Cognitive Radio Jamming Attack Detection Using an Autoencoder for CRIoT Network

Nallarasan v (nallarav@srmist.edu.in)
SRM Research Institute Kattankulathur
Kottilingam Kottursamy
SRM Institute of Science and Technology

Research Article

Keywords: Cognitive Radio Internet of Things, various attacks, architecture-based jamming attack

Posted Date: April 7th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-355056/v1

Version of Record: A version of this preprint was published at Wireless Personal Communications on August 15th, 2021. See the published version at https://doi.org/10.1007/s11277-021-08786-5.

Cognitive Radio Jamming Attack Detection Using an Autoencoder for CRIoT Network

V.Nallarasan[1], Kottilingam Kottursamy[2]
Research Scholar[1],Associate Professor[2]
Department of Computer Science and Engineering[1]
Department of Information Technology[2]
SRM institute of science and Technology, Chengalpattu ,[1,2]

nallarav@srmist.edu.in[1],kottilik@srmist.edu.in[2]

Abstract

IoT network-connected devices will be kept on increasing and will cross million, but it is impossible to allocate spectrum for those million and million of the devices. This spectrum scarcity can be handled by incorporating cognitive radio-based dynamic spectrum sharing, which is referred to as Cognitive Radio Internet of Things (CRIoT). But CRIoT sufferers from the Physical layer attack in cognitive radio, which affects the spectrum sensing accuracy and reduces the spectrum utilization. There are various attacks at the physical layer of cognitive radio among jamming attacks resulting in a denial of cognitive radio services and make spectrum underutilization. Continuous jamming can be detected quickly based on time delay on spectrum access, but discrete random jamming detection is challenging. This article proposes an autoencoder deep learning architecture-based jamming attack detection in cognitive radio. The jamming detection problem is modeled as anomaly detection. The autoencoder architecture is used to detect the jammer anomaly of the jammer. The proposed system involves the simulation of a random jamming attack and detecting it at a particular time instant information that may help mitigate the jammer attack .the proposed mechanism able to detect the jammer with 89% of accuracy.

Keywords: Cognitive Radio Internet of Things, various attacks, architecture-based jamming attack.

1.Introduction

internet of things is ever-growing with an increased number of connected devices in the order of millions and millions of devices. In the future, it will not be possible to allocate the spectrum for those connected devices because most of the spectrum is allocated for the other wireless services. Even though there is a new spectrum band proposed for the scarcity issue like millimeter-wave spectrum and Tera Herz spectrum, they are still at laboratory and simulation level only. There is a lot of deployment issue need to be addressed in those new spectral band. Moreover, those new spectral band hardware costs will be very high, making it possible to accommodate IoT applications. The only feasible solution for this issue will be applying the cognitive radio concept in the IoT network for dynamic spectrum sharing. Cooperative cognitive is mostly suitable [14] for IoT applications since, by default, all IoT nodes are engaged with sensing jobs already. It also provides energy efficiency [16].

There are many kinds of literature that explored the spectrum sharing mechanism for IoT . There are many couples of works in the direction of resource management [17].But the security aspect of the cognitive radio for spectrum sharing in IoT applications is not explored much .There are many physical layers attack in the cognitive radio that disables the dynamic spectrum

sharing [19-23]like Primary user emulation attack, data falsification jamming attack. Among those attacks, jamming attacks are very simple to make, which could be a prominent one in the IoT application with cognitive radio. The jamming attack with continuous jamming is easier to detect. But the intelligent jammer will randomize the jamming attack, which is very difficult to detect. Thus this research article is intended to solve such kind of ransom jamming attack. The detection of such jamming attacks is the first step to mitigate that attack. Under a random attack scenario detecting the attack time instant will be very much essential to alleviate the attack. So, this research article intended to detect the attack with the exact time instant of the attack.

Few kinds of literature deal with CR in IoT and jamming attack detection.

The limited availability of spectrum and inefficient usage of range opens a concept called cognitive Radio Networks (CRN)"[13], which can be effectively utilized for the IoT network. Routing algorithms for Cognitive Radio Based IoT network analyzed with channel switching cost, end-to-end delay cost, energy efficiency and bandwidth dependent cost[13].

An integrated cognitive radio (CR) with the IoT called CR-IoTNet is introduced [1]. In the proposed CR-IoTNet, given with multiple primary user (PU) base-stations and SU devices and joint spectrum sensing and optimal allocation of spectrum is proposed. In this, an intelligent fusion centre (IFC) is utilized for signal spectrum sensing decisions. Support vector machines (SVM) is employed to learn and adapt to network dynamics and identify the PU spectrum usage. Trained SVM classifier provides 95.11% accuracy.

The jamming attack is one of the leading security issues for spectrum sharing in cognitive radio, especially in an IoT network. CR networks security issue of proactive jamming and reactive jamming in spectrum sharing is addressed [2]. The channel assignment process in presence of both proactive and reactive jamming attacks is carried out with a probabilistic-based channel assignment mechanism. The proposed mechanism tries to minimize the invalidity ratio of CR packet transmissions with a delay constraint. The statistical information of primary users' activities, fading conditions and jamming attacks over idle channels are used as base data to achieve the lowest invalidity ratios with a quality-aware channel assignment algorithm.

Machine learning and deep learning applied Cognitive IoT network provides much promising solution because it establishes mathematical models using observations, i.e., training data then the model can be used, to predict or make decisions[15,24,25]. Those approaches enable learning and improvement from experience automatically.

Another jamming attack work for the cognitive radio network with an anti-jamming task with the help of a Markov decision process and deep reinforcement learning method is proposed [3]. The mechanism used to learn a policy to maximize the rate of successful transmission. A Double Deep Q Network (Double DQN) model us used to detect the jammer. The Q network is trained using the Transformer encoder to estimate action-values pair from raw spectrum data.

Channel hopping is one of the schemes for anti-jamming in cognitive radio, which requires pre-sharing of access information and not taking care of the traffic loads' variations. An anti-jamming scheme with the dynamic adjustment of the sending/receiving ratio to maximize the throughput is proposed [4]. The mechanism work based on Load Awareness with Anti- channel hopping for anti-jamming, which uses extended Langford pairing.

