applied sciences

MDPI

Article

Detection of Primary User Emulation Attack Using the Differential Evolution Algorithm in Cognitive Radio Networks

Rehna Batool [1], Nargis Bibi [1,*], Nazeer Muhammad [2] and Samah Alhazmi [3,*]

[1] Department of Computer Science, Fatima Jinnah Women University, The Mall, Rawalpindi 44000, Pakistan
[2] Department of Software Engineering and IT, Pak-Austria Fachhochschule Institute of Applied Sciences and Technology, Mang, Haripur 22621, Pakistan
[3] Computer Science Department, College of Computing and Informatics, Saudi Electronic University, Riyadh 11673, Saudi Arabia
* Correspondence: nargis@fjwu.edu.pk (N.B.); s.alhazmi@seu.edu.sa (S.A.)

Abstract: Cognitive Radio Network (CRN) is an emerging technology used to solve spectrum shortage problems in wireless communications. In CRN, unlicensed secondary users (SUs) and licensed primary users (PUs) use spectrum resources at the same time by avoiding any interference from SUs. However, the spectrum sensing process in CRN is often disturbed by a security issue known as the Primary User Emulation Attack (PUEA). PUEA is one of the main security issues that disrupt the whole activity of CRN. The attacker transmits false information to interrupt the spectrum sensing process of CRN, which leads to poor usage of the spectrum. The proposed study uses a proficient Time Difference of Arrival (TDOA) based localization method using the Differential Evolution (DE) algorithm to identify the PUEA in CRNs. The DE algorithm is used to solve the objective function of TDOA values. The proposed methodology constructs a CRN and identifies PUEA. The proposed method aims to sense and localize PUEA efficiently. Mean Square Error (MSE) is the performance evaluation parameter that is used to measure the accuracy of the proposed technique. The results are compared with the previously proposed Firefly optimization algorithm (FA). It is clear from the results that DE converges faster than FA.

Keywords: Primary User Emulation Attack (PUEA); Differential Evolution (DE); Time Difference of Arrival (TDOA); Cognitive Radio Networks (CRNs)

check for updates

Citation: Batool, R.; Bibi, N.; Muhammad, N.; Alhazmi, S. Detection of Primary User Emulation Attack Using the Differential Evolution Algorithm in Cognitive Radio Networks. *Appl. Sci.* **2023**, *13*, 571. https://doi.org/10.3390/app13010571

Academic Editors: Christos Bouras and Amalia Miliou

Received: 10 November 2022
Revised: 17 December 2022
Accepted: 27 December 2022
Published: 31 December 2022

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Cognitive Radio Network (CRN) is an emerging technology introduced by Mitiola in 2000, developed to utilize the radio spectrum in an opportunistic way. It has been examined in previous studies, showing that the licensed band is not used efficiently in both the spatial and temporal spheres [1,2]. Many wireless applications can use the unused radio frequencies in licensed bands. Thus, a viable solution, Cognitive Radio (CR), has been presented to use this opportunity [3].

The main aim of a CRN is to efficiently use the spectrum and allow strong communication any time. The problem of inadequate spectrum bands for wireless applications arises with the rapid increase in wireless networks over the internet; hence, the need for more frequency channels also increases. The spectrum scarcity issue is reduced due to the evolution of a CRN. This new technology embeds an efficient node in lightweight devices like PDAs to fulfill primary transmission requirements [4,5]. Wireless spectrum becomes a precious resource for advancements in information technology (IT), particularly, the Internet of Things (IoT). Most of the time, spectrum remnants are unused due to their fixed assignment and flexibility in their usage. Thus, the CRN has been perceived to be a key to achieving efficient utilization of the spectrum [6]. Apart from the advantage of providing maximum spectrum utilization, the CRN also attracts security threats as well. It provides random and open access to SUs to use free channels for their communication.

A lot of wireless devices that are not licensed use free bands when licensed users are not transmitting. In this way, the CRN becomes more vulnerable to attacks [4]. The CRN works proficiently if the model design for channel sensing is effective. The objective of designing an efficient model is to correctly allocate a free channel to secondary users (SUs). While transmitting, however, these models may be infected by incorrect and adulterated information [7]. This misinformation is the result of various attacks like data falsification or primary user (PU) emulation.

In previous studies, many different techniques against a PUEA have been proposed. A new concept of spectrum access function is proposed by [8]. In this proposed technique, spectrum access is defined by channel access function denoted by $\varphi(y)$ given in (1) that describes a novel communication law to access the PU band frequency using the energy detection method. The energy detection procedure is used to recognize the PUs in the CRN.

$$\varphi(y) \triangleq \Pr\{T|Y = y\} \quad (1)$$

A surveillance strategy based on game theory against a PUEA is proposed by [9]. To accurately detect the PUEA and to consider the effect of noise on the CRN, an improved RSS-based localization approach using maximum likelihood estimation (MLE) is proposed by [10]. Ref. [11] offered a Kalman filter-based detection technique for the cases where the PU is mobile. This technique was proposed because the result of the algorithms where the PU is fixed are not more efficient. The Kalman filter is used to find the position of the PU, and the power of the received signal along with the distance between the transmitter node and the PU is calculated to exactly detect the attacker. To avoid the training process and the previous information about the location of all types of nodes, Ref. [12] introduced a feasible RSS-based detection approach. It allows the node's mobility in the network. To find out the exact location of the PUEA in the CRN, Ref. [13] proposed an approach in which the position of an attacker is determined by using two occupants in the network. Ref. [14] studied the effect of malicious users in the CRN.

