The simulation area of the CRN will cover 30 km², and the PU-BS will be positioned 30 km to 150 km from the CR-BS.

In a CRN, the CR-BS possesses the precise coordinates of the SUs and PUs. A PUEA is randomly deployed in the network, and it endeavors to capitalize on the available spectrum holes by imitating a PU. If an SU detects the presence of a PU while sensing the spectrum holes, it needs to authenticate if it is a licensed PU or a malicious user. The position of an attacker is anonymous and is appraised through a collaborative localization algorithm. This problem can be deemed a localization problem, where the attacker is located using a TDOA technique. The presented TDOA-based localization algorithm is examined in the next section.

The CR-BS is positioned at the center (χ_o, Υ_o), while a PUEA is randomly set at $(\chi,\ \Upsilon)$. The SUs are dispersed at $((\chi_k, \Upsilon_k)$. The distance across a PUEA and an SU_k is denoted by Γ_k, whereas the span between the CR-BS and the PUEA is described by Γ_o. The $\Gamma_{k,o}$ indicates the basic difference in the distance across a PUEA and the SU_k with CR-BS as a reference. The calculated distance through a TDOA is represented by $\Gamma_{k,o}$. It is considered that AWGN N_k is counted to the measurements with zero mean and σ_k^2variance.

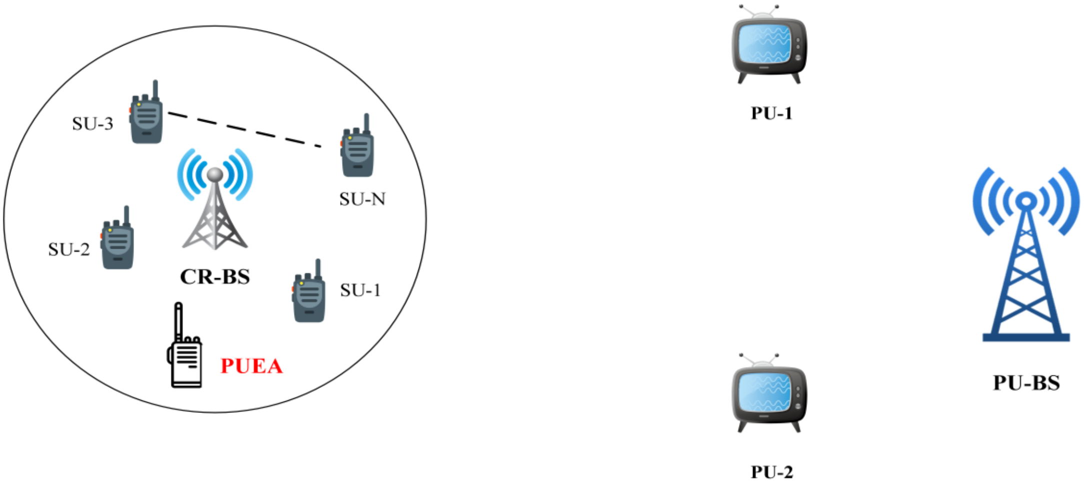

Figure 1. Network model of the proposed problem [9].

The expression for the TDOA can be found in [9], and it is presented in Eq.1 in mathematical form.

$$\Delta_k = \mathrm{T}_k - \mathrm{T}_0 \qquad (\text{Eq. } 1)$$

Where the time of arrival of the SU_k signal is T_k and T_o is arrival time of the signal at CR-BS is to, Eq. 1 is extended to Eq. 2.

$$\begin{aligned} \Gamma_{k,o} &= c \times \Delta_k \qquad (\text{Eq. } 2) \\ &= \Gamma_k - \Gamma_o \end{aligned}$$

Where c is indicated as the speed of light, and Δ_k is the TDOA. The distance without noise is presented in Eq.3.

$$\Gamma_{k,o} = \sqrt{(\chi - \chi_k)^2 + (\Upsilon - \Upsilon_k)^2} - \sqrt{(\chi - \chi_o)^2 + (\Upsilon - \Upsilon_o)^2} \qquad (\text{Eq. } 3)$$

The addition of AWGN noise has a significant impact on the measurements received at the receivers which is given in Eq. 4, thereby affecting the accuracy of the received data. It is important to be aware that the actual measurements are not immune to the effects of the added noise.

$$\widehat{\Gamma_{k,o}} = \Gamma_{k,o} + \mathrm{N}_k \qquad (\text{Eq. } 4)$$

The Eq. 5 denotes the TDOA computation carried out at the receiver. The error can be determined by contrasting the real and measured distance. Subsequently, a cost function can be formulated, and the primary goal is to minimize this cost function i.e. mean square error (MSE).

