International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6534
***Article Received**: 25 January 2023 **Revised**: 21 February 2023 **Accepted**: 08 March 2023*

A Jamming Attacks Detection Approach Based on CNN based Quantum Leap Method for Wireless Sensor Network

M. Sahaya Sheela[1], M. Balasubramani[*2], J. J. Jayakanth[3], R. Rajalakshmi[4], K. Manivannan[5], D. Suresh[6]
[1]Assistant Professor ,Department of Electronics and Communication Engineering
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology
Chennai, Tamil Nadu-600062
e-mail: hisheelu@gmail.com
[2]Assistant Professor Senior Grade 2,School of Information Technology and Engineering
Vellore Institute of Technology-Vellore
Tamil Nadu 632014
e-mail: m.balasubramani@vit.ac.in (Corresponding Author)
[3]Assistant Professor,Department of Computational Intelligence
SRM Institute of Science & Technology
Kattankulathur, Chennai, India – 603203
Email: jj.jayakanth@gmail.com
[4]Assistant professor Grade-1, Department of Electronics and Communication Engineering, Panimalar Engineering college, Poonamallee, Chennai, Tamil Nadu 600123, India, Email: rajeeramanathan@gmail.com
[5]Professor , School of Computer Science and Engineering
Faculty of Engineering and Technology, JAIN (Deemed-to-be) University
Bengaluru, Karnataka, India – 562112.
Email: manivannan.k@jainuniversity.ac.in
6Professor,Department of Computer Science and Engineering
PSNA College of Engineering and Technology
Dindigul-624622, Tamil Nadu, India

Abstract— The wireless sensor network is the most significant largest communication device. WSN has been interfacing with various wireless applications. Because the wireless application needs faster communication and less interruption, the main problem of jamming attacks on wireless networks is that jamming attack detection using various machine learning methods has been used. The reasons for jamming detection may be user behaviour-based and network traffic and energy consumption. The previous machine learning system could not present the jamming attack detection accuracy because the feature selection model of Chi-Squared didn't perform well for jamming attack detections which determined takes a large dataset to be classified to find the high accuracy for jamming attack detection. To resolve this problem, propose a CNN-based quantum leap method that detects high accuracy for jamming attack detections the WSN-DS dataset collected by the Kaggle repository. Pre-processing using the Z-score Normalization technique will be applied, performing data deviations and assessments from the dataset, and collecting data and checking or evaluating data. Fisher's Score is used to select the optimal feature of a jamming attack. Finally, the proposed CNN-based quantum leap is used to classify the jamming attacks. The CNN-based quantum leap simulation shows the output for jamming attacks with high precision, high detection, and low false alarm detection.

Keywords- CNN based Quantum leap, wireless sensor networks, Z-score Normalization technique, Fisher's Score.

I. INTRODUCTION

Wireless communication uses by the military and air force, government sectors and various places. WSN communication needs the privacy of one user to another user. The major problem of WSNs is jamming attacks based on users' behaviours. The jamming problems mainly occur in energy problems, simultaneous multi-users using the network, or users uploading a large dataset that places the network jamming.The jamming attack detection mostly low and high energy consumption might interrupt the network communication issues that occur, the third party users sometimes hacking the network at time jamming attack occurs. So some differences arise in our networks. The problem may be packet delay performance, packet dropping problems, transmission delays, etc.

The proposed method is deep learning high-level jamming attack detection and accuracy. The above algorithms could not

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6534
***Article Received**: 25 January 2023 **Revised**: 21 February 2023 **Accepted**: 08 March 2023*

have enough detection accuracy, but CNN has enough given some level of accuracy, which is not enough for the proposed system to export CNN based Quantum leap method have full fill the jamming detection and accuracy. The Quantum Leap method has been fast and quickly detecting jamming attacks. The proposed experimental evaluation uses the WSN-DS dataset (Wireless Sensor Networks DataSet) for using jamming attack detection and classification using the CNN-based Quantum leap method detecting the jamming attack detection.

The proposed system of the CNN-based Quantum leap method has improved detection accuracy, increased the packet delivery ratio, improved network transmission level and quickly found out the jamming attacks and packet loss easily found out there. More wireless applications might cause the jamming attack to interrupt the working; the CNN-based Quantum leap method has the best result and given the excellent jamming attack accuracy of wireless sensor networks.