The Neyman–Pearson criterion is used for statistical analysis of the system model. An active smart attacker design in the spectrum sensing of the CRN is presented by [15]. Optimum joining techniques for PUEAs in the CRN is presented by [16]. These joining approaches are used to detect both selfish attackers and malicious attackers. The time difference of arrival (TDOA) method is used to detect the precise position of a PUEA, proposed by [17]. SUs in the CRN cooperate with each other based on TDOA values. Ref. [18] proposed the localization technique to detect the attacker in the CRN. The technique aims to detect the PUEA not only inside but also outside the network with high accuracy. Localization error is reduced by using particle swarm optimization (PSO), novel bat algorithm (NBA), and the modified particle swarm optimization (MPSO) based on the TDOA technique [19]. MPSO has higher performance than the other two. Ref. [20] uses a K nearest neighbor classifier (KNN) algorithm to identify PUEAs and grouped all malicious nodes together. Data encryption is used to maintain network security, but this technique has an overhead of training the classifier, which is time-consuming and costly.

Property identification-based detecting with dual threshold value has been proposed by [21] to avoid spectrum degradation. If the sensed signal has greater value than the upper threshold or lesser value than the lower threshold, then it is reflected as a PU signal, but if the signal value lies in between the two thresholds, then that signal is recognized as an attacker. To make detection of signals more accurate, a game model is used along with thresholds. In this approach, it is very critical to carefully choose the two thresholds in order to make the optimal decision. The Extreme Machine Learning (EML) algorithm and Time–Distance with Signal Strength Evaluation (TDSE) algorithm are used by [22] to detect and prevent PUEAs. TDSE is used to detect the malicious node in the CRN, whereas EML decides whether the detected node is an attacker or not. The detecting ability of the proposed algorithms is high, and it reduces the total delay in the network. This proposed approach, however, has a high complexity rate in mobile networks.

Our main contributions in this work are mentioned below:

- An efficient method is proposed to diminish the PUEA efficiently.
- A TDOA-based localization approach is used along with the DE algorithm.
- Intervention during the spectrum sensing process is reduced, which increases bandwidth usage.
- The fitness function is minimized to correctly estimate the attacker's position.
- Correct detection probability is increased.
- False detection probability is decreased.

The outline of the paper is given below. Section 2 provides materials and methods. Section 3 includes the results. Section 4 shows the discussion of the results. Section 5 concludes this research work.

2. Materials and Methods

2.1. Problem Formulation

The proposed approach in this paper comprises a CRN with a central point called Cognitive Radio Base Station (CRBS) and randomly deployed N SUs. Along with the CRN, there is a PU set-up that consists of a PU transmitter and many fixed receivers. In our model, the PU transmitter is called the source, and the receivers are TV sinks. The PU transmitter is the source that wants to send signals for communication with TV sinks. CRBS has all the information regarding the PU transmitter, as it is the licensed sender. The diagrammatical representation is shown in Figure 1. The positions of the PU transmitter and SUs are known to the CRBS. The distance of the PU transmitter ranges from 30 km to 100 km. The PU is placed at a certain position outside the CRN.

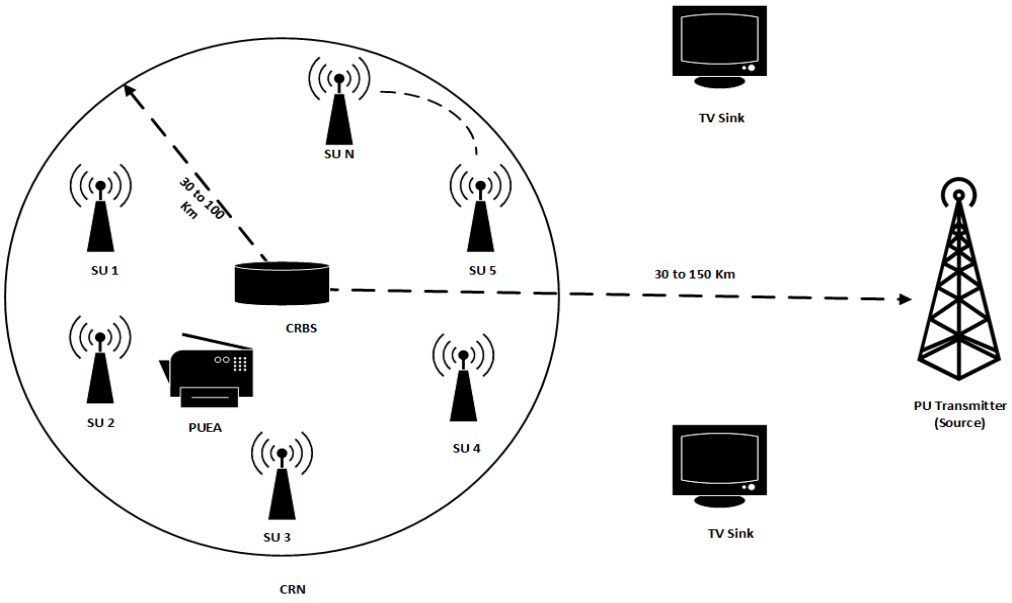


Figure 1. System design.

This work aims to detect the attacker (PUEA) in or out of the CRN by maximum precision to accurately recognize the invader when it is close to the PU by lessening the localization positioning inaccuracy while diminishing the quantity of required coordinating clients and the time to localize the attacker.

The following assumptions are made in the detection of a PUEA:

The CRN does not have any information regarding the malicious node or its scheme.
The PUEA is located near the PU or positioned within the CRN.
The PUEA radio conduct is similar to that of the PU.
The signal characteristics of the PUEA can be the same or different from that of the PU.