$$\mathcal{F}(\tilde{\chi}, \tilde{\Upsilon}) = \min \sum_{\mathrm{k}=1}^{M} (\widehat{\Gamma_{k,o}} - \sqrt{(\tilde{\chi} - \chi_k)^2 + \left(\tilde{\Upsilon} - \tilde{\Upsilon}_k\right)^2} + \sqrt{(\tilde{\chi} - \chi_o)^2 + \left(\tilde{\Upsilon} - \tilde{\Upsilon}_o\right)^2})^2 \qquad (\text{Eq. } 5)$$

Where $(\tilde{\varkappa}, \tilde{\gamma})$ estimated for a PUEA are the ones that effectively minimize the error.

In the previous section, the localization problem is formalized and stated as a cost function in Eq. 5. This problem is strictly NP-hard and demands an optimization algorithm for resolution. To tackle this issue effectively, we will employ optimization algorithms based on heuristics that work towards minimizing the margin of error. Once the PUEA is detected, the CR-BS will immediately and confidently broadcast its information to all the SUs.

The CS algorithm is an incredibly efficient optimization algorithm for quick converging problems that is inspired by the aggressive breeding behavior of cuckoos. It was first introduced to solve numerical function optimization problems and has since been widely used for complex optimization problems. In CS, an egg represents a candidate solution where its position denotes a set of coordinates.

A detailed explanation of the CS algorithm can be found in [13]. The DE is a nature-inspired stochastic optimization algorithm that is used for solving nonlinear optimization problems, and the further details can be found in [14].

Figure 2 presents the flowchart for the optimized TDOA algorithm proposed to detect PUEA effectively.

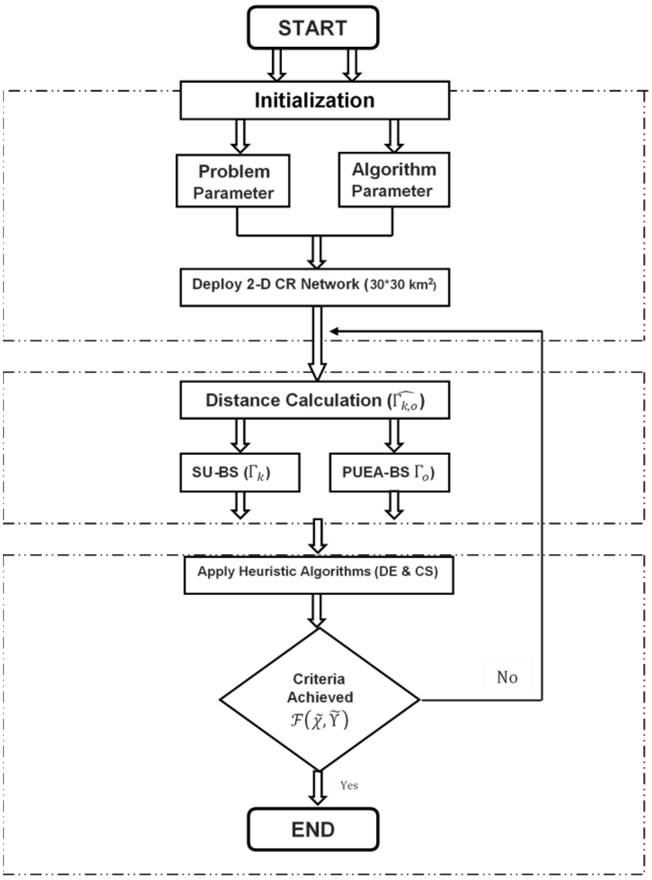
START
Initialization
Problem Parameter
Algorithm Parameter
Deploy 2-D CR Network (30*30 km²)
Distance Calculation ($\widehat{\Gamma_{k,o}}$)
SU-BS (Γ_k)
PUEA-BS Γ_o)
Apply Heuristic Algorithms (DE & CS)
Criteria Achieved $\mathcal{F}(\tilde{\chi},\tilde{\Upsilon})$
No
Yes
END

Figure 2. Proposed solution for PUEA detection

Table 1. Simulation parameters for the proposed PUEA detection algorithm

Parameters	**Values**
Number of SUs	70
Number of Malicious users	1
Simulation area	30*30 km^2
Height of PUEA Antennae	1.5m
Candidate Solutions	50
SNR	[-10dB - 10dB]
Epochs	200
Noise	AWGN
BS coordinates	(0,0)
SU coordinates	Random
PUEA coordinates	
Crossover Rate	0.3
Discovery Probability	0.3
σ	0.8
β	4

4. Simulation Results

In this section, we will delve into the effectiveness of the proposed system and present a thorough comparison of the heuristic algorithms. To simulate the proposed PUEA attack detection algorithm, we have used Matlab and the simulation parameters have been outlined in Table 1.