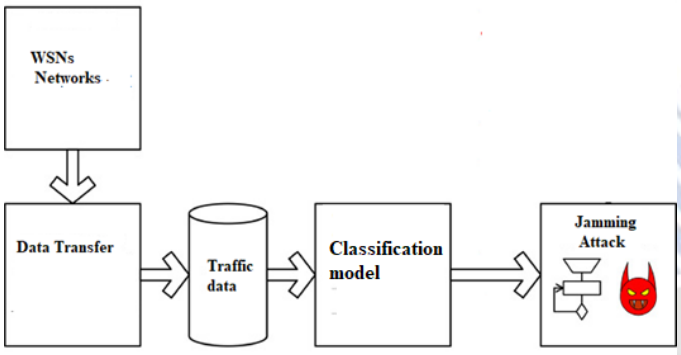

Figure.1 general architecture WSN jamming Attacks

The figure.1 define the general architecture of wireless sensor networks, it has been analysing the data transfer and jamming attack detection The previous machine algorithm of linear regression, SVM, Naive Bayes, and Random forest algorithm gave low jamming attack detection accuracy. Machine learning has low levels of dataset-only classification of the networks. The user expert the large dataset classification by we are using deep understanding based CNN-based Quantum leap method to full fill the jamming detection and accuracy of wireless sensor networks

II. Related Works

Utilizing Programming Defined Radio (SDR), four kinds of sticking assaults, specifically barrage, convention acknowledgement, single tone and progressive heartbeat, are sent off and explored. The range of interference, the complexity of the launch, and the severity of the attack are all considered when evaluating each class qualitatively [1].

For vehicular traffic environments, a plan based on machine learning is proposed as a finite anti-jamming protocol. It focuses on discriminative vehicle signal detection and filtering to pinpoint the precise location of overloaded vehicles. The proposed anti-interference strategy's performance is compared to that of cutting-edge technologies. [2].

Implement a detection framework based on a series of tests of multiple hypotheses using algorithms based on variation and Channel State Information (CSI) to detect these attacks. Using a quaternary hypothesis test, the diagnostic framework distinguishes between legal and illegal transfers and the nature of unlawful transfers. [3].

Propose a structure for mental security diagnostics that incorporates an assault identification module that utilizes supervised learning (SL), semi-supervised learning (SSL), and unsupervised learning (UL) strategies, as well as an assault limitation module that decides the area of a messed up Connection and terrible association. [4].

This model is based on Bayesian learning with discovery and moderation parts. Then again, the assault location part makes an example of test proof for distinguishing sneak assaults. Conversely, the alleviation part utilizes streamlining hypothesis to accomplish the vital harmony among execution and security. [5].

Because of capacity to manage encrypted threat techniques are quickly advancing, machine learning (ML)- based interruption and peculiarity location has as of late acquired notoriety. This paper looks at the advantages, disadvantages, and capability of machine learning (ML) and deep learning (DL) techniques for IoT gadget security. [6].

A lot of research has been done to find a better way to protect IoT devices, deal with those problems, eliminate those risks, or reduce their impact on user privacy and security requirements. There are four parts to the questionnaire. The most critical IoT device limitations and their solutions are examined in the first section. [7].

Two remarkable cases are the focal point of insightful models. Because of the intricacy of the general issue, we present a calculation that utilizes simulated intelligence strategies to manage the open case. Our reenactment exhibits that our strategies have high recognition rate and low misleading positive rate to recognize unapproved range utilization successfully. [8]

A combination center is utilized in the proposed plan to consolidate recognition information from various sub-clients. Heavily influenced by the necessary phony problem likelihood, the consolidated loads are upgraded to boost the recognition likelihood of accessible channels. Likewise, inspect what channel assessment mistakes mean for recognition probabilities. [9].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6534
***Article Received**: 25 January 2023 **Revised**: 21 February 2023 **Accepted**: 08 March 2023*

A self-cooperative portion's relapse model is examined to further develop early assault identification in the proposed location framework. The outcome shows the way that this strategy can distinguish digital assaults before they have a huge effect, with actual effect. A promising methodology for safeguarding ICS is a multifaceted information based digital assault discovery framework that utilizations organization, plan and execution information. [10].

Two test rules are created in view of the summed up probability proportion test and the Rau test, whose asymptotic way of behaving is inspected and an upper bound is given. Likewise, a widespread GMNP-based helpful phantom identification technique has been created to increment discovery effectiveness. Furthermore, point by point re-enactments are introduced to check the presentation of the proposed plans under different boundary settings. [11].

Attackers can take advantage of reconfiguration by installing malicious code on cognitive radios. Also, since cognitive radio organizations are remote, they face every one of the exemplary dangers in regular remote organizations. This paper means to outline the risks and security challenges confronting Mental Radios and Mental Radio Organizations, alongside the present status of the artistry in recognizing related assaults. In addition, the difficulties that lie ahead are addressed. [12].

The proposed CR networks characterize an enemy of the PUE assault technique by conviction engendering, which tries not to utilize other sensor organizations and costly equipment on the organizations used in the current writing. Each secondary user computes a local and matching function, calculates messages and transfers messages with neighbours, and calculates beliefs until convergence in our proposed method. [13].