2.2. Mathematical Model for TDOA Localization Technique

A framework for TDOA localization is given below:

An anonymous source transmitted an altered signal.
The transmitted signal is captured by three or more receivers that are positioned around the source.
To calculate the exact position of the source, the time of each captured signal at each receiver is calculated.
The change in time of signal at each receiver is important, as it is used to calculate the distance variance between receivers.
The time difference is calculated by hyperbolic lines.
The connection points of hyperbolas show the target positioned by TDOA.

Due to an error in calculated TDOA values, the connection points of hyperbolas do not always point out the target. Optimization algorithms are therefore used along with TDOA to correctly locate the target.

The calculated model for the TDOA localization technique is described below:

(a, b) represents the exact position of the unknown sender. The sender can be an authorized user or attacker.
(a_0, b_0) represents the position of CRBS.
(a_i, b_i) represents the position of the ith SU.
r_i indicates the interspace of the unknown sender with the ith SU.
r_0 indicates the interspace of CRBS with the unknown sender.
$r_{i,0}$ represents the real distance difference of the PUEA with the ith SU, where CRBS is the static node.

Real distance difference measurements of the PUEA and the ith SU with the CRBS are given in (2).

$$\begin{aligned} r_{i,o} &= r_i - r_0 \\ &= \sqrt{(a-a_i)^2 + (b-b_i)^2} \\ &\quad -\sqrt{(a-a_0)^2 + (b-b_0)^2} \end{aligned} \tag{2}$$

where $r_i = \sqrt{(a-a_i)^2 + (b-b_i)^2}$ and $r_o = \sqrt{(a-a_0)^2 + (b-b_0)^2}$.

Here i ranges from 1, . . . , N. N is the total number of SUs.

Values obtained from the TDOA method contain Gaussian noise due to the surroundings. The variations in distance values with Gaussian noise are given in (3).

$$\widehat{r_{i,0}} = r_{i,o} + n_i \tag{3}$$

Here, $\widehat{r_{i,0}}$ is the measured range of different distances. n_i is Gaussian error with 0 mean and σ^2 variance. The fitness function for the localization problem is given in (4).

$$f(\widetilde{y}, \widetilde{z}) = \sum_{i=1}^{N} \left(\widehat{r_{i,0}} - \sqrt{(\widetilde{y} - y_i)^2 + (\widetilde{z} - z_i)^2} + \sqrt{(\widetilde{y} - y_0)^2 + (\widetilde{z} - z_0)^2} \right)^2 \tag{4}$$

Here, $(\widetilde{y}, \widetilde{z})$ represents the estimated location of the unknown sender, ${\sigma_i}^2$ represents the variance at the ith SU, and ${\sigma_0}^2$ represents the variance at the CRBS. Equation (5) is used to find the path loss value. The Hata model is used in this paper.

$$\Delta L_P(\mathrm{dB}) = [44.9 - 6.55 \cdot \mathrm{Log}(h)] \log \frac{r_i}{r_0} \tag{5}$$

Here, ΔL_P represents the Hata model and h represents the transmitter antenna height. The value of SNR_i is given in (6).

$$SNR_i = SNR_0 - \Delta L_P(\mathrm{dB}) \tag{6}$$

Here, SNR_i represents SNR at the ith SU, and SNR_0 represents the basic SNR at CRBS.

2.3. Firefly Optimization Algorithm

The firefly optimization algorithm (FA) was developed by Yang in 2007 and is a metaheuristic technique motivated by the flashing of fireflies. A flash of light is used to search food and is considered to be the fitness function during optimization of a problem. FA has the following three assumptions:

- Fireflies are unisex and attracted to each other irrespective of their sex.
- Attractiveness and brightness are inversely proportional. Less bright fireflies will be attracted to brighter fireflies.
- Fireflies with the same brightness move randomly.

Equation (7) is used to calculate the attractiveness of fireflies.

$$\beta = \beta_0 e^{-\gamma r^2} \tag{7}$$

Here β_0 represents initial attractiveness; r is the distance between fireflies; and γ is the absorption factor. The distance between two fireflies i and j is calculated by using Equation (8):

$$r_{ij} = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} \tag{8}$$

Movement process can be calculated using Equation (9) with β_0 attractiveness and distance r = 0. α represents the random variable, and vector ϵ_i^t contains a random value calculated from the Gaussian distribution.

$$x_i^{t+1} = x_i^t + \beta_0 e^{-\gamma r_{i,j}^2} \cdot \left(x_j^t - x_i^t\right) + \alpha \cdot \epsilon_i^t \tag{9}$$

2.4. Detection of PUEAs Using the DE Based Localization Algorithm

Figure 1 shows the proposed system design, which consists of a CRN with a PU transmitter and TV sinks, a CRBS, randomly deployed SUs, and a PUEA. The radius of CRN ranges from 30 km to 100 km. The main components of the system are PUs, SUs, and PUEAs. The PU is considered to be fixed and located outside the network at a distance of 30 km to 100 km. The PU is licensed and has a high priority for transmitting using the band. SUs are not licensed and use the PU only when it is free. The PUEA does not interfere with the PU, but it destroys the spectrum and damages the spectrum sensing process of the system; in this way, the spectrum remains unused by the SUs when there is no transmission from the PUs. The PUEA can capture the PU signal, imitate it, and recommunicate its very peculiar sign, having attributes similar to the PU sign, to cheat the SUs.

The PUEA can be positioned outside or inside the CR network. Based on predefined information stored in BS, the attacker can be identified. The attacker's position is measured and matched with the PU position stored in BS. If the location matches, then the sender is the PU, otherwise the PUEA. Here, TDOA finds the location by calculating the distance differences between the PU transmitter and the TV sinks. This distance difference is calculated from the time of arrival signal data using Equation (8).