In the simulation, a CRN is strategically placed over a vast area of 30x30 square kilometers, with a CR-BS situated at the center. Numerous SUs are randomly deployed across the region to perform seamless cooperative spectrum sensing, with data relayed to the BS. The CRN's deployment is aptly illustrated in Figure 3. A PUEA, cunningly positioned within the CRN, relentlessly disrupts the network's sensing process. However, the PUEA is swiftly and accurately located using the optimization algorithms.

In this study, we thoroughly analyze the optimization of a single PUEA that is randomly placed in the CRN, as shown in Figure 4. Our highly efficient algorithm is capable of localizing the PUEA with utmost precision and broadcasts the attacker's coordinates to the entire network. Furthermore, we have conducted a meticulous comparison of our proposed system's mean square error (MSE) with the existing technique in three distinct cases to evaluate its performance.

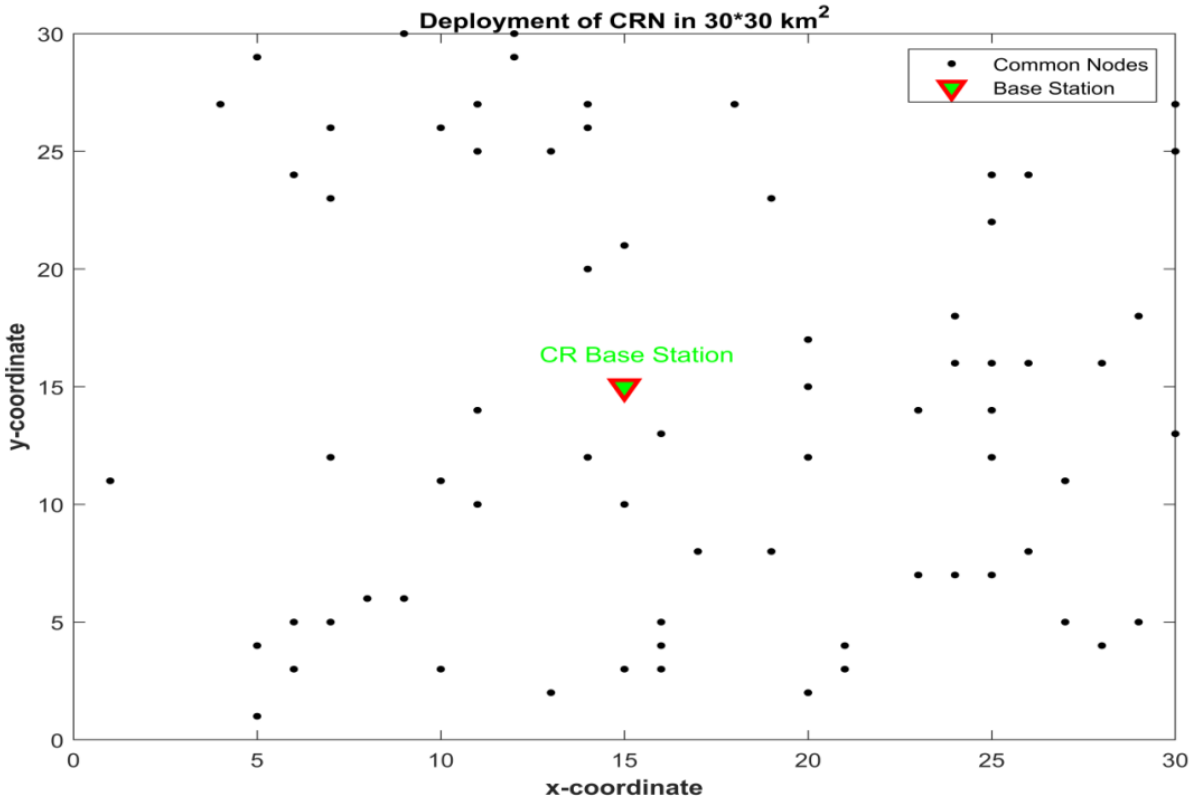

Figure 3. CRN deployment in 30x30 km^2.