In a cognitive radio organization, without a trace of essential (authorized) clients, optional (unlicensed) clients are permitted to get to the authorized range. To prevent PUE attacks in the first place, we offer our scan-intensive algorithm. The consequences of our reproduction show that our proposed power examination strategy gives improved results than existing methods. 14].

In wired and wireless networks, privacy and security challenges are valuable. These difficulties are most severe in CR networks. Due to their distinctive features and intended uses, these networks are tempting targets for attacks and intrusions. Spectrum Sensing faces one of the most significant security risks: the master user spoofing attack. [15].

The security of mental radio organizations has become a critical consider the improvement of mental radio innovation. In mental radio organizations, a mix of assaults called Principal User Emulation Attacks (PUEA) is utilized. In the plan, we pick delicate combination as combination strategy and helpful range detecting framework as our model. [16].

This optimisation problem aims to identify the beam-forming coefficients with the lowest probability of spoofing sensitive data into the spectrum. The simulation results show that the effective countermeasure is effective compared to optimized techniques in various channel conditions. [17].

Investigate the presentation of the proposed procedure utilizing reenactment models and hypothetical examination. In basic client pantomime assaults, essential and noxious clients can be related to high precision utilizing an AES-helped DTV plot. It ought to be underlined that the proposed conspire requires no framework design or equipment changes, with the exception of a pluggable AES chip. [18].

Cognitive radio (CR) is a promising methodology for expanding network range use and productivity. In any case, individuals from a CR association might consolidate destructive enemies who embrace misleading and pointless practices to seek after the association. [19].

Furthermore, mental radio organizations face each of the customary threats related with ordinary remote organizations, since they are wireless. Additionally, the forthcoming difficulties have been tended. [20]. Most cases cluster ensemble approach are implemented with Fuzzy logic based on ANN to resolve the detection problem [21]. In addition MANET resources Clusters are implemented bases on feature selection and classification model [22, 23]. The purpose behind this paper is to give an outline of the condition of the hardships looked by security danger discovery and insight radios, radio organizations and related assaults.

2.1 Problem Definition

Jamming attack is one of the main problems in WSN. The hacker creates various attack models to affect the data transmission using a jammer point in the communication medium. So jamming feature principles are more difficult to analyse increasing false rate, time complexity give a chance to attackers more vulnerable.

2.2 Objective of the Paper

The main objective of this paper improving jamming attack detection and accuracy performance in WSN. To design a proposed methodology deep learning based quantum leap method to identify the jamming attack. Pre-processing using the Z-score Normalization technique will be applied, performing data deviations and assessments from the dataset and collecting and evaluating data. Fisher's Score is used to select the optimal feature of a jamming attack. Finally the proposed CNN based quantum leap method efficiently identifies the jamming attacks in WSN.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6534
Article Received: 25 January 2023 Revised: 21 February 2023 Accepted: 08 March 2023

III. PROPOSED METHODOLOGY

The wireless application is faster communication and less interruption in the real world, the main problem of jamming attack detection on wireless networks. Previous various detection methods using but not better results for jamming attack detection and accuracy. The proposed system discusses the CNN-based quantum leap method to apply here. This method is used to improve the best jamming detection and accuracy.

3.1 WSN-DS Description

WSN-DS, a specific remote dataset for interruption recognition, was utilized to characterize assaults for test results. Every one of the 374,661 straightforward linkage vectors has 23 capabilities and is sorted as one or the other steady.

Table I: Number of records used in training and testing datasets

Class	Number of records used in dataset	
	Training set (70%)	Testing set (30%)
Normal	238103	101963
Constant jamming	10233	4363
Random jamming	6960	3089
Deceptive jamming	4650	1988
Reactive jamming	2316	996

The particular sorts of attacks, aside from the commonplace case (no episode), are assembled into various kinds of assault: steady, irregular, tricky, and responsive. WSN-DS is parted into 70% of preparing information and 30% of testing. Table I shows the information division. Fisher scientific scoring is a measurable strategy principally utilized for dimensionality decrease. The choice of characteristics containing fundamental data is not difficult to decipher and lessens the computational time expected, as displayed in figure 2.