The TDOA obtains this difference in arrival of the signals by using the cross-correlation technique at two or more nodes. To locate the transmitter, the TDOA uses two hyperbolic curves. These curves intersect at a point that is the location of the transmitter. This location is further compared with the PU location in terms of the PUEA. To refine this location identification process, the DE is used. The DE reduces the possible error in the location identification process by optimizing the search space iteratively, as shown in Figure 2. This helps to attain the high fitness value for the required optimization.

The main aim of the proposed algorithm is to detect the PUEA correctly and with maximum accuracy. Three main steps need to be followed for the proposed technique:

- Characteristics of the PU and the SU signals match with the received signals.

- By using the DE algorithm, the TDOA measurements for an appropriate distance need to be used.
- Measured location is compared with the PU transmitter's location to distinguish between the PU and the PUEA.

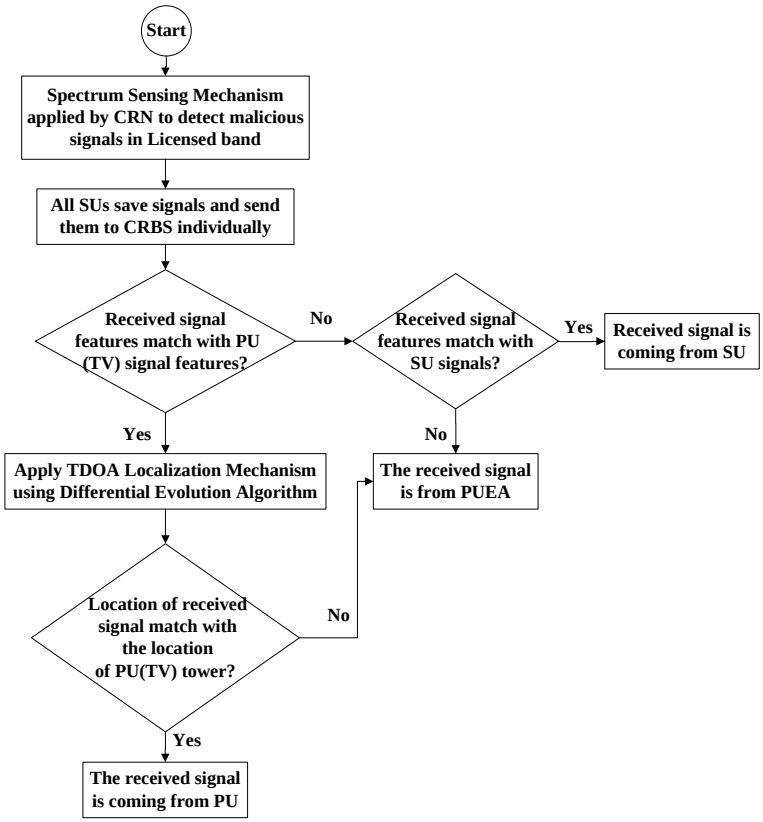


Figure 2. Workflow of TDOA based localization technique using Differential Evolution.

3. Results

In this section, the simulation results are compared with the Firefly optimization algorithm (FA). The MATLAB R2018a tool was used to build the simulations for the proposed algorithm used for detecting the PUEA in the CRN. In this work, a CRN is built and simulated in which 50 random SUs are deployed as shown in Figure 3. The simulation area is 30×30 km^2. The DE approach is used to reduce the fitness function value and to increase accuracy and performance. The proposed TDOA based localization technique using DE uses some parameters during simulation procedures. These parameters with their values are given in Table 1.

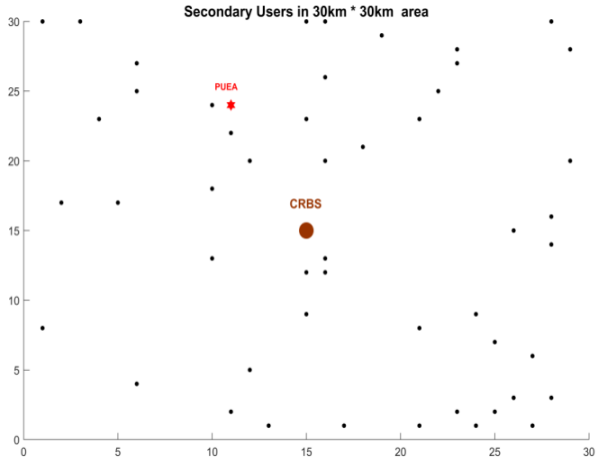


Figure 3. Deployment of SUs in a CRN with area of 30 km × 30 km.

Table 1. Simulation parameters and values.

Parameters	Values
Secondary Users (N)	50
Number of PUEA (n)p	1
Simulation Area	30×30 km^2
PUEA Antenna Height (Ah)	2 m
Crossover Rate (CR)	0.3
Population Size (M)	50
SNR	−10 to 20
Iterations	[1, 150]
Noise	AWGN
BS Location (CRBS)	Center of the Network
SU Locations	Randomly Selected
PUEA Location	Random

3.1. Parameters for Performance Evaluation

To assess the efficiency of the proposed TDOA based localization method using DE with the previous FA, evaluation parameters used in this research are mean square error (MSE) and cumulative distribution function (CDF).

The proposed algorithm has a higher precision, which means it is more effective than the previous one. Additionally, the probabilities of false detection and correct detection are calculated to find how accurate the proposed algorithm is at detecting the attacker.

