Detection of SSDF Attack in Cooperative CR Networks with Machine Learning approach

C.Rajeswari[1,2*] and S.Saheb Basha [3]

[1]Research Scholar, Department of ECE, JNTUA,Anantapuram, India
[2]Assistant Professor,Department of ECE, G.Pulla Reddy Engineering College, Kurnool, India
[3] Professor,Department of ECE, G.Pulla Reddy Engineering College, Kurnool, India
rajeswari.ch@gmail.com

Abstract. Cognitive radio network is a Swireless network with transceivers that can intelligently detects which communication channels are in use and which are not in use. In a cognitive radio network, a transceiver uses intelligence to determine which communication channels are being used and which are not. By allowing secondary users to occasionally use spectrum allotted to primary users without disturbing them, Cognitive Radio Networks (CRNs) are intended to increase spectrum utilisation. Tosense the spectrumand to data transfer in this dynamic environment, CRNs depend on user cooperation. Malicious actions, such spectrum sensing data falsification (SSDF) attacks, can interfere with CRN functionality, resulting in data corruption, network inefficiencies, and missed spectrum opportunities. Byzantine assaults are another name for spectrum sensing data falsification (SSDF) attacks. This assault is a situation where malevolent nodes or attackers attempt to undermine the network's integrity by supplying inaccurate information. These attacks can happen in CRNs during spectrum sensing, where the attackers may trick the network into erroneously determining whether primary users are present or not. In the first place, this assault makes a group of benign nodes in any network malicious. The attacker then uses this group of nodes to take over the network. This group of nodes eventually turns into selfish nodes and is the cause of network data manipulation. This study suggests a unique method that uses decision trees and random forests to identify byzantine attacks in CR networks.

Keywords: Spectrum Sensing, Machine Learning, Cognitive Radio Network, Byzantine Attack, spectrum sensing data falsification Attack.

1 Introduction

Cognitive Radio Networks (CRNs) represent an innovative approach to wireless communication systems by integrating cognitive capabilities into traditional radio devices. The main intent of CR networkis enhancement of utilization of spectrum, improve communication reliability, and enable dynamic spectrum access. This tech-

B. S. Babu et al. (eds.), *Proceedings of International Conference on Advanced Materials, Manufacturing and Sustainable Development (ICAMMSD-2024)*, Advances in Engineering Research 257,
https://doi.org/10.2991/978-94-6463-662-8_82

nology is driven by the increasing demand for wireless communication services and the deficit of available frequency bands. Cognitive Radio (CR) refers to a type of intelligent radio that can sense its operating environment, learn from it, and adapt its parameters to optimize spectrum usage. In the context of networks, Cognitive Radio Networks employ multiple cognitive radios to create a dynamic and flexible communication infrastructure. Among the fundamental aspects of CRNs sensingthe spectrum is one, where devices analyse the radio frequency spectrum to identify unused or underutilized frequency bands. This enables CR devices to opportunistically access available spectrum without causing interference to licensed users.

2 Literature Work

Danish Mehmuda, Dhrupam Patel, and Chinmay Bhagat presented a method in 2023 for identifying byzantine attacks in cognitive radio networks as Because they can opportunistically exploit white spaces to increase the utilization of underutilized spectrum, Cognitive Radios (CRs) have become increasingly popular [1]. Cooperative spectrum sensing (CSS) is a technique used by Cognitive Radio to find free licensed spectrum. This study investigates centralized CSS in which secondary users (unlicensed users) detect a band that is owned by the primary user and inform the decisioncentre, which takes the ultimate decision to grant access to the channel. There are many assaults that can result in different security risks in cognitive radio networks (CRNs) due to their openness. Among these attacks is thefalsification (SSDF) attack.In order to identify attackers in the CRN, this research suggests an anomaly detection approach based on isolation forests. To demonstrate how well the suggested system detects malevolent users in various attack scenarios, a number of simulations are run.

In 2020, RupamSarmah, Amar Taggu, and NingrinlaMarchang presented a machine learning-based solution for detecting byzantine attacks in CR networks. Spectrum sensing is one of the main roles of a CR network [2]. In an infrastructure-based CRN, a decision centre (FC) combines the reports of sensing from each nodeand makes the final conclusion rather than each node separately detecting the incumbent signal and making judgments based on it. It is recognized that this type of collaborative spectrum sensing (CSS) improves sensing accuracy. However, the Byzantine security attack can compromise CSS. This attack, in which a node intentionally fabricates the report of sensing before forwarding it to the FC so that interfere with the spectrum sensing procedure. In order to detect SSDF assaults in a CR networkin which the reports of sensing are binary, this study examines the application of machine learning methods, specifically Neural Networks, Naive Bayes, SVM and Ensemble classifiers. Two experimental scenarios are utilized to study the learning techniques: (a) dataset usedfor both training and testing is same, and (b) different data sets for robust, demonstrating consistently excellent performance even when there are different levels of attackers present in the system.