3.2. The Deployment Architecture

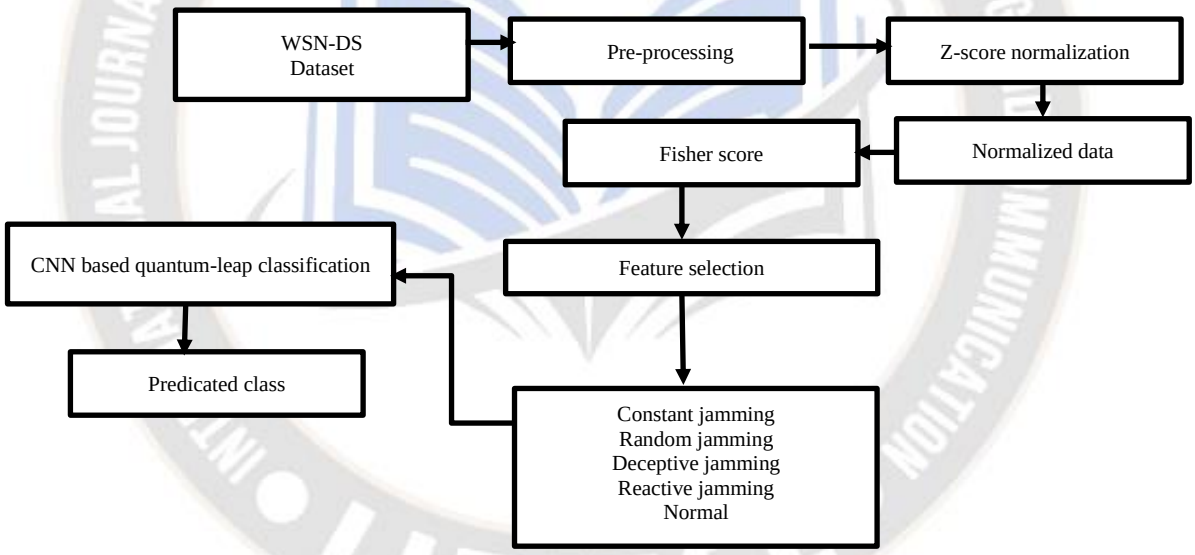

Figure.2 proposed system

Reasons for interference detection may be based on user behaviour and network traffic, and power consumption. The currently proposed system uses the CNN-based quantum leap method deep learning method shown in Fig. 2. Propose a CNN-based quantum leap method that detects high accuracy for interference attack detections on the WSN-DS dataset collected by the Kaggle repository.

3.3 Pre-processing based on Z-score normalization

Preprocessing is used to gather information from the data set. The attribute has ordered the training model, and after the best training model to apply preprocessing, the processing involves three phases.

(1)The training process has processed the data collection and transfer to another node or fed to the node.
(2)The validation process is used to collect the offline data to test data using a new algorithm.
(3).The testing process is used for real-time data collection and to apply the test to find the jamming attacks.

The Z-score is a proportion of change that addresses how much standard deviations from the mean. You will utilize the z-score to ensure that your part disseminations mean = 0 and sexually transmitted disease = 1. This can be important when there are a few exemptions, yet not so many that you need to scale back.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6534
***Article Received**: 25 January 2023 **Revised**: 21 February 2023 **Accepted**: 08 March 2023*

The formula for calculating the z-score of a point, x, is as follows:

Z-score normalization $x' = \frac{x-\mu}{\sigma}$ (1)

x is original values , μ: Mean of data,

σ: Standard deviation of data

Calculate variance: $\sigma = \sqrt{\sum(x-\mu)^2/N}$ (2)

Standardization is the concept and step of putting different variables on the same scale. This concept allows comparing scores between different types of variables.

Equation of Standardization:

$z = (x-\mu)/\sigma$ (3)

Where x is the original feature

A z-score addresses the quantity of standard deviations a worth (x) is above or underneath the mean of the numbers when the information is typically dispersed. Utilizing z-scores permits you to decipher a worth's mean separation from the standard into units of standard deviations.

Renormalize the ostensible Fisher's F-score to manage ordinal information. In this sense, we add a holding up period which presents a more exorbitant cost for different classes. This cost will compel the element determination technique to zero in additional on highlights that assistance to separate courses a ways off in the consistency basis (to keep away from the above blunder).

3.4 Fisher score based Feature selection

Fisher score for include choice We currently depict the issue of regulated highlight determination with an informational collection {xi, yi} i=1. Our point is to track down a subset of elements of size m (where m < d) that contains undertakings with extra data. Fisher's score for highlight determination [6] is proposed as a heuristic methodology to figure a free score for each element utilizing the notable idea of Fisher's relationship.

Let μ_k^i and σ_k^i k be the mean and standard deviation of the k-th class and i-th feature (and μ i and σ i the mean and standard deviation of the whole dataset for the i-th feature. The Fisher score for the i-th feature (x') can be computed as:

$$f(x') = \frac{\sum_{k=1}^{K} N_k(\mu_k^i - \mu')^2}{\sum_{k=1}^{K} N_k(\sigma_k^i)^2} \quad (3)$$

Another measure of dispersion applies the arithmetic mean (AM) and the geometric mean (GM). For a given (positive) feature Xi on n patterns, the AM and GM are given by

$$AM_i = x' = \frac{1}{n}\sum_{j=1}^{n} x^i \quad (4)$$

$$GM_i = \sum_{j=1}^{n}(\pi^n x')^2 \quad (5)$$

Respectively; since if (AMi ≥ GMi,) with equality holding if and only

$$RM_i = \frac{AM_i}{GM_i} \in (1+\infty) \quad (6)$$

Here Equation (6) can be used as a dispersion measure. Higher dispersion implies a higher value of Ri, thus a more relevant feature

N_k is the quantity of states of class C_k. As this score is determined separately, the chose highlights address a subset. Likewise, this heuristic might neglect to choose highlights that are repetitive or have a high consolidated discriminative power. In exploratory outcomes this strategy is named ostensible Nominal Feature Selection (NFS).Constant jamming: a constant jammer continuously produces radio signals completely random.