3.1.1. Mean Square Error (MSE)

The performance of the techniques that are used to find localization errors is evaluated by MSE. To calculate the MSE, the location of the attacker is calculated t number of times, so that coordinated population is determined as (a_1, b_1 … … a_t, b_t). The mean of these coordinates is determined by using (10) [23].

$$MSE\left(\overline{a},\overline{b}\right) = E[(\overline{a}-a)^2 + \left(\overline{b}-b\right)^2)] \tag{10}$$

Here:
(a,b) = real coordinates, as in (10).

$$\overline{a} = \frac{1}{t}\sum_{j=1}^{t} A_j \qquad \overline{b} = \frac{1}{t}\sum_{j=1}^{t} B_j \tag{11}$$

3.1.2. Cumulative Distribution Function (CDF)

To define how accurately the random variables are distributed, the CDF is used. The CDF aims is to finds out the likelihood that the random variable 'A' may take equal or less value to 'a' as shown in (12) [14].

$$F_A(a) = Pr(A < a) \forall\, a \in R \tag{12}$$

Here:
A = Random Variable,
$F_A(a)$ = CDF,
a = Distance Error,
$Pr(A \leq a)$ is the probability that the random variable A takes on a value less than or equal to a.

3.2. Detection Probabilities

To determine how accurately the proposed system is performing and what its probability detection rate is, two evaluation metrics are used in this research. These metrics are the probability of false alarm or false detection probability and the likelihood of detection or correct detection probability.

3.2.1. False Detection Probability

False detection probability means the likelihood of a SU affirming the existence of a PU when there is no other user in the spectrum and the channel is free. It means that PUs are inactive and SUs can use free bands easily. In this way, the system output will increase. The lower the false detection probability, the higher will be the usability of the free band. It also provides an advantage to SUs as they can send their transmissions through the band that is unoccupied by licensed users [24].

3.2.2. Correct Detection Probability (CDP)

CDP means the likelihood of a SU affirming the existence of a PU when there is a PU in the spectrum and the channel is not free. It is the time when the channel is occupied by PUs. If sensing time is much higher for SUs, PUs find no interference from SUs and can easily finish their transmissions during that period. After the PUs' transmissions are completed, SUs find the channel free [24].

3.3. Research Results

The CDF of the localization error of the PUEA for the DE algorithm is shown in Figure 4. The population size 'M' is 2, and the crossover rate 'CR' is 0.3. This plot is generated for 50 SUs. We can see that the proposed approach upgraded the limitation precision. Clearly, the higher plot shows that the performance of DE is better. When the CDF is 0.72, the MSE values increase from 0.4 m to 0.8 m. At 0.8 m MSE, CDF starts increasing from 0.72 to 0.91. The figure shows that at 0.91, the value of MSE has a higher increment from 0.8 m to 2.1 m. This increment in MSE increases the position accuracy of the attacker.

It shows that increment in the iteration number increases the localization precision. The number of SUs remains 50 for this simulation. The MSE of DE decreases with the increase in the iteration number as shown in Figure 5. Between 0 and 10 iterations, the localization error decreases, and convergence occurs faster and is supposed to be a predictable behavior. From iteration 10 to 30, the error decreases a little bit, and the plot for DE is nearly constant. When the iteration increases from 30 up to 100, the MSE value remains constant. Above 100, the MSE decreases further, but it does not touch 0, as the predictable values used for DE are not true. For FA, the MSE is a constant value above 150 iterations. It is clear from Figure 4 that the proposed DE approach is performing better than the FA.

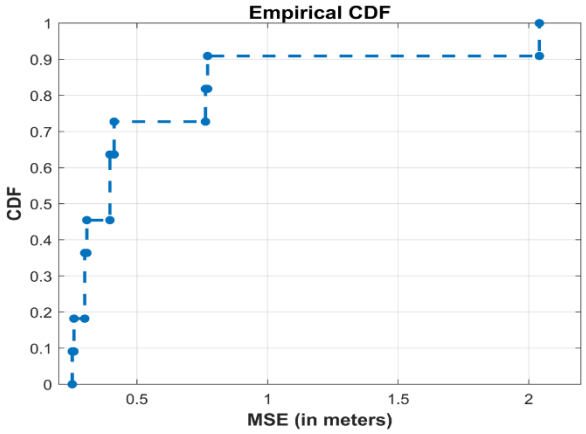


Figure 4. CDF of localization error for the DE algorithm.

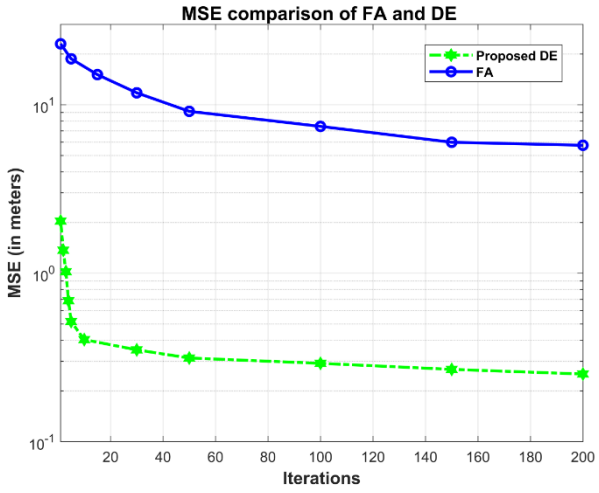


Figure 5. Effect on MSE with increase in iterations.

The deviation in MSE with the increment in SNR is shown in Figure 6. The SNR values increase from −10 dB to 30 dB where the SUs remain at 50. It is obvious from Figure 6 that DE has better performance than FA. The results show that, as the SNR values increase, the MSE declines rapidly for DE and slowly for FA. For FA, when the SNR ranges between 10 dB and 20 dB, the MSE remains constant and decreases further until 30 dB SNR. The MSE for DE declines with the increment in SNR until it reaches 30 dB. This decline in MSE shows that the proposed DE model is close to the estimated position of the attacker, as a lower MSE normally specifies an enhanced approximation.