The coexistence of IoT and CRN makes it possible to deploy a broad range of solutions. The time-sensitive IoT applications suffer from communication security, especially when CR concepts are utilized in IoT, prone to more attacks. A security-aware routing protocol with jamming attacks is presented[5]. This mechanism assigns the most secure channel for every hop of communication by solving an optimization problem. An Ensemble-based Jamming Behaviour Detection and Identification (E-JBDI) technique is also presented to identify the behavior anomaly of jamming attack. Results also show the proposed mechanism achieves accuracy and precision-recall rates of approximately 100%.

An active anti-jamming method based on frequency diverse array (FDA) radar phase center is presented[6]. This cognitive activity ensures the radar difficult for a jammer to detect or locate during the normal operation. The Bayesian filter is applied to realize cognitive beamforming to make anti-jamming.

The security issues over the physical layer of cognitive radio are summarized [7]. The various threat types, detection mechanisms, and countermeasures are reported.

The jamming issue in Cognitive radio (CR) WiFi network with dynamic channel switching is presented [8]. This integration is called a Cognitive WiFi (CWF) network. A new LU-MAC protocol is proposed for CWF network, which can work dynamically in licensed and unlicensed bands to increase jamming resistance. The protocol has a new control frame, Data Channel Switching (DCS) process and coordination modules, control channel switching process. Few algorithms are analyzed for the antijamming, namely 1. Intrusion Detection System (IDS), 2.Random Frequency Hopping Pattern (RFHP) 3.Statistic-based Reactive Channel Switching (SRCS).

In cognitive radio, any malicious user can observe communication and emits a false message to block communication due to shared frequency. Software-defined radio (SDR) technology makes jamming attacks very easy since the waveforms are defined in software. A jammer transmits radio signal diable communication reducing signal to noise ratio. Different jammer detection methods are analyzed [9]. Few network parameters are used to detect the jamming attack that can be 1. packet delivery ratio (PDR)2. packet send ratio (PSR)3.bad packet ratio (BPR) 4.signal to noise ratio (SNR). The communication parameter used in SDR like 1.synchronization indicator, 2.iteration 3.adaptive signal to jammer plus noise ratio (ASNJR) are the new detectings the detection of the jamming attack for the software-defined radio hardware.

The Internet of Medical Things (IoMT) is the innovation that enables e-healthcare to make treatments more flexible and convenient. But security and privacy become the central issue of IoMT which is challenging to have highly computational cryptographic to solve because of the following characteristic of the IoMT devices 1. limited computational capability2. Limited memory space 3.has energy constraints. A friendly jamming (Fri-jam) scheme is proposed for potential countermeasures to the security of IoMT[10]. This Fri-jam protects the confidential medical data collected by medical sensors from eavesdropping. It is also possible to integrate Fri-jam schemes communication technologies like 1. Beamforming2.Simultaneous Wireless Information and Power Transfer (SWIPT) 3.full duplexity.

A rational attacker made for a specific transmission characteristics waveform has the highest impact on cognitive radio. The software-defined radio platform makes it possible to generate

such a target attack. A honeynet-based defense for jamming is presented [11]. The honeynet learns the attacker's strategy and adapts the preemptive process. It s proved that the proposed mechanism makes CRN successfully avoids jamming attacks and improves the packet delivery ratio.

The primary user emulation (PUE) attack is another type of attack in cognitive radio which diable accessing idle frequency spectrums. An adaptive Bayesian learning automaton algorithm (Multichannel Bayesian Learning Automata (MBLA)) is proposed to defend PUE[12]. The algorithm MBLA learning in non-stationary environments and selecting the optimal frequency channel. An uncoordinated frequency hopping (UFH) is utilized for sending data on different channels.

Vehicular ad-hoc networks (VANET) deployed with safety-critical applications to be protected from jamming attacks. A jamming detection approach for wireless vehicular networks using unsupervised machine learning is presented[12]. The variations of the relative speed between the jammer and the receiver are used as a parameter for detecting the jamming attack. The mechanism can differentiate intentional and unintentional jamming with their unique characteristics.

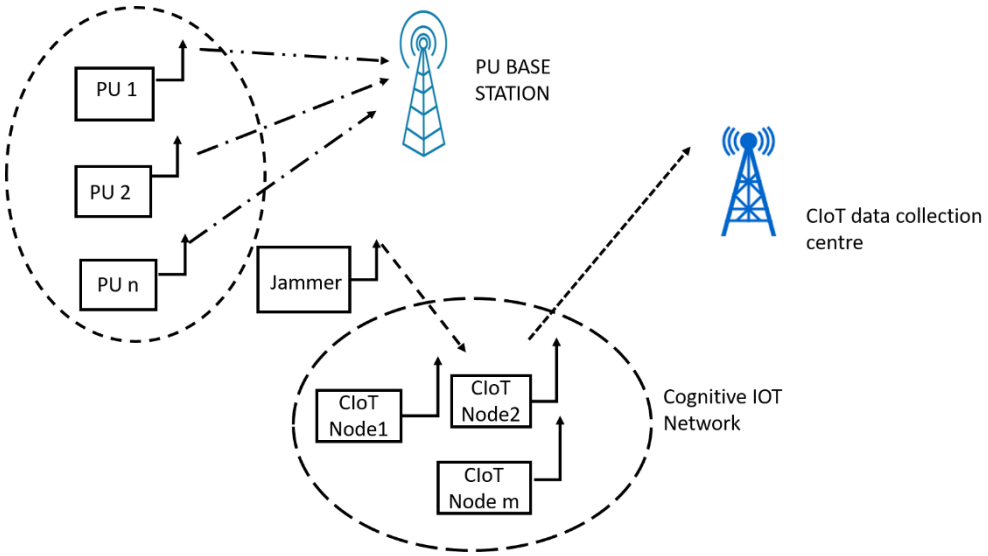
Jammer localization finding essential one because it helps for jamming-avoidance routing. It is easy to detect location in the presence of usage of omnidirectional antennas. It is challenging for directional jammers to use directional antennas. An Adaptive Jammer Localization Algorithm (AJLA) method which estimates the jammer’s antenna type and selects the appropriate algorithm based on the type of antenna is presented [26]. Centroid Localization (CL), Virtual Force Iteration Localization (VFIL) algorithms are used for omnidirectional antennas. An Improved Gravitational Search Algorithm (IGSA) is used for a directional antenna.