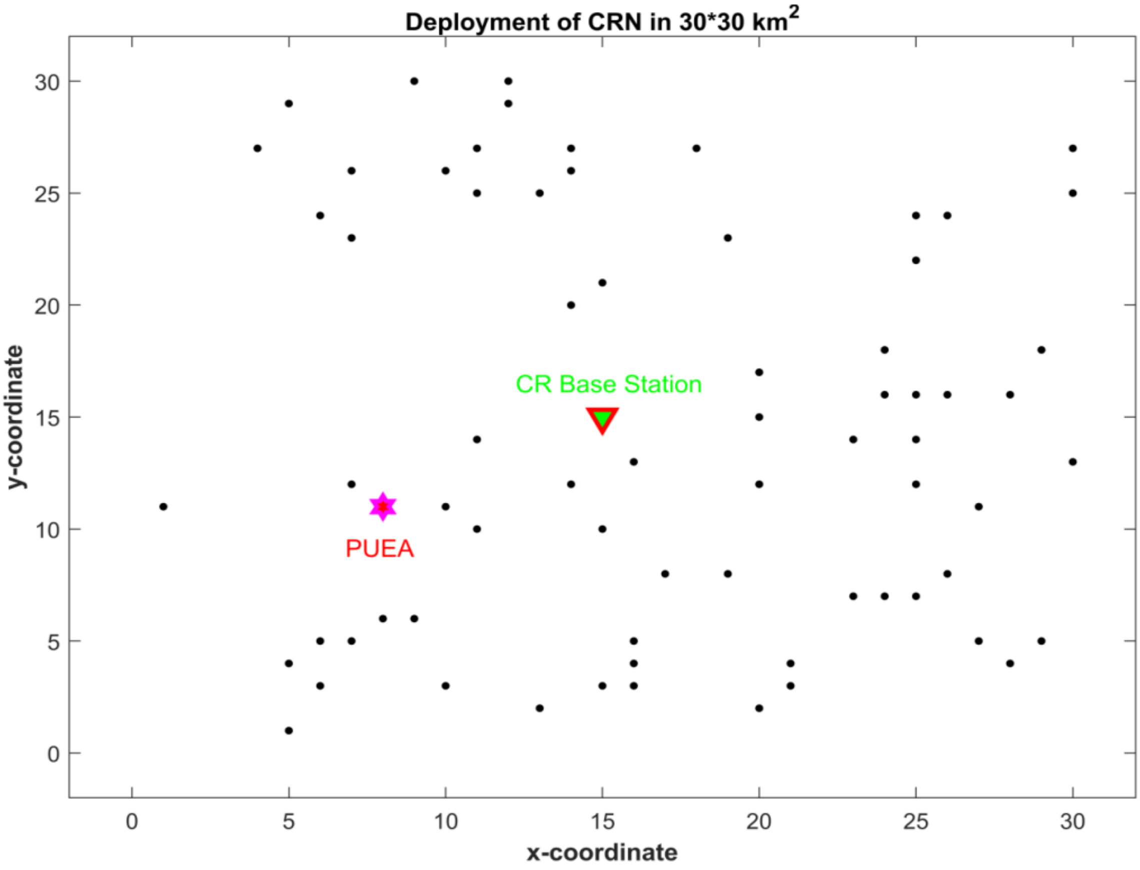

Figure 4. Randomly placement of PUEA.