According to a 2015 system suggested by Linyuan Zhang, GuoruDing, and QihulWu, wireless networks are endangered to a variety of reliabilitythreats, assaults, including

wiretaps, spoofing, jamming, and others, because wireless channels are open. In general, attackers seek to impair wireless networks' availability, confidentiality, integrity, and access control [3]. CRnetworks, which provide a propitiousmodel to enhance radio spectrum utilization by enabling cognitive or unlicensed secondary users (SUs) to strategically utilize frequency band gaps not used by licensed primary users (PUs), do present all of these security risks. The intelligent behaviour of CRNs created a number of new types of assaults in addition to the well-known traditional security issues. These attacks significantly hinder the use of cognitive radio techniques in the military and in commerce. In particular, the main threats to effectiveness of CRNs is attacks on band sensing.It is considered as a crucial enabling method that allows cognitive radios to detect the presence of spectrum holes and learn from their surroundings. However, spectrum sensing is susceptible to spectrum sensing attacks and can be deceived by hostile opponents in an open wireless environment.

3 Methodology

The block diagram shown in the figure-1 depicts the various methods and steps included in the proposed method. Using Dijkstra's algorithm, create a node and determine the shortest path. The Byzantine assault dataset was used as input for this system. The dataset repository provided the raw data. The data pretreatment procedure must then be put into action. In order to prevent incorrect predictions, we must deal with the missing values in this stage. Label encoding must then be used. The data separation must then be put into practice. We must separate the data into test and train sets in this step. Next, in order to detect the assault, we applied machine learning techniques algorithms Random Forest and Decision Tree. The performance metricsare accuracy, precision, recall and F1 score.

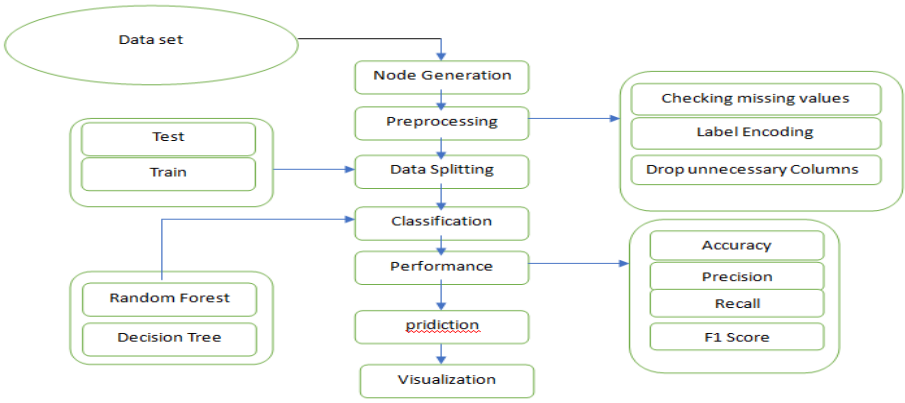

Fig.1. Block Diagram

4 Experimental Results

The figures shown below are the images obtained at each step of detection of byzantine attack. The figure 5 is the interface that is created with the code written and the figure 6 is the graph in which the source and destination nodes are created successfully. The figure 7 shows that the path is created between the nodes successfully**.**