Reactive jamming is most challenging to detect. Jammer detection and localization in a WiFi network are presented[28]. The mechanism uses the fact that the jammer increases the interference range and keeps the access point busy with more time.

2.System Model

The system model used for the simulation of the proposed method is given in figure 1. The system model in figure one consists of a primary user network of cellular communication with licensed spectrum access. It is assumed that there is n number of primary users in the primary user network. The secondary network called cognitive radio IoT network has m number of nodes that sense data from the environment and communicate to the data collection center. This CRIoT network uses dynamic spectrum access using cognitive radio, which enables to share the primary user spectrum which the primary user does not use. It is assumed that there is a spectrum sensing algorithm running on each CRIoT node that can detect the spectrum hole by using an energy detector. Since the energy detector is a low complex algorithm for the spectrum sensing, which is utilized in the CRIoT because those nodes are low cost and less computational capable. There is a jammer in the close vicinity of the CRIoT network that will be injecting random jamming signal to the CRIoT nodes in the same frequency set of the primary network with the aim to disable the CRIoT node not to utilize the spectrum hole point spectrums properly. Since the energy detector algorithm detects the spectrum hole through the received signal energy on a particular frequency and the jamming signal injects a high energy signal in

the primary user frequency, the CRIoT node will wrongly interpret the jammer signal as the direct signal. It will not use the primary user frequency even though they are free without utilizing at the given instant of the time. It is also assumed that the jammer signal impact on the primary user network is minimum since it is away from the jammer and the transmit power of those nodes is higher than the jammer signal.



–

Figure 1. system model of CIoT network with jamming attack

The received signal at cognitive radio when primary alone user present

$$y_{cp} = h_p x_p + n \quad (1)$$

Where h_p is the channel coefficient between the primary user and cognitive radio, x_p is the primary user transmit symbol, n is the additive white gaussian noise.

The received signal at cognitive radio when no primary user and jammer present

$$y_{cp} = n \quad (2)$$

The received signal at cognitive radio when primary user and jammer present

$$y_{cp} = h_p x_p + h_J x_J + n \quad (3)$$

Where h_J is the channel coefficient between the cognitive radio and jammer, x_J is the jammer transmit symbol, n is the additive white gaussian noise.
The received signal power of the primary user at cognitive radio is

$$P_{PRX} = \frac{P_P G_P c^2 G_c}{4\pi^2 f^2 R_{pc}^2} \quad (4)$$

The received signal power of the jammer at cognitive radio is

$$P_{JRX} = \frac{P_J G_J c^2 G_c}{4\pi^2 f^2 R_{Jc}^2} \quad (5)$$

The impact of the jamming effect is based on the jamming to signal power ratio

$$JSPR = \frac{P_J G_J R_{pc}^2}{P_P G_P R_{jc}^2} \quad (6)$$

Where P_J and P_P are the transmit power of the jammer and primary user, respectively. G_J , G_P are the antenna gain of jammer and primary user R_{pc} and R_{jc} are the range or distance between the primary user and cognitive radio, the distance between the jammer and cognitive radio.
If the $JSPR$ is more significant than one, it has an impact on the primary user detection .whenever $P_{JRX} \geq$ threshold , then the jammer signal will be treated as the primary user signal, then the primary user frequency occupied decision will be made wrongly. this wrong detection makes the cognitive user not use the primary user spectrum hole and reduces the spectrum utilization

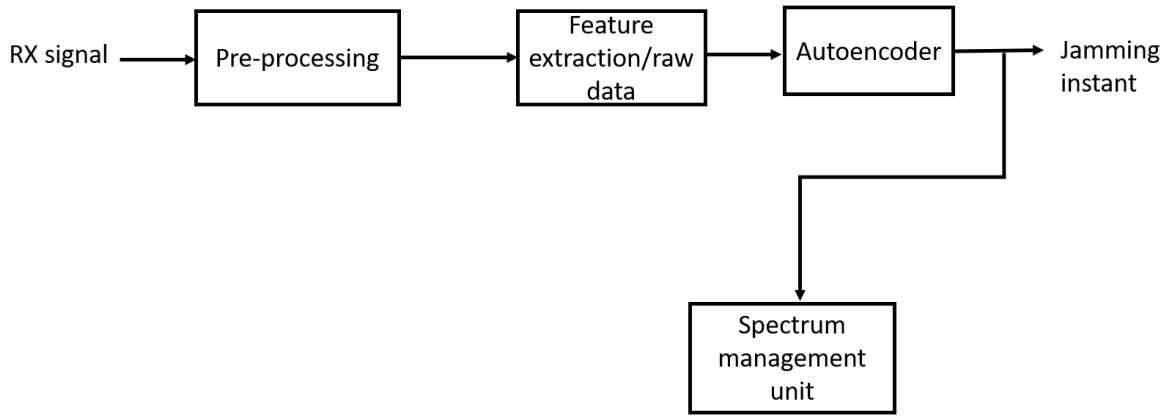


Figure 2. Block diagram of jammer detection using an autoencoder

Figure 2 shows the mechanism of the jammer detection. The data obtained from the receiver is pre-processed by shaping the data in the 2D form, splitting the data into training a test set, windowing to have 256 samples at a time for the training. The formatted data can be applied as raw data and as well as feature extraction. The Fourier transform is applied to the raw data then the amplitude-frequency spectrum is taken as a feature set used for training the autoencoder. Autoencoder is configured as an anomaly detector to find the jamming attack.