The increment in the number of SUs greatly affects the MSE of the attacker position as shown in Figure 7. As the number of SUs is increasing, the MSE value is decreasing. The higher the number of SUs, the lower the MSE will be. The SNR value remains 10 for this simulation. It is obvious from Figure 7 that the MSE for DE is less than FA at 10 SUs. For FA, the MSE decreases faster up to 60 SUs but remains constant until the number of SUs reaches 90. After 90 SUs, the decline in MSE for FA is not significant. For DE, MSE decreases a little bit and remains constant from 30 to 90 SUs, but as the number of cooperating users increases, it further declines to some extent. Figure 7 shows that the proposed DE has higher precision than the FA.

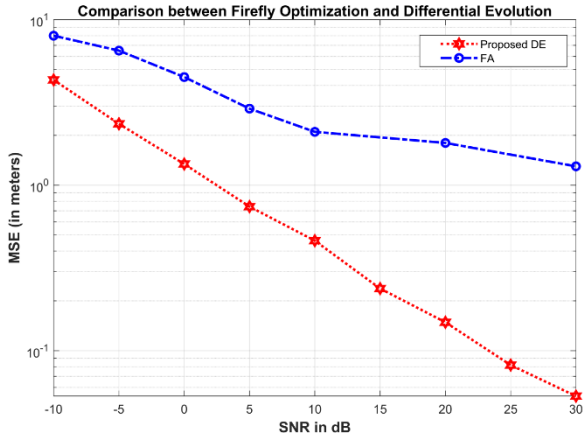


Figure 6. The deviation in MSE with SNR.

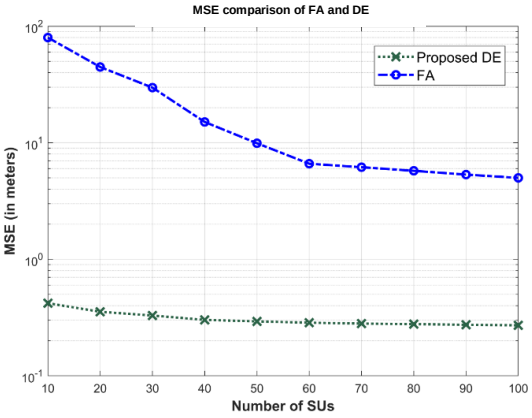


Figure 7. The deviation in MSE with the variation in the number of SUs.

The effect of changing the SNR value on the correct detection probability is shown in Figure 8. It is obvious from the graph that as the SNR increases, the likelihood for the correct detection of the PU also increases. This shows that the performance of the proposed technique is good with varying SNR. The SNR ranges from 0 dB to 200 dB, and SUs are 50.

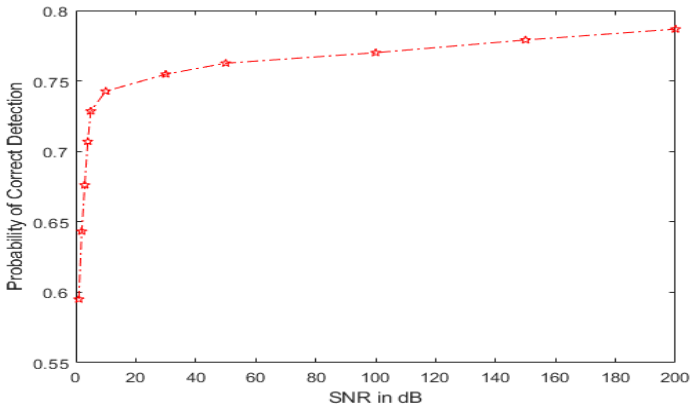


Figure 8. Probability of correct detection against SNR.

The impact of SNR on the false detection probability is shown in Figure 9. As the SNR increases, the probability decreases. It shows that the proposed system is providing free band to SUs for their transmissions because the probability of false detection is decreasing, and the channel is free for SUs.

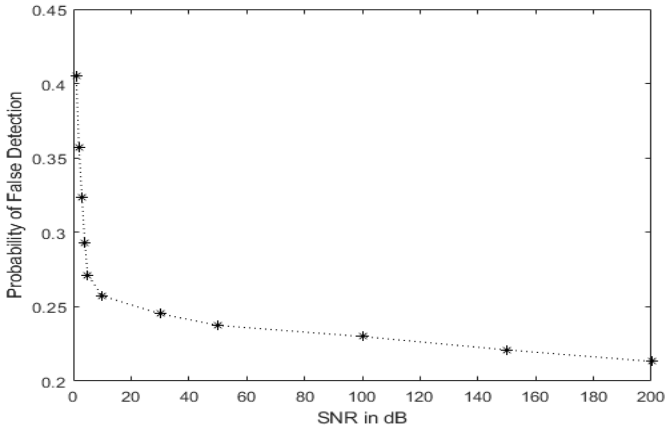


Figure 9. Probability of false detection against SNR.

The impact of varying the iteration on the probability of correct detection is shown in Figure 10. The SNR is 10 dB, and the iterations vary from 0 to 200. The number of SUs is 50 for this simulation. The value of the correct probability increases from 0 to 10 iterations. After 10 iterations, there is a little increase in probability. At 200 iterations, the probability is 0.8. It is clear from Figure 10 that the probability for correct detection increases with the increment in iterations.