- Random jamming: a random jammer works randomly in two states; sleep and jamming.
- Deceptive jamming: as deceptive jammer is a constant jammer that continuously transmits regular packets
- Reactive jamming: presented a machine learning-based jamming detection approach capable of detecting constant and reactive jammers under various scenarios
- Normal: In a false negative, the system decides that the situation is normal while in reality there is an attack.

3.5 CNN-based quantum-leap classification

The classifier is the best from CNN-based quantum-leap classification. This is the best result for jamming detection and accuracy of the wireless sensor network because previous classification algorithms are differentiated but CNN based quantum-leap classification has been best result for jamming detection and accuracy.

The decision limit or so-called hyper plane separating the classes has weighting coefficients given by the x is original values, which we need to estimate. Figure.3 discuss the CNN based quantum-leap classifier tries to maximize the distance W (α), this $x'is$ z − score normalization and the nearest points so that it becomes our constraint. This is equivalent to minimizing the following equation:

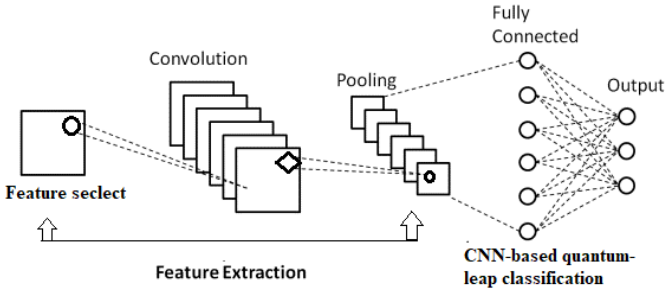

Figure.3 CNN-based quantum-leap classification

$$W(\alpha) = \sum_{i=1}^{l} f(x') + N_k(\mu_k^i - \mu')^2 + RM_i \quad (4)$$

Subject to $\sum_{i=1}^{l} y_i\alpha_i = 0$ (5)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6534
***Article Received**: 25 January 2023 **Revised**: 21 February 2023 **Accepted**: 08 March 2023*

Here equation (4) and (5) where l is the number of data points in our training data, y denote the outputs of the data points, x is the feature in each training example, and α is the constant. Figure.2 is a quantum-leap classification performance that has been defined here. How to detect the jamming attack in wireless sensor networks.

Algorithm-CNN based quantum-leap

Step1:

Input d: dataset, dataset true labels W:

d= RM_i

W=d

Step2:

Score of CNN Trained model on test dataset (w)

Step3:

Let f be feature select from W

Step 4:

For j in i do

Vj <= victories (j, w)

Filter the feature select Vj to fi

Filter the score of fi to f

Step5:

f_{train}, f_{test}, f_{train} , l_{test}, - split feature set labels in to train subset and test subset

Step6:

M<= CNN based quantum-leap (f_{train}, f_{test})

Score <=Evaluate (I, $l_{test,}$ M)

Step7:

Return score

The above algorithm is a CNN-based quantum leap classification. Quantum leap has been high-level filtering data collection. Here step1 d is the input dataset, and W is the actual label of the dataset. Step 2 is the quantum leap model applied here. Step 3 W is feature selection; step 4 is processing for training and testing. Finally, evaluate the score for classification output.

IV. Result And Discussion

The proposed system is compared to various learning algorithms; GANs, RNNs, LSTMs, CNNs to compare but CNN based quantum-leap classification is best accuracy for jamming attack detection.

Table. I Simulation Parameters of the Proposed Method

Parameters	Value
OS	Window 10 pro
Language	Python
Support tool	Anaconda
Dataset	WSN-DS
Total Records	374,661
Feature `	23
From	Kaggle repository

Table.1 displays that the simulation parameters outperform one of the measured analogue conditions, in which the proposed method's various parameters evaluate their performance.