Table 1. Autoencoder architecture configuration

Layer	Filters	Kernel size	padding	strides	Activation
Input layers - Conv1D	32	7	same	2	relu
Dropout(rate=0.2)					
Conv1D	16	7	same	2	relu
Conv1DTranspose	16	7	same	2	Relu
Dropout(rate=0.2)					
Conv1DTranspose	32	7	Same	2	Relu
Conv1DTranspose	1	7	Same	2	Relu

Table 1 shows the autoencoder architecture with the layer information. it can be observed that the encoder part has one 1D convolutional layer with 32 filters with a kernel size of 7, padding mechanism of the same and strides size 2 with activation function of relu. Followed by a drop-

out layer is provided with drop-out rate of 0.2. a second layer, another convolution layer, is provided with 16 filters with a kernel size of 7, padding mechanism of same, and strides size 2 with activation function of relu. Then the decoder section, the first layer, has the weight value of the transposed of the last encoder layer with the same configuration of the last layer in the encoder section, i.e., with 16 filter with kernel size 7, padding mechanism of same and strides size 2 with activation function of relu. Then a dropout layer is used with the rate of drop out 0.2. the second layer in the decoding section has a transpose weight value of the first layer of the encoder with the same configuration parameter of it i.e., 1D convolutional layer with 32 filters with a kernel size of 7, padding mechanism of same and strides size 2 with activation function of relu. The decoder's last layer has only one filter with kernel size 7, padding mechanism of same and strides size 2 with activation function of relu.

The algorithm of jammer detection using autoencoder is given below

Autoencoder anomaly detection based jammer detection for cognitive radio

Training phase :

Step1: configure the primary user to generate x_p QPSK signal at ransom instant of time on frequency f and propagate signal on the channel h_p with the transmit power of P_P

Step2: Receive the signal at cognitive radio y_{cp}

$$y_{cp} = h_p x_p + n$$

Step3: Split the data as training, validation and test set

Step4: apply a windowing technique of rectangular window to generate 256 samples at a time to feed and train the autoencoder

Step5:for training sample window=1 to M

propagate training samples and train the autoencoder to reproduce the exact same input signal and record the range of mean absolute difference values by computing as

a)compute encoder output $o_{en} = y_{cp} W^T$

b) compute decoder output $Y_{Pdec} = o_{en} V^T$

c)calculate mean absolute error $MAE_{train} = \frac{1}{M} \sum_{win=1}^{M} \left| Y_{Pdec} - y_{cp} \right|$

jammer detection phase :

Step1: configure the jammer to generate a Phased Barrage Jammer signal x_J at ransom instant of time on frequency f and propagate signal on the channel h_J

Step2: Receive the signal at cognitive radio y_{cp}

$$y_{cp} = h_p x_p + h_J x_J + n$$

Step 3: apply a windowing technique of rectangular window to generate 256 samples at a time to feed the autoencoder

Step 4: compute mean absolute difference values as

a)compute encoder output $o_{enj} = y_{cp} W^T$

b) compute decoder output $Y_{Pjdec} = o_{enj} V^T$

c)calculate mean absolute error $MAE_{test} = \frac{1}{M} \sum_{win=1}^{M} \left| Y_{Pjdec} - y_{cp} \right|$

Step 5:for i= 1 to M

a)compute the MAE difference between the training values MAE_{train} and MAE_{test}

$$jam_{score}(i) = |MAE_{train}(i) - MAE_{test}(i)|$$

b)if $jam_{score}(i) > jamtheshold$ then jammer signal presents at the ith instant of the window; else no jamming signal at ith moment of window

3.Result and discussion

the entire proposed system is simulated in MATLAB and python. The MATLAB software is used for signal generation.i.e. data generation with PU, Jammer and cognitive radio. then the generated data is used for the jammer detection by using an autoencoder as a anomality detector.

Table 2 The simulation parameter for data generation

Si.no	Parameter	Value
1	Number of PU node	1
2.	Number of CR node	1
3.	Number of jammer node	1
4.	Jammer type	Phased Barrage Jammer
5.	Phased Barrage Jammer parameters	ERP =10,SamplesPerFrame=400
6	PU signal parameters	QPSK modulation, ERP =10
7	Transmit filter for PU	Raised Cosine Transmit Filter, Roll off Factor =0.3, Output Samples Per Symbol = 2

Table 2 shows the simulation set of parameters used for the data generation in MATLAB. The Phased Barrage Jammer is used with ERP =10 with 400 samples per frame generation. The simulation is repeated 10 times to realize 4000 samples of data. The PU signal is generated with QPSK modulation and ERP =10.the signal of PU is propagated through the transmit filter of Raised Cosine with Roll off Factor =0.3 and Output Samples Per Symbol = 2. This PU signal and jammer signal are combinedly received at CR receiver and stored in the autoencoder training file. The autoencoder with the layer information given in table 1 is trained using this data-generated file.

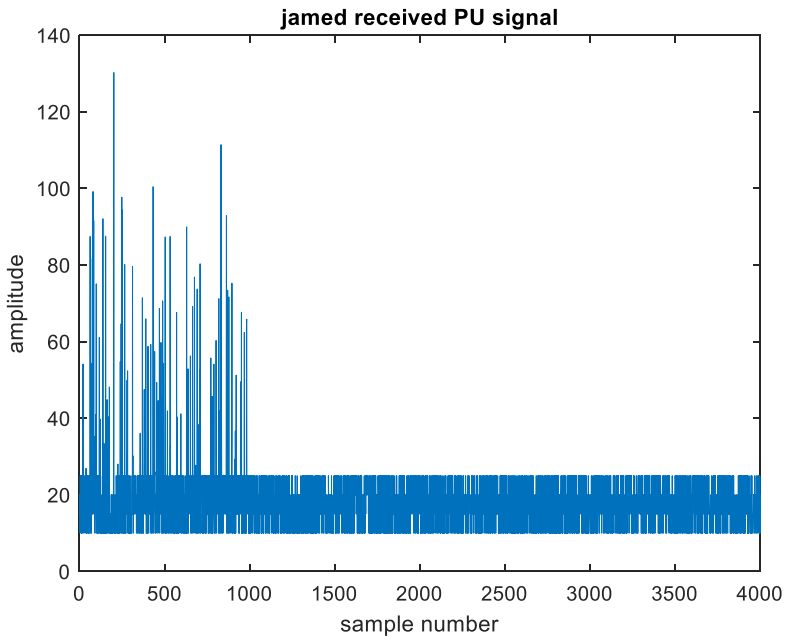


Figure 4. Cognitive radio received signal with jammer and PU signal components

Figure 4 shows the received signal at a cognitive radio node with PU signal components and jammer signal components. The signal level with amplitude within 20 is the PU components. The signal level with more than 20 up to 130 is the jammer component. From figure 4, it is also evident the jammer signal is added randomly with the PU signal.