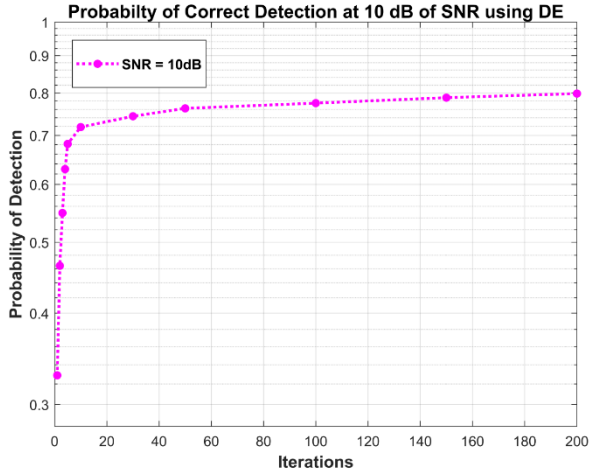


Figure 10. The probability of correct detection with varying iterations at 10 dB SNR.

4. Discussion

The effectiveness of the proposed TDOA based localization technique using the DE algorithm is examined in this section by discussing the different graphs for three types of metric parameters as presented in Section 3. PUEA is one of the most important threats that occur during the spectrum sensing process. To make the transmissions more accurate and to achieve high usage of free channels, a PUEA must be detected with higher accuracy. The proposed model has 50 random coordinates (SUs) deployed randomly in an area of 30×30 km^2. For each coordinate, distance from CRBS and fitness function are calculated, and then MSE is determined. The MSE values are checked against iterations, SNR, and number of SUs as shown in Figures 5–7, respectively. The MSE is compared with the CDF of the localization error, as shown in Figure 4. To check how accurately the proposed DE is at detecting the attacker, the probabilities for correct and false detection are checked against SNR, as shown in Figures 8 and 9, respectively.

The CDF of MSE shown in Figure 4 shows how correctly the random solutions are distributed. The higher the CDF value with the increasing MSE, the more accurate the random variables are disseminated. The comparison of MSE against iterations, SNR, and

number of SUs for the FA and proposed DE are shown in Figures 5–7, respectively. This comparison shows that the suggested DE model has better performance than FA. The MSE value for random solutions is calculated and will stop until the criteria to stop the simulation are reached. The error is calculated as:

For 200 iterations, where SUs are kept at 50 and SNR is 10 dB.
For SNR ranges from −10 dB to 30 dB, where SUs are kept at 50 and iterations are 200.
For 100 SUs, where SNR is 10 dB and iterations are 200.

The minimum value of MSE means that performance is high. Apart from these metrics, the performance is also evaluated by checking the effect of varying SNR on correct and false detection probabilities. The higher the correct detection probability, the higher the performance will be, whereas the lower the false detection probability, the higher the performance will be. It is obvious from the results that the presented DE model has an improved performance in terms of convergence speed compared to FA.

5. Conclusions

Cognitive Radio Network (CRN) is an innovative technology that utilizes free spaces in the authorized spectrum by SUs without interfering with PUs. CRN depends on spectrum sensing to look for the free spaces in the authorized spectrum that PUs are not using for their transmissions. This process of spectrum sensing, however, is interrupted by some malicious entities. These malicious entities copy the signal features of PUs and cause PUEAs, limiting the SUs from using the free band.

In this research, a TDOA based localization methodology using DE is proposed to mitigate the PUEA. The proposed CRN consists of CRBS, one PU, 50 random SUs, and a PUEA. The position of the PUEA is fixed and it can be positioned inside or outside the network. The network is designed in such a way that both the SUs and the attacker know the position of the PU. All the SUs cooperate during spectrum sensing and send the sensing information to the CRBS. The CRBS gathers all the information and applies cross-correlation to find the TDOA measurements. Afterward, these values are used to find the location of the sender, whether it is a PU or a PUEA. The DE algorithm is used for the correct estimation and to minimize the MSE so that convergence occurs faster.

The performance of the proposed algorithm is evaluated using metrics such as CDF, MSE, and the correct and false detection probabilities. The MSE is checked against three parameters: iterations, number of SUs, and SNR. As these parameters increase, the MSE decreases. Simulation results show that the proposed method increases the efficiency and the accuracy of the correct estimation of the location of the attacker. It is also obvious from the results that the proposed approach is more enhanced, precise, and effective than the techniques presented in the literature. The proposed approach is applicable only when PUs, SUs, and a PU attacker are fixed, so in the future, we will explore this technique for mobile setups with more than one attacker.