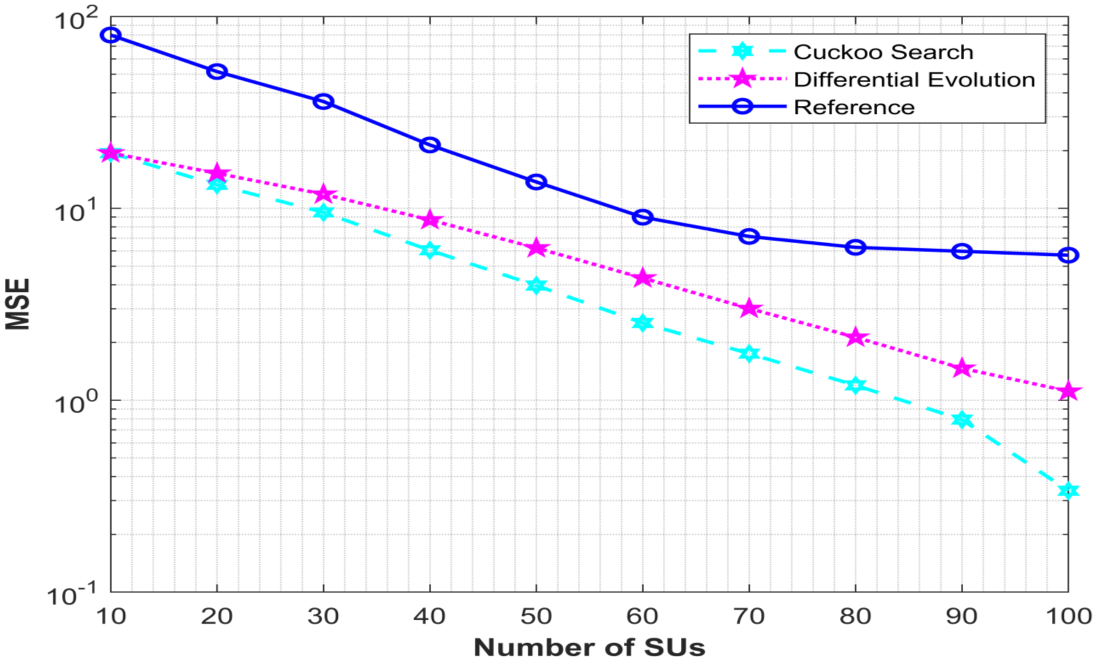

Figure 5. Comparative analysis of heuristic algorithm with increasing SUs.

A. Effects of increasing SUs

The optimization algorithms proposed, namely DE and CS, have been effectively utilized to optimize the Mean Squared Error (MSE). The performance evaluation of the proposed techniques is presented in Figure 5, which depicts the MSE performance evaluated by varying the number of SUs while keeping the iterations and SNR constant. The simulation results strongly indicate that the proposed CS algorithm outperforms the Firefly algorithm (reference) as well as the DE algorithm. Additionally, the performance of the localization error is observed to improve significantly with increasing the number of SUs. A comparative analysis of the proposed techniques is presented, where the proposed algorithm is compared with the Firefly-based optimization algorithm. For N=90 number of SUs, the CS algorithm gives an MSE of less than 100, and it decreases dramatically as the number of SUs increases.

B. Effects of increasing iterations

After a thorough evaluation of the proposed technique, which involved varying the number of iterations while keeping the SNR and SUs constant, it has been established that increasing the number of iterations results in a substantial decrease in MSE. The simulations in Figure 6 indicate that the DE algorithm significantly outperforms the CS and firefly methods when the number of iterations varies. Although the CS may perform better than DE for fewer iterations, DE provides the minimum error at higher iterations, particularly at 200 iterations. Based on these results, it can be confidently concluded that the number of iterations plays a crucial role in the performance of the technique. Although increasing the iterations results in a reduction of the localization error, it comes at the expense of increased computational complexity.

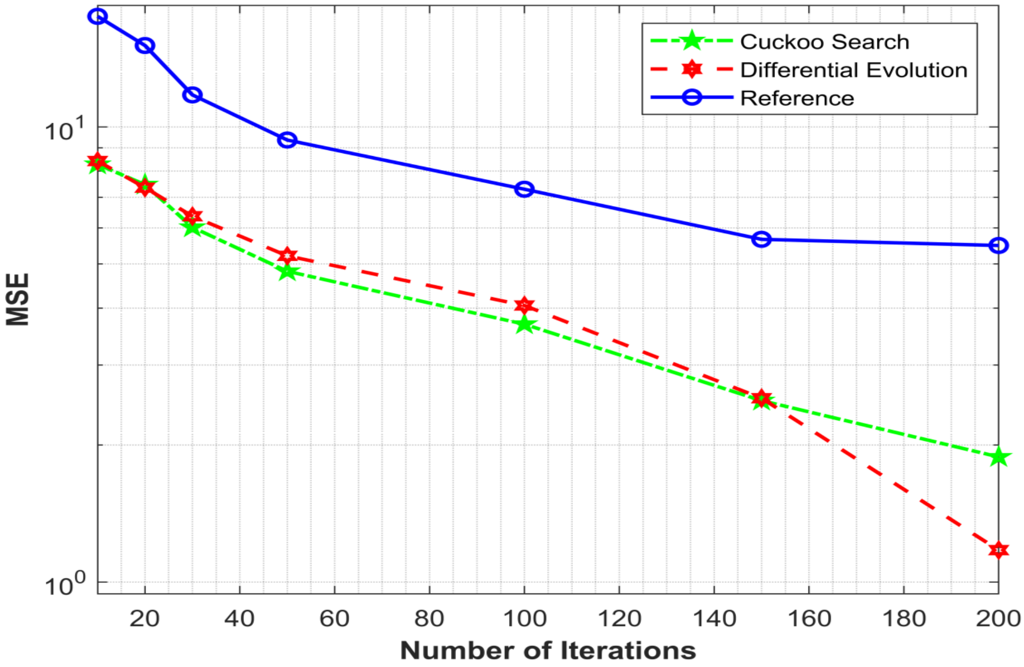

Figure 6. Comparative analysis of heuristic algorithm with increasing SUs.