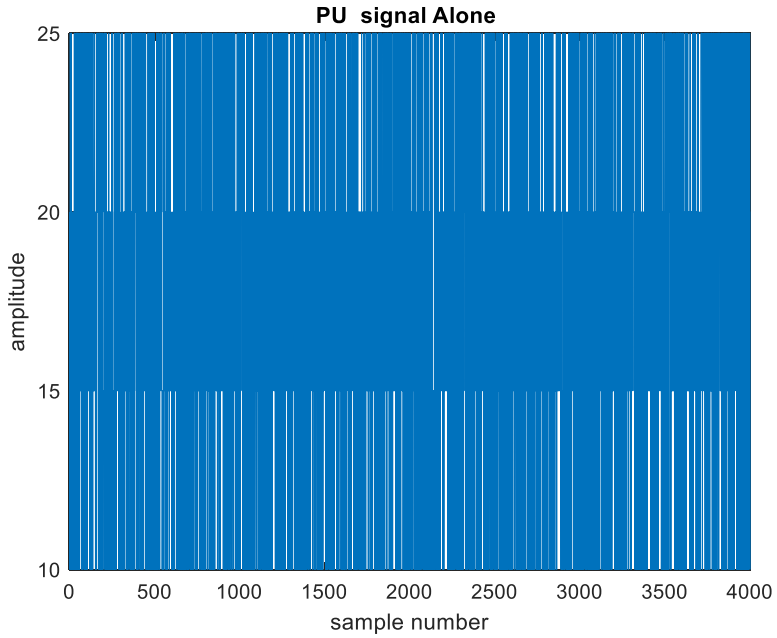


Figure 5.PU signal alone

Figure 5 shows the QPSK modulated PU signal.it takes an amplitude of 25 units as maximum amplitude. This signal is generated at random instant of time such that we can observe some spectrum hole .in the graph, the white line instants are the spectrum hole points.

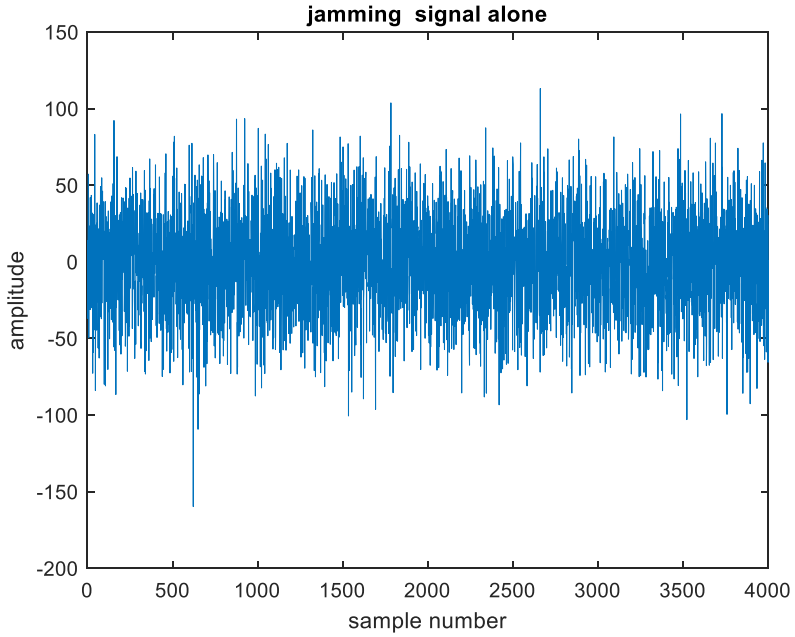


Figure 6 jammer signal alone

Figure 6 shows the jammer signal alone.it takes from -50 to +120. This jammer signal is also generated randomly such that the detection of the random attack is difficult. Moreover, the random time instant of the jammer injection is recorded for the comparison purpose after finding the autoencoder's jammer injection instant.

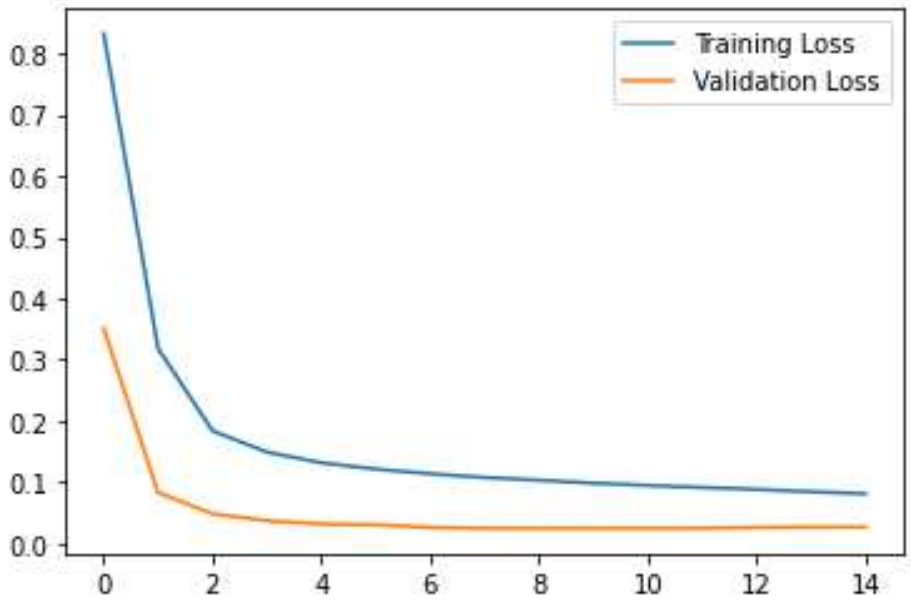


Figure 7. training and validation losses

Tracking the deep learning model's training and validation losses will give an idea of whether the model is overfitted or under fitted. Moreover, it also gives an idea of whether the furthermore training is required or more training data is required. Figure 7 gives the training and validation losses of the designed autoencoder. The figure shows that the model is not overfitting or underfit, but there is a scope of improving the accuracy by new data set or feature set.