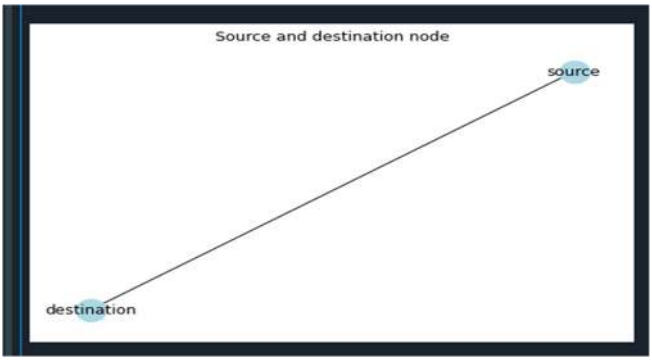

Fig.2. Node Creation

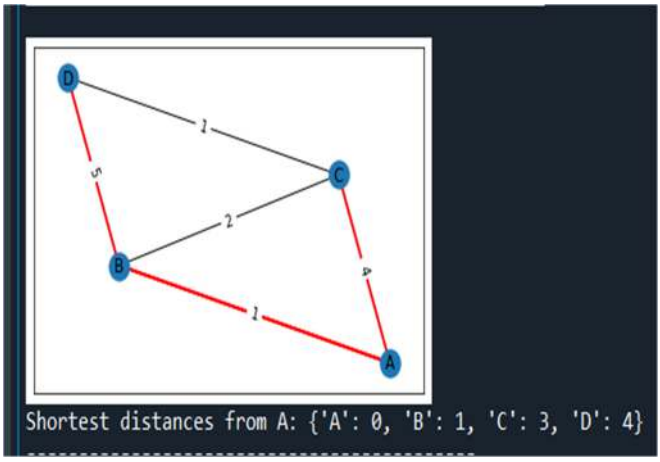

Fig.3. Path Creation

The data selected is shown in the Fig. 4. and the accuracy value, classification report of the data based on the random forest classifier is shown in the Fig. 5.

```
------------------------------------------
BYZANTINE ATTACK IN COGNITIVE RADIO NETWORKS
------------------------------------------

-------------------------------
Data Selection
-------------------------------

       id   Time   Is_CH  ...   send_code   Expaned Energy  Attack type
0   101000     50       1  ...           0         2.46940       Normal
1   101001     50       0  ...           4         0.06957       Normal
2   101002     50       0  ...           3         0.06898       Normal
3   101003     50       0  ...           4         0.06673       Normal
4   101004     50       0  ...           3         0.06534       Normal
5   101005     50       0  ...           3         0.06717       Normal
6   101006     50       0  ...           4         0.06214       Normal
7   101007     50       0  ...           3         0.06662       Normal
8   101008     50       0  ...           4         0.06649       Normal
9   101009     50       0  ...           1         0.07903       Normal
10  101010     50       1  ...           0         2.36110       Normal
11  101011     50       0  ...           4         0.06130       Normal
12  101012     50       0  ...           4         0.06425       Normal
13  101013     50       0  ...           3         0.07263       Normal
14  101014     50       0  ...           3         0.06716       Normal

[15 rows x 19 columns]
```

Fig.4. Data Selection

```
          Random Forest Classifier
-------------------------------------------

1) Accuracy =  99.71441154097661 %

2) Classification Report

              precision    recall  f1-score   support

           0       0.99      1.00      0.99      2024
           1       0.95      0.99      0.97       656
           2       0.99      0.99      0.99      3002
           3       1.00      1.00      1.00     67965
           4       1.00      0.93      0.96      1286

    accuracy                           1.00     74933
   macro avg       0.98      0.98      0.98     74933
weighted avg       1.00      1.00      1.00     74933
```

Fig.5. Simulation parameters based on RF classifier

The accuracy value and performance metrics in the classification report are shown in the Fig. 6. and Fig. 7. is the information containing in the dataset and type of attack detected.

```
-------------------------------------------
          Decision Tree Classifier
-------------------------------------------

1) Accuracy =  99.72108416852387 %

2) Classification Report

              precision    recall  f1-score   support

           0       0.99      1.00      0.99      2024
           1       0.95      0.99      0.97       656
           2       0.99      0.99      0.99      3002
           3       1.00      1.00      1.00     67965
           4       1.00      0.93      0.96      1286

    accuracy                           1.00     74933
   macro avg       0.98      0.98      0.98     74933
weighted avg       1.00      1.00      1.00     74933
```

Fig.6. Simulation parameters based on DT classifier

```
102024
103
1
102024
0
1
3
0
37
1
0
0
0
1258
16
113.27654
0
2.16533
Byzantine attack
```

Fig.7. Type of Attack

5 Conclusion

To sum up, this work addressed the crucial problem of SSDF attacks in CR networks, acknowledging the possible risks they represent to the dependability and functionality of these systems. The study emphasizes how serious Byzantine attacks are in cognitive wireless networks and how the network can jeopardize accuracy of sensing and coming to conclusion about availability of frequency band. In the zestful and decentralized CR networks, detecting Byzantine attacks is a difficult task. The detection procedure is made more complex by the dynamic nature of spectrum availability and the requirement for quick decision-making. The study suggested a method for identifying this kind of attacks in dynamic network like CRNs that makes use of Dijkstra's algorithm, Random Forest (RF), and Decision Tree (DF) classifiers. Through simulation, the suggested mechanism's efficacy was shown. The suggested approach's 99.7% accuracy rate in identifying byzantine attacks is significantly higher than that of the current system. The findings show that the capacity to identify and separate rogue nodes has significantly improved. The suggested detection mechanism opens the door for more secure and dependable communication in dynamic contexts by significantly improving the durability and credibility of these networks.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Mehmuda, Danish, Chinmay Bhagat, Dhrupam Patel, Kamal Captain, and Ashok Parmar,Defense against Byzantine attack in cognitive radio using isolation forest. In 2023 15th International Conference on Communication Systems & Networks (COMSNETS), pp. 314-318, IEEE(2023).
2. Sarmah, Rupam, Amar Taggu,NingrinlaMarchang,Detecting Byzantine attack in cognitive radio networks using machine learning. Wireless Networks 26, no. 8,pp. 5939-5950 (2020).
3. Yu, F. Richard, Helen Tang, Minyi Huang, Zhiqiang Li, and Peter C. Mason,Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios. In MILCOM 2009-2009 IEEE Military Communications Conference, pp. 1-7. IEEE9(2009).
4. Burbank, Jack L,Security in cognitive radio networks: The required evolution in approaches to wireless network security.In 2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications , pp. 1-7, (2008).
5. Rifà-Pous, Helena, Mercedes Jiménez Blasco, and CarlesGarrigues,Review of robust cooperative spectrum sensing techniques for cognitive radio networks, Wireless Personal Communications 67 pp 175-198.,(2012).