C. Effects of increasing received signal strength

A higher SNR undoubtedly leads to superior performance and lower localization errors. Our proposed scheme has undergone meticulous analysis for various SNRs. The findings of our comparative analysis of DE and CS against the Firefly algorithm in Figure 7 leave no doubt about the superiority of our approach. Although there is not much difference in the MSE values at lower SNRs, at 10 dB of SNR, a significant improvement is observed in the results, and DE outperforms with better MSE. Meanwhile, CS is on par with the Firefly method. It is worth noting that the number of iterations and the number of SUs are kept constant in this case, which further highlights the robustness of our approach.

Figure 7 unequivocally shows that the MSE of the CS, DE, and firefly algorithms decreases as the SNR increases from -10dB to 10dB. However, the DE algorithm stands out as the most efficient algorithm in optimizing the MSE. It's important to note that the proposed algorithm outperforms the reference algorithms (Firefly and CSA) with fixed SUs by a significant margin. Therefore, the conclusion is indisputable: the proposed algorithm outperforms the reference algorithms without any ambiguity.

D. Probability of Correct Detection

The metric of probability of correct detection is crucial in accurately identifying malicious users. As per the findings of Figure 8, the detection accuracy increases with the number of iterations performed. At 200 iterations, CS provides a detection accuracy of 94%, while DE provides a detection accuracy of 98%. Additionally, Figure 9 presents the probability of false detection.

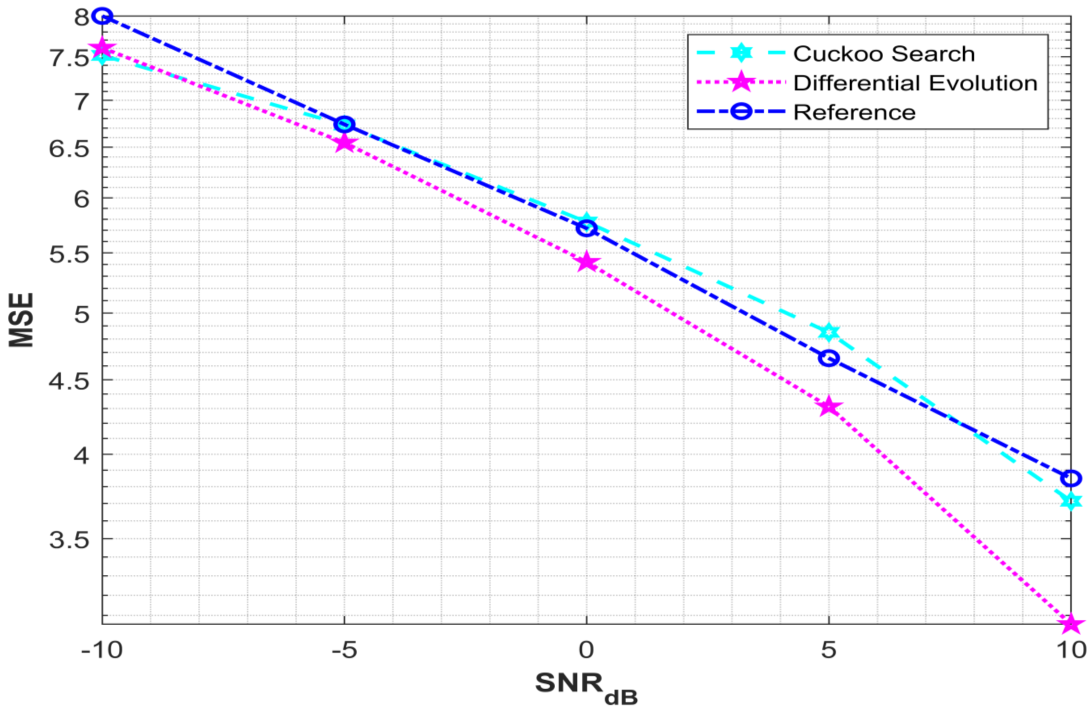

Figure 7. Performance comparison with increasing SNRs.