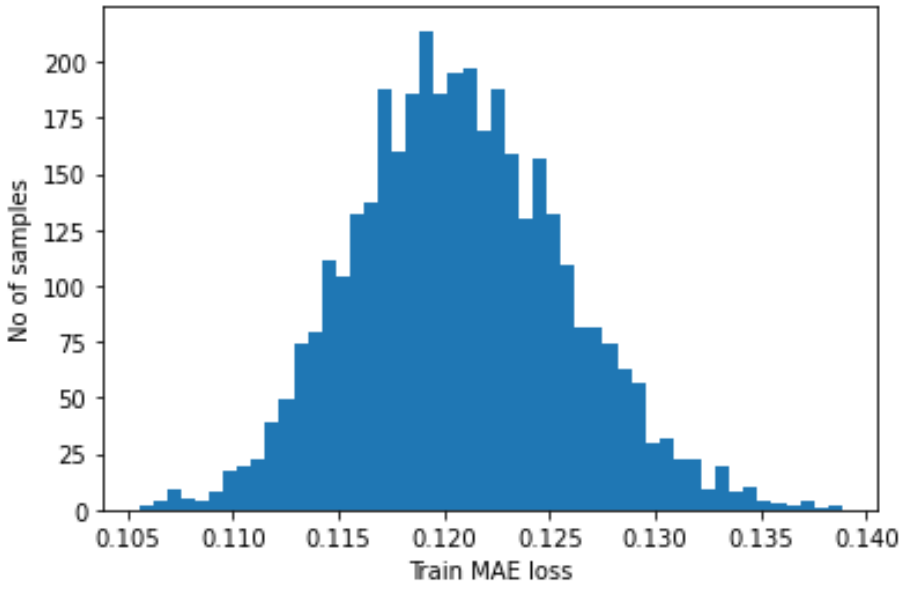


Figure 8. Histogram of the training mean absolute error

The mean absolute error is used as a loss function in the autoencoder and the model is trained to minimize this loss value. Figure 8 shows the histogram of the training time mean absolute error value. it is evident from the graph that the error is taken from 0.105 to 0.140. this small variation indicates that the data set does not have much variance to make more weight changes. It is also evident that the error value of around 0.118 is taken much of the time.

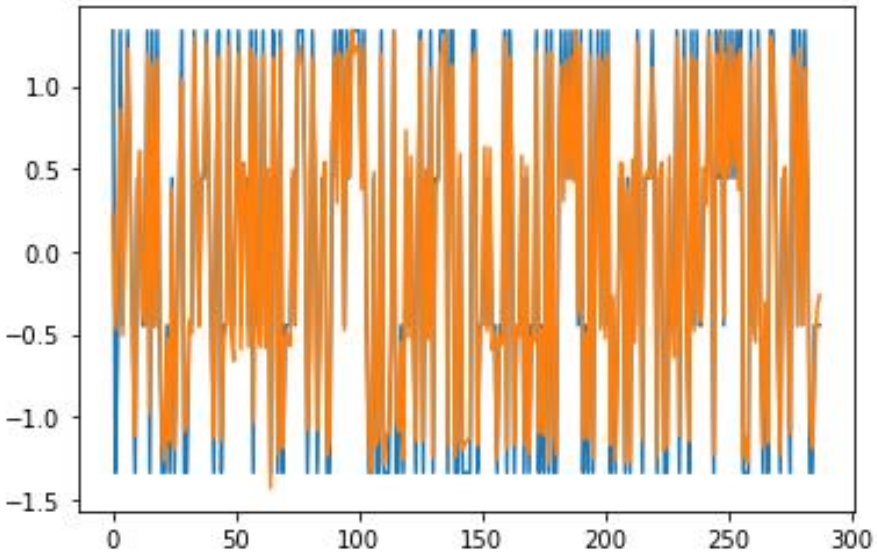


Figure 9. PU signal and decoded PU signal

The autoencoder is designed and trained to encode the PU signal in the encoder part and reprocess the PU signal exactly at the output of the decoder. In order to access the reproducing capability of the autoencoder after training the PU signal, the decoded PU signal and the original input PU signal which is used to train is plotted in a single graph as shown in figure 9. in figure 9 blue color signal indicate the input original PU signal which fed during the training phase and the orange colour signal is the reconstructed signal at the autoencoder output by taking the compressed component of the signal from the outcome of the encoder part.

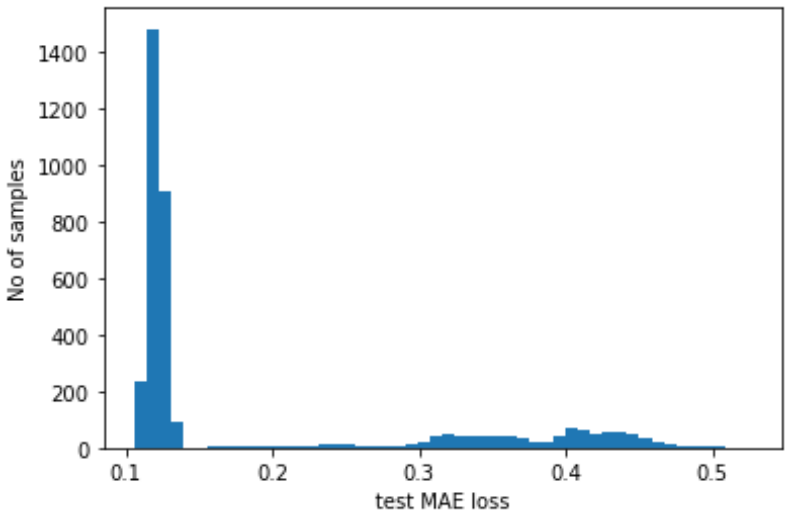


Figure 10. Test Mean Absolute error histogram

The error performance of the deep learning model for the test data set is required to access the model's generalization capability. Figure 10 shows the test error performance of the autoencoder. The figure shows that for the then-new unseen data set during the test phase, the model mostly provides around 0.13, i.e., 13% error.