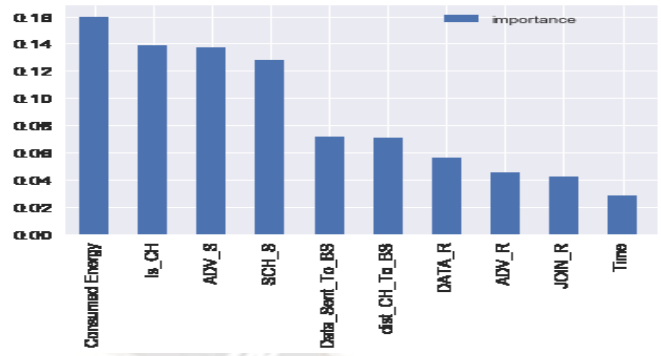

Figure.4 WSN-DS feature datasets

Table II show the classification accuracy obtained for each stage

Method used	Accuracy
GANs	88%
RNNs	89%
LSTMs	92%
CNNs	93%
CNN based quantum-leap	95.3%

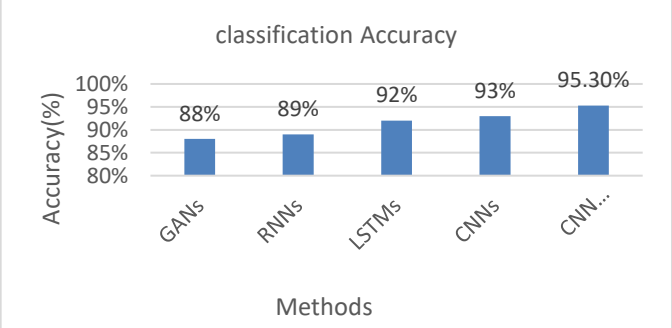

Figure.5 classification accuracy

Figure.5 define the classification accuracy performance compared with various algorithm GANs is 88% of accuracy, RNNs is 89% of accuracy, LSTMs is 92%, and proposed is 95.30% of accuracy. To evaluate the proposed approach, compared our multistage model with another work that used just applied to the same dataset to confirm that our approach is the most appropriate. Table III illustrates that our model can provide better accuracy of attacks classification than just the CNN- based quantum-leapmodel.

Table III Accuracy of jamming attacks.

Model	Accuracy of attacks classification (%)					Accuracy
	Random.	Const.	React.	Decept.	Norm.	
Chi-Squared	92.8	75.2	99.4	92.2	99.8	92.1
CNN based quantum-leap	93.5	78.5	99.5	93.2	99.9	95.4

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6534
***Article Received**: 25 January 2023 **Revised**: 21 February 2023 **Accepted**: 08 March 2023*

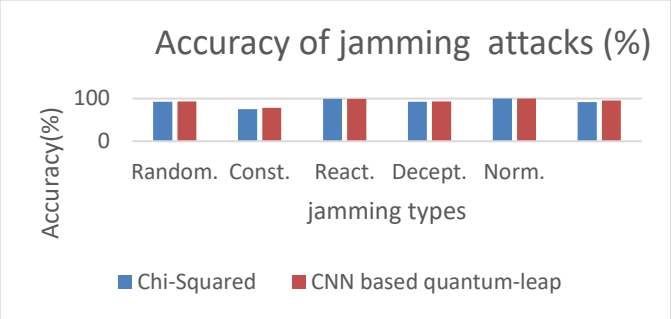

Figure.6 Accuracy of jamming attacks (%)

Figure.6 define the jamming attack accuracy performance compared with various attack types random is 92.8 % of accuracy, Constant is 99.4% of accuracy, Deceptive is 92.2%, and CNNs is 93% of accuracy; all the algorithms compared to the best result for CNN-based quantum leap is 95.3% of accuracy.

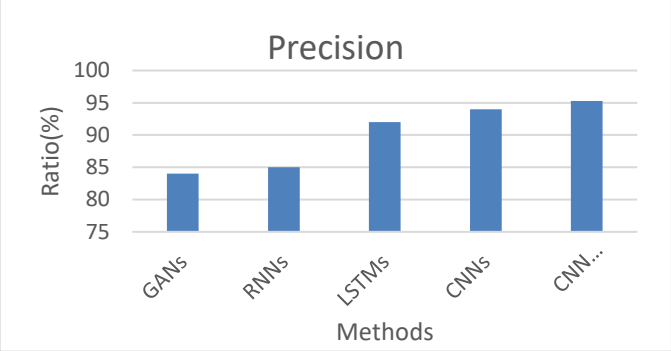

Figure.7 Precision

Figure.7 defines the Precision accuracy performance compared with various algorithms GANs is 84% of accuracy, RNNs is 85% of accuracy, LSTMs have 92% accuracy, CNN is 95.30% and proposed 96% accuracy.

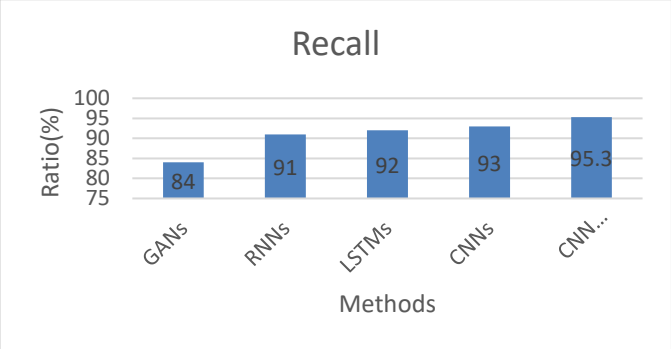

Figure.8 Recall

Figure.8 defines the Recall accuracy performance compared with various algorithms GANs is 84% of accuracy, RNNs is 91% of accuracy, LSTMs have 92% accuracy, and CNN is 93% and proposed 95% accuracy.