Author Contributions: Conceptualization, R.B. and N.B.; methodology, R.B. and N.B.; software, R.B.; validation, R.B., N.B. and N.M.; formal analysis, R.B., N.B., N.M. and S.A.; investigation, R.B., N.B., N.M. and S.A.; resources, R.B.; data curation, R.B.; writing—original draft preparation, R.B., N.B., N.M. and S.A.; writing—review and editing, R.B., N.B., N.M. and S.A.; visualization, R.B., N.B., N.M. and S.A.; supervision, N.B. and S.A.; project administration, N.B.; funding acquisition, S.A. and N.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank Fatima Jinnah Women University, Pak-Austria Fachhochschule Institute of Applied Sciences and Technology and Saudi Electronic University.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mitola, J. Cognitive Radio: An Integrated Agent Architecture for Software Sefined Radio. Ph.D. Dissertation, Royal Institute of Technology, Stockholm, Sweden, 2000; pp. 271–350.
2. Arjoune, Y.; Kaabouch, N. A comprehensive survey on spectrum sensing in cognitive radio networks: Recent advances, new challenges, and future research directions. *Sensors* **2019**, *19*, 126. [CrossRef] [PubMed]
3. Zheng, Y.; Chen, Y.; Xing, C.; Chen, J.; Zheng, T. A scheme against primary user emulation attack based on improved energy detection. In Proceedings of the IEEE International Conference on Information and Automation (ICIA), Ningbo, China, 1–3 August 2016.
4. Sohu, I.A.; Rahimoon, A.A.; Junejo, A.A.; Sohu, A.A.; Junejo, S.H. Analogous study of security threats in cognitive radio. In Proceedings of the 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 30–31 January 2019.
5. Ghane, A.H.; Harsini, J.S. Physical-layer information hiding technique for cognitive radio communications in cooperative relaying systems. *IET Commun.* **2019**, *13*, 124–134. [CrossRef]
6. Gul, N.; Naveed, A.; Elahi, A.; SaleemKhattak, T.; Qureshi, I.M. A combination of double sided neighbor distance and genetic algorithm in cooperative spectrum sensing against malicious users. In Proceedings of the 14th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 10–14 January 2017.
7. Sun, X.; Zhou, R.; Wu, H.; Gao, L.; Zhang, Y. Angle based malicious user detection for wideband cognitive radio network. In Proceedings of the 20th International Symposium on Wireless Personal Multimedia Communications (WPMC), Bali, Indonesia, 17–20 December 2017.
8. Karimi, M.; Sadough, S.M.S. Efficient transmission strategy for cognitive radio systems under primary user emulation attack. *IEEE Syst. J.* **2017**, *12*, 3767–3774. [CrossRef]
9. Ta, D.T.; Nguyen-Thanh, N.; Maillé, P.; Nguyen, V.T. Strategic surveillance against primary user emulation attacks in cognitive radio networks. *IEEE Trans. Cogn. Commun. Netw.* **2018**, *4*, 582–596. [CrossRef]
10. Bouabdellah, M.; Ghribi, E.; Kaabouch, N. RSS-based localization with maximum likelihood estimation for PUE attacker detection in cognitive radio networks. In Proceedings of the IEEE International Conference on Electro Information Technology (EIT), Brookings, SD, USA, 20–22 May 2019.
11. El Mrabet, Z.; Arjoune, Y.; El Ghazi, H.; Abou Al Majd, B.; Kaabouch, N. Primary user emulation attacks: A detection technique based on Kalman filter. *J. Sens. Actuator Netw.* **2018**, *7*, 26. [CrossRef]
12. Dong, Q.; Chen, Y.; Li, X.; Zeng, K.; Zimmermann, R. An adaptive primary user emulation attack detection mechanism for cognitive radio networks. In Proceedings of the International Conference on Security and Privacy in Communication System, Singapore, 8–10 August 2018; Springer: Cham, Switzerland, 2018.
13. Saifuddin, K.M.; Reza, K.F.; Fahim, M.A.; Alam, S.S. Detection of primary user emulation attack in cognitive radio environment. In Proceedings of the 6th International Conference on Informatics, Electronics and Vision and the 7th International Symposium in Computational Medical and Health Technology (ICIEV-ISCMHT), Himeji, Japan, 1–3 September 2017.
14. Armi, N.; Gharibi, W.; Khan, W.Z.; Zangoti, H.; Rizvi, S.; Wael, C. Error detection of malicious user attack in cognitive radio networks. In Proceedings of the International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), Jakarta, Indonesia, 23–24 October 2017.
15. Karimi, A.; Taherpour, A.; Cabric, D. Smart traffic-aware primary user emulation attack and its impact on secondary user throughput under rayleigh flat fading channel. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 66–80. [CrossRef]
16. Li, K.; Wang, J. Optimal joining strategies in cognitive radio networks under primary user emulation attacks. *IEEE Access* **2019**, *7*, 183812–183822. [CrossRef]
17. Ghanem, W.R.; Shokair, M.; Desouky, M.I. An improved primary user emulation attack detection in cognitive radio networks based on firefly optimization algorithm. In Proceedings of the 33rd National Radio Science Conference (NRSC), Aswan, Egypt, 22–25 February 2016.
18. Ghanem, W.R.; Essam, R.; Dessouky, M. Proposed particle swarm optimization approaches for detection and localization of the primary user emulation attack in cognitive radio networks. In Proceedings of the 35th National Radio Science Conference (NRSC), Cairo, Egypt, 20–22 March 2018.
19. Mohammed, A.S.; Olaleru, G.; Ohize, H.; Dauda, U.S. Optimal Detection Technique for Primary User Emulator in Cognitive Radio Network. In Proceedings of the 2021 1st International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS), Abuja, Nigeria, 15–16 July 2021.
20. Inamdar, M.A.; Kumaraswamy, H.V. Accurate primary user emulation attack (PUEA) detection in cognitive radio network using KNN and ANN classifier. In Proceedings of the 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), Tirunelveli, India, 15–17 June 2020; pp. 490–495.
21. Jayapalan, A.; Savarinathan, P.; Chenna Reddy, J.; Baskar, J.D. Detection and Defense of PUEA in Cognitive Radio Network. *Arab. J. Sci. Eng.* **2021**, *46*, 4039–4048. [CrossRef]
22. Sureka, N.; Gunaseelan, K. Investigations on detection and prevention of primary user emulation attack in cognitive radio networks using extreme machine learning algorithm. *J. Ambient. Intell. Humaniz. Comput.* **2021**, 1–10. [CrossRef]

23. Nurellari, E.; McLernon, D.; Ghogho, M. A secure optimum distributed detection scheme in under-attack wireless sensor networks. *IEEE Trans. Signal Inf. Process. Netw.* **2018**, *4*, 325–337. [CrossRef]
24. Mor, T.; Arora, D. Simulation of probability of false alarm and probability of detection using cyclo stationary detection technique in coginitive radio. *Int. J. Electron. Commun. Technol.* **2015**, *6*, 62–66.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.