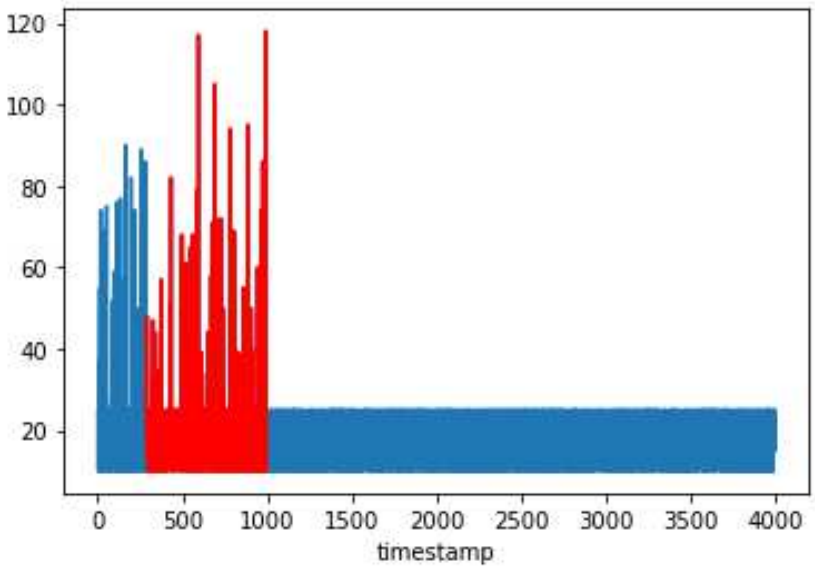


Figure 11. Detected jammer with time stamp information

Detecting the jammer signal's presence at the receiver of CR radio and the time when jammer enters into the system is essential. Under the proposed autoencoder, the detection of the jammer signal and the time instant on which it is detected is given. Figure 11 shows such detection of the jammer signal. The red color mark in the figure shows the jammer signal component detected by the autoencoder. The axis value shows the timestamp of the detected jammer component. From the figure, it is evident that the jammer signal component is detected after the sampling instant 256 onwards. It happens because the first window of size data 256 needs to be processed by the autoencoder, then only it can recognize that the samples are from the jammer .it is the limitation of the proposed mechanism.

In order to evaluate the performance of the proposed jamming dettction mechanism, the spectral efficiency of the CRIoT network node after jammer detection with various jamming timing is calculated and plotted in figure 12 against the spectral efficiency of the same node with a jammer. Figure 12 is drawn by considering the 10 seconds transmission time, and the performance is analyzed. Figure 12 proves that the proposed mechanism maintains spectral efficiency with negligible reduction comparing to that of jammer .around 2 bits/Hz/sec, spectral efficiency gain is achieved by the proposed jammer detection algorithm for the 5 seconds jamming time comparing to that of the spectral efficiency with a jammer.

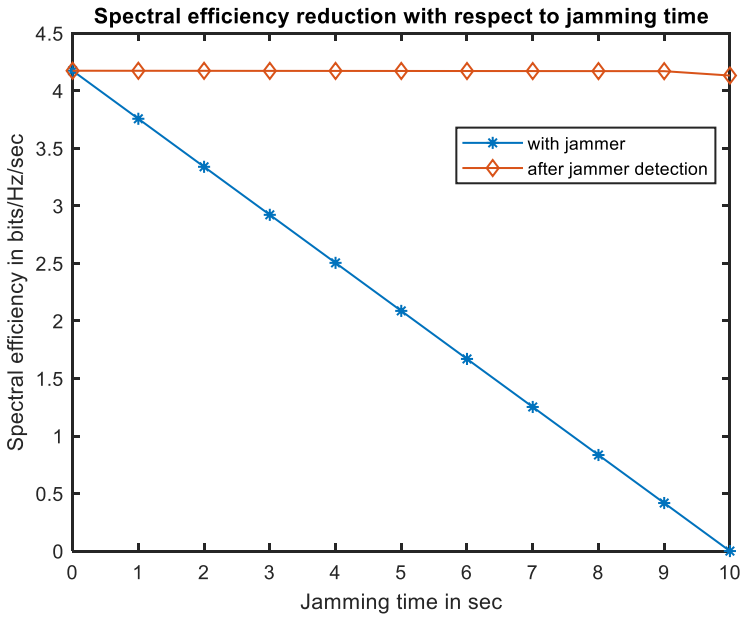


Figure 12.spectral efficiency with a jammer and after jammer detection

4.Conclusion

Jamming attack in cognitive IoT network diable the dynamic spectrum sharing .the detection of jamming attack predominantly random jamming is challenging to detect, which is solved by using autoencoder deep learning model. The autoencoder is configured as an anomaly detector, and the jamming attack is detected using that. The proposed mechanism able to detect the jammer with the time instant of jamming. The proposed mechanism has the limitation of detecting the jammer if the jammer's signal is strong enough compared to that of the primary user. This limitation will be addressed in future work, and the jammer mitigation strategy also will be addressed in future work.

Author declaration statement

No part of this manuscript is published in any other journal and this work is truly a combined work of all the authors.

Funding

This research received no external funding.

Conflicts of interest

The author declares no conflict of interest

Availability of data and material

NO

Code availability

software application only

Reference

1.Ahmed, Ramsha, Yueyun Chen, Bilal Hassan, and Liping Du. "CR-IoTNet: Machine learning based joint spectrum sensing and allocation for cognitive radio enabled IoT cellular networks." *Ad Hoc Networks* 112 (2021): 102390.

2. Salameh, Haythem A. Bany, Sufyan Almajali, Moussa Ayyash, and Hany Elgala. "Spectrum assignment in cognitive radio networks for internet-of-things delay-sensitive applications under jamming attacks." IEEE Internet of Things Journal 5, no. 3 (2018): 1904-1913.

3. Xu, Jianliang, Huaxun Lou, Weifeng Zhang, and Gaoli Sang. "An Intelligent Anti-Jamming Scheme for Cognitive Radio Based on Deep Reinforcement Learning." *IEEE Access* 8 (2020): 202563-202572.