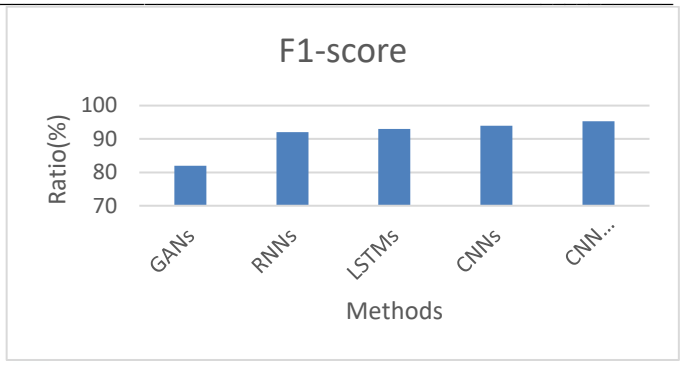

Figure.9 F-score

Figure.9 defines the Recall accuracy performance compared with various algorithms GANs is 82% of accuracy, RNNs is 92% of accuracy, LSTMs have 93% accuracy, and CNN is 94% and proposed 97% accuracy.

Likewise, a CNN based Quantum-Leap classifier is utilized to picture the presentation of the classifiers. It gives a compromise between the true positive rate (TPR) and the false positive rate (FPR) at various grouping edges. As displayed in the situations above, TPR is the extent of perceptions accurately anticipated as certain, be that as it may, FPR is the extent of perceptions erroneously anticipated as sure.

$$TPR = \frac{TP}{TP + FN}$$

$$FPR = \frac{TP}{TN + FP}$$

As displayed in the situations over, the TPR is the extent of perceptions that are accurately anticipated as certain. Notwithstanding, FPR is the extent of perceptions that are falsely predicted as positive

V. Conclusion

The wireless application needs faster communication and less interruption, the main problem of jamming attacks on wireless networks is that jamming attack detection using various machine learning methods has been used. The reasons for jamming detection may be user behaviour-based and network traffic and energy consumption. The previous machine learning system could not present the jamming attack detection accuracy because the feature selection model of Chi-Squared didn't perform well for jamming attack detections which determined takes a large dataset to be classified to find the high accuracy for jamming attack detection. To tackle this issue, propose a CCNN-based quantum leap method with high precision for clog assault discoveries. The proposed arrangement ensures high recognition and characterization accuracies that can reach up to 95.4%.

Reference

[1]. Y. Li et al., "Jamming Detection and Classification in OFDM-Based UAVs via Feature- and Spectrogram-Tailored Machine

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6534
Article Received: 25 January 2023 Revised: 21 February 2023 Accepted: 08 March 2023

Learning," in IEEE Access, vol. 10, pp. 16859-16870, 2022, doi: 10.1109/ACCESS.2022.3150020.

[2]. S. Kumar, K. Singh, S. Kumar, O. Kaiwartya, Y. Cao and H. Zhou, "Delimitated Anti Jammer Scheme for Internet of Vehicle: Machine Learning Based Security Approach," in IEEE Access, vol. 7, pp. 113311-113323, 2019, doi: 10.1109/ACCESS.2019.2934632.

[3]. B. Upadhyaya, S. Sun and B. Sikdar, "Multihypothesis Sequential Testing for Illegitimate Access and Collision-Based Attack Detection in Wireless IoT Networks," in IEEE Internet of Things Journal, vol. 8, no. 14, pp. 11705-11716, 15 July15, 2021, doi: 10.1109/JIOT.2021.3059880.

[4]. M. Furdek, C. Natalino, F. Lipp, D. Hock, A. D. Giglio and M. Schiano, "Machine Learning for Optical Network Security Monitoring: A Practical Perspective," in Journal of Lightwave Technology, vol. 38, no. 11, pp. 2860-2871, 1 June1, 2020, doi: 10.1109/JLT.2020.2987032.

[5]. L. Zhang, F. Restuccia, T. Melodia and S. M. Pudlewski, "Taming Cross-Layer Attacks in Wireless Networks: A Bayesian Learning Approach," in IEEE Transactions on Mobile Computing, vol. 18, no. 7, pp. 1688-1702, 1 July 2019, doi: 10.1109/TMC.2018.2864155.

[6]. G. Kornaros, "Hardware-Assisted Machine Learning in Resource-Constrained IoT Environments for Security: Review and Future Prospective," in IEEE Access, vol. 10, pp. 58603-58622, 2022, doi: 10.1109/ACCESS.2022.3179047.