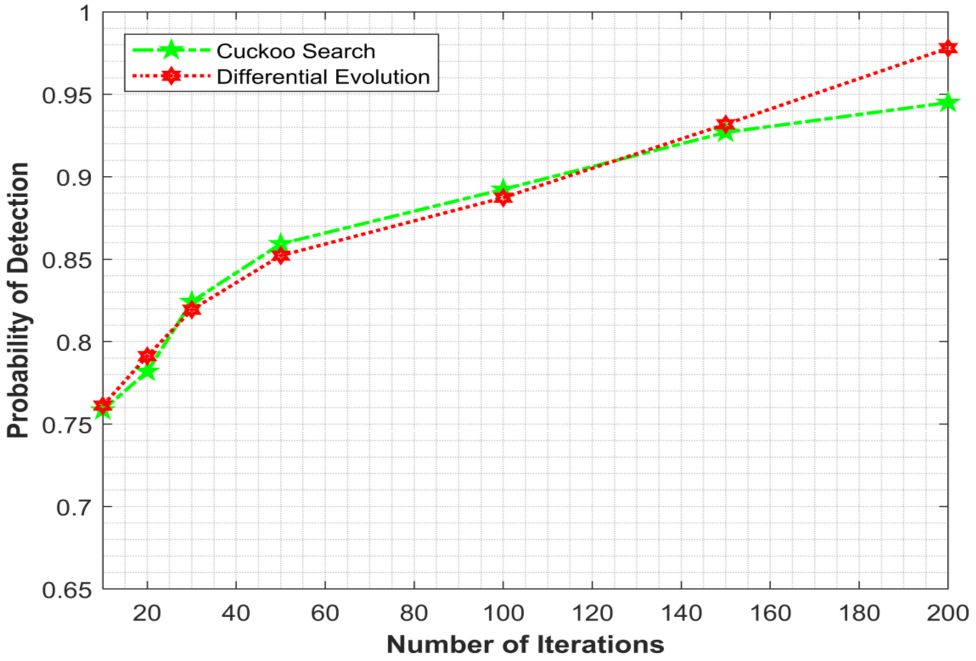

Figure 8. Probability of correct detection vs number of iterations.

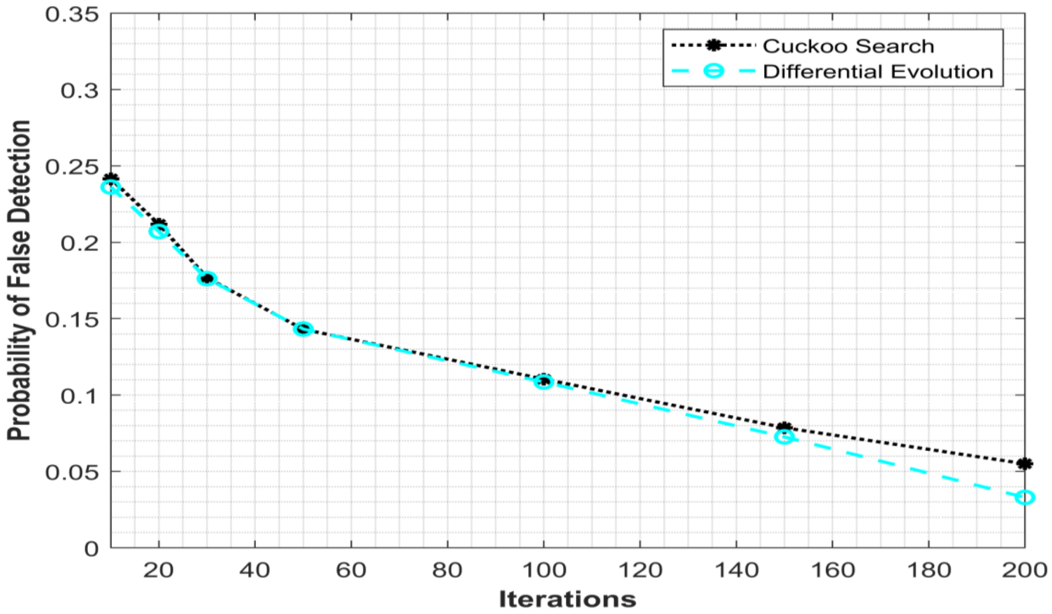

Figure 9. Probability of false detection vs number of iterations.