[7]. Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250-1258, Oct. 2017, doi: 10.1109/JIOT.2017.2694844.

[8]. S. Liu, Y. Chen, W. Trappe and L. J. Greenstein, "ALDO: An Anomaly Detection Framework for Dynamic Spectrum Access Networks," IEEE INFOCOM 2009, Rio de Janeiro, Brazil, 2009, pp. 675-683, doi: 10.1109/INFCOM.2009.5061975.

[9]. C. Chen, H. Cheng and Y. -D. Yao, "Cooperative Spectrum Sensing in Cognitive Radio Networks in the Presence of the Primary User Emulation Attack," in IEEE Transactions on Wireless Communications, vol. 10, no. 7, pp. 2135-2141, July 2011, doi: 10.1109/TWC.2011.041311.100626.

[10]. F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines and J. Coble, "Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data," in IEEE Transactions on Industrial Informatics, vol. 15, no. 7, pp. 4362-4369, July 2019, doi: 10.1109/TII.2019.2891261.

[11]. L. Zhang, G. Ding, Q. Wu and Z. Han, "Spectrum Sensing Under Spectrum Misuse Behaviors: A Multi-Hypothesis Test Perspective," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 4, pp. 993-1007, April 2018, doi: 10.1109/TIFS.2017.2774770.

[12]. G. Fragkiadakis, E. Z. Tragos and I. G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks," in IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 428-445, First Quarter 2013, doi: 10.1109/SURV.2011.122211.00162.

[13]. Z. Yuan, D. Niyato, H. Li, J. B. Song and Z. Han, "Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks," in IEEE Journal on Selected Areas in Communications, vol. 30, no. 10, pp. 1850-1860, November 2012, doi: 10.1109/JSAC.2012.121102

[14]. C. Sumathi, R. Vidhyapriya and C. Kiruthika, "A proactive elimination of Primary User Emulation Attack in cognitive radio networks using Intense Explore algorithm," 2015 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2015, pp. 1-7, doi: 10.1109/ICCCI.2015.7218110.

[15]. P. K. Niranjane, V. M. Wadhai, S. H. Rajput and J. B. Helonde, "Performance analysis of PUE attacker on Dynamic Spectrum access in cognitive radio," 2015 International Conference on Pervasive Computing (ICPC), Pune, India, 2015, pp. 1-6, doi: 10.1109/PERVASIVE.2015.7086985.

[16]. J. Yang, Y. Chen, W. Shi, X. Dong and T. Peng, "Cooperative spectrum sensing against attacks in cognitive radio networks," 2014 IEEE International Conference on Information and Automation (ICIA), Hailar, China, 2014, pp. 71-75, doi: 10.1109/ICInfA.2014.6932628.

[17]. Ö. Cepheli and G. Karabulut Kurt, "Physical layer security in cognitive radio networks: A beamforming approach," 2013 First International Black Sea Conference on Communications and Networking (BlackSeaCom), Batumi, Georgia, 2013, pp. 233-237, doi: 10.1109/BlackSeaCom.2013.6623415.

[18]. A Alahmadi, M. Abdelhakim, J. Ren and T. Li, "Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 5, pp. 772-781, May 2014, doi: 10.1109/TIFS.2014.2310355.

[19]. M. Thanu, "Detection of primary user emulation attacks in Cognitive Radio networks," 2012 International Conference on Collaboration Technologies and Systems (CTS), Denver, CO, USA, 2012, pp. 605-608, doi: 10.1109/CTS.2012.6261113.

[20]. G. Fragkiadakis, E. Z. Tragos and I. G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks," in IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 428-445, First Quarter 2013, doi: 10.1109/SURV.2011.122211.00162.

[21]. Gopalakrishnan Subburayalu, Hemanand Duraivelu, Arun Prasath Raveendran, Rajesh Arunachalam, Deepika Kongara & Chitra Thangavel (2021) Cluster Based Malicious Node Detection System for Mobile Ad-Hoc Network Using ANFIS Classifier, Journal of Applied Security Research, DOI: 10.1080/19361610.2021.2002118.

[22]. Gopalakrishnan, S. and Kumar, P. (2016) Performance Analysis of Malicious Node Detection and Elimination Using Clustering Approach on MANET. Circuits and Systems, 7, 748-758. doi: 10.4236/cs.2016.76064.

[23]. D. Hemanand, G. . Reddy, S. S. . Babu, K. R. . Balmuri, T. Chitra, and S. Gopalakrishnan, “An Intelligent Intrusion Detection and Classification System using CSGO-LSVM Model for Wireless Sensor Networks (WSNs)”, Int J Intell Syst Appl Eng, vol. 10, no. 3, pp. 285–293, Oct. 2022.