5. Conclusion

This research focuses on detecting a severe attack known as PUEA in CRNs, which poses a significant security threat to spectrum sensing. By falsely identifying itself as a PU, the attacker can compromise CRN communication. It is of utmost importance to accurately detect attackers and ensure uninterrupted communication. With the use of heuristic-based optimization algorithms, the study showcases exceptional performance in diverse scenarios, where SUs, iterations, and SNR are varied. It has been concluded that the CS algorithm performs exceptionally well in the first case, where MSE is compared to the number of SUs. When there are a higher number of SUs, the CS algorithm produces less than MSE of 100, whereas DE produces approximately MSE of 100. Both algorithms perform better than the Firefly algorithm. In the second case, where MSE is compared to the number of iterations, DE outperforms the other algorithms and produces roughly an MSE of 100. Finally, DE shows better performance than the CS and Firefly algorithms in the third case, where MSE is compared to the SNR. The third case shows a remarkable 25% improvement with DE in comparison to the Firefly method. The increasing demand for CR in smart grids is a potential target for attackers that can seriously compromise the communication process. Acknowledging the problem and defining it based on the constraints of CR-based communication networks in smart grids is an imperative step toward finding a solution This research proposed a model using heuristic-based optimization which is a sub-optimal solution. To address this issue, the model can be extended to a convex optimization problem, ensuring globally optimal results with lower computational complexity. This adaptation considers the constraints CR-based smart grid communication networks, enhancing security in response to the increasing demand for CR in smart grids. .

References

[1] S. Alam, M. Sarfraz, M. B. Usman, M. A. Ahmad, and S. Iftikhar, "Dynamic resource allocation for cognitive radio based smart grid communication networks," *Int. J. Adv. Appl. Sci*, vol. 4, no. 10, pp. 76–83, 2017.

[2] S. Alam, A. N. Malik, I. M. Qureshi, S. A. Ghauri, and M. Sarfraz, "Clustering-based channel allocation scheme for neighborhood area network in a cognitive radio based smart grid communication," *IEEE Access*, vol. 6, pp. 25773–25784, 2018.

[3] M. Ranjbar, N. Tran, T. Karacolak, and K. D. Pham, "On the Energy Efficiency and Spectral Efficiency Trade-Off of Multi-User Full-Duplex Cognitive Radio Networks under Imperfect Spectrum Sensing," in *AIAA SCITECH 2024 Forum*, 2024, p. 1736.

[4] P. Chithaluru, F. Al-Turjman, T. Stephan, M. Kumar, and S. Kumar, "An Optimized Bio-inspired Localization Routing Technique for Sustainable IIoT Networks & Green Cities," *Sustain Cities Soc*, vol. 97, p. 104722, 2023.

[5] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on selected areas in communications*, vol. 26, no. 1, pp. 25–37, 2008.

[6] M. Sharifi, A. A. Sharifi, and M. J. M. Niya, "Cooperative spectrum sensing in the presence of primary user emulation attack in cognitive radio network: multi-level hypotheses test approach," *Wireless Networks*, vol. 24, pp. 61–68, 2018.

[7] W. R. Ghanem, M. Shokair, and M. I. Desouky, “Defense against selfish PUEA in cognitive radio networks based on hash message authentication code,” *International Journal of Electronics and Information Engineering*, vol. 4, no. 1, pp. 12–21, 2016.

[8] W. R. Ghanem, M. Shokair, and M. I. Desouky, “An improved primary user emulation attack detection in cognitive radio networks based on firefly optimization algorithm,” in *2016 33rd National Radio Science Conference (NRSC)*, IEEE, 2016, pp. 178–187.

[9] W. R. Ghanem, R. E. Mohamed, M. Shokair, and M. I. Dessouky, “Particle swarm optimization approaches for primary user emulation attack detection and localization in cognitive radio networks,” *arXiv preprint arXiv:1902.01944*, 2019.

[10] T. N. Le, W.-L. Chin, and W.-C. Kao, “Cross-layer design for primary user emulation attacks detection in mobile cognitive radio networks,” *IEEE Communications Letters*, vol. 19, no. 5, pp. 799–802, 2015.

[11] A. Albehadili, A. Ali, F. Jahan, A. Y. Javaid, J. Oluochy, and V. Devabhaktuniz, “Machine learning-based primary user emulation attack detection in cognitive radio networks using pattern described link-signature (PDLS),” in *2019 wireless telecommunications symposium (WTS)*, IEEE, 2019, pp. 1–7.

[12] H. M. Furqan, M. A. Aygül, M. Nazzal, and H. Arslan, “Primary user emulation and jamming attack detection in cognitive radio via sparse coding,” *EURASIP J Wirel Commun Netw*, vol. 2020, no. 1, p. 141, 2020.

[13] S. Alam, N. Aqdas, I. M. Qureshi, S. A. Ghauri, and M. Sarfraz, “Joint power and channel allocation scheme for IEEE 802.11 af based smart grid communication network,” *Future Generation Computer Systems*, vol. 95, pp. 694–712, 2019.

[14] M. Sohail, S. Alam, A. Hussain, S. A. Ghauri, M. Sarfraz, and M. Ahmed, “Multiuser detection: Comparative analysis of heuristic approach,” *Int. J. Adv. Appl. Sci*, vol. 4, pp. 115–120, 2017.