4. Chao, Chih-Min, and Wei-Che Lee. "Load-aware anti-jamming channel hopping design for cognitive radio networks." *Computer Networks* 184 (2021): 107681.

5. Salameh, Haythem Bany, Safa Otoum, Moayad Aloqaily, Rawan Derbas, Ismaeel Al Ridhawi, and Yaser Jararweh. "Intelligent jamming-aware routing in multi-hop IoT-based opportunistic cognitive radio networks." *Ad Hoc Networks* 98 (2020): 102035.

6. Ge, Jiaang, Junwei Xie, and Bo Wang. "A cognitive active anti-jamming method based on frequency diverse array radar phase center." *Digital Signal Processing* 109 (2021): 102915.

7. Salahdine, Fatima, and Naima Kaabouch. "Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey." *Physical Communication* 39 (2020): 101001.

8. Karunambiga, K., and M. Sundarambal. "LU-MAC: licensed and unlicensed MAC protocol for cognitive WiFi network with jamming-resistant." *Procedia Computer Science* 47 (2015): 424-433.

9. Bhojani, Ronak, and Rutvij Joshi. "An integrated approach for jammer detection using software defined radio." *Procedia Computer Science* 79 (2016): 809-816.

10. Li, Xuran, Hong-Ning Dai, Qubeijian Wang, Muhammad Imran, Dengwang Li, and Muhammad Ali Imran. "Securing internet of medical things with friendly-jamming schemes." *Computer Communications* (2020).

11. Bhunia, Suman, Edward Miles, Shamik Sengupta, and Felisa Vázquez-Abad. "CR-Honeynet: A cognitive radio learning and decoy-based sustenance mechanism to avoid intelligent jammer." *IEEE Transactions on Cognitive Communications and Networking* 4, no. 3 (2018): 567-581.

12. Mahmoudi, Mohsen, Karim Faez, and Abdorasoul Ghasemi. "Defense against primary user emulation attackers based on adaptive Bayesian learning automata in cognitive radio networks." *Ad Hoc Networks* 102 (2020): 102147.

13. Arat, Ferhat, and Sercan Demirci. "Analysis of Spectrum Aware Routing Algorithms in CR Based IoT Devices." In *2019 4th International Conference on Computer Science and Engineering (UBMK)*, pp. 751-756. IEEE, 2019.

14. Moayedian, Naghmeh Sadat, Shirin Salehi, and Majid Khabbazian. "Fair Resource Allocation in Cooperative Cognitive Radio Iot Networks." *IEEE Access* 8 (2020): 191067-191079.

15. Awin, Faroq A., Yasser M. Alginahi, Esam Abdel-Raheem, and Kemal Tepe. "Technical issues on cognitive radio-based Internet of Things systems: A survey." *IEEE Access* 7 (2019): 97887-97908.

16. Ansere, James Adu, Guangjie Han, Hao Wang, Chang Choi, and Celimuge Wu. "A reliable energy efficient dynamic spectrum sensing for cognitive radio IoT networks." *IEEE Internet of Things Journal* 6, no. 4 (2019): 6748-6759.

17. Liu, Miao, Tiecheng Song, and Guan Gui. "Deep cognitive perspective: Resource allocation for NOMA-based heterogeneous IoT with imperfect SIC." *IEEE Internet of Things Journal* 6, no. 2 (2018): 2885-2894.

18. Alzahrani, Bander, and Waleed Ejaz. "Resource management for cognitive IoT systems with RF energy harvesting in smart cities." *IEEE Access* 6 (2018): 62717-62727.

19. Lin, Shih-Chang, Chih-Yu Wen, and William A. Sethares. "Two-tier device-based authentication protocol against PUEA attacks for IoT applications." *IEEE Transactions on Signal and Information Processing over Networks* 4, no. 1 (2017): 33-47.

20. Bhattacharjee, Shameek, Shamik Sengupta, and Mainak Chatterjee. "Vulnerabilities in cognitive radio networks: A survey." *Computer Communications* 36, no. 13 (2013): 1387-1398.

21. Haldorai, Anandakumar, and Arulmurugan Ramu. "Security and channel noise management in cognitive radio networks." *Computers & Electrical Engineering* 87 (2020): 106784.

22. Salahdine, Fatima, and Naima Kaabouch. "Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey." *Physical Communication* 39 (2020): 101001.

23. Ponnusamy, Vijayakumar, Kottilingam Kottursamy, T. Karthick, M. B. Mukeshkrishnan, D. Malathi, and Tariq Ahamed Ahanger. "Primary user emulation attack mitigation using neural network." *Computers & Electrical Engineering* 88 (2020): 106849.

24. Ponnusamy, Vijayakumar, and S. Malarvihi. "Hardware impairment detection and prewhitening on MIMO precoder for spectrum sharing." *Wireless Personal Communications* 96, no. 1 (2017): 1557-1576.

25. Vijayakumar, Ponnusamy, and S. Malarvihi. "Green spectrum sharing: Genetic algorithm based SDR implementation." Wireless Personal Communications 94, no. 4 (2017): 2303-2324.

26. Wang, Tongxiang, Xianglin Wei, Jianhua Fan, and Tao Liang. "Adaptive jammer localization in wireless networks." *Computer Networks* 141 (2018): 17-30.

27. Karagiannis, Dimitrios, and Antonios Argyriou. "Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning." *Vehicular Communications* 13 (2018): 56-63.

28. Cai, Yifeng, Konstantinos Pelechrinis, Xin Wang, Prashant Krishnamurthy, and Yijun Mo. "Joint reactive jammer detection and localization in an enterprise WiFi network." *Computer Networks* 57, no. 18 (2013): 3799-3811.

29.P.Vijayakumar, George J., Malarvizhi S, Sriram A, “Analysis and Implementation of Reliable Spectrum Sensing in OFDM Based Cognitive Radio”, Smart Computing and Informatics, Smart Innovation, Systems and Technologies, vol 77, pp 565-572 ,2018

30. P. Vijayakumar, S. Malarvizhi, “Wide Band Full Duplex Spectrum Sensing with Self-Interference Cancellation–an Efficient SDR Implementation “Mobile Networks & Applications, 22(4), 702-711,2017.

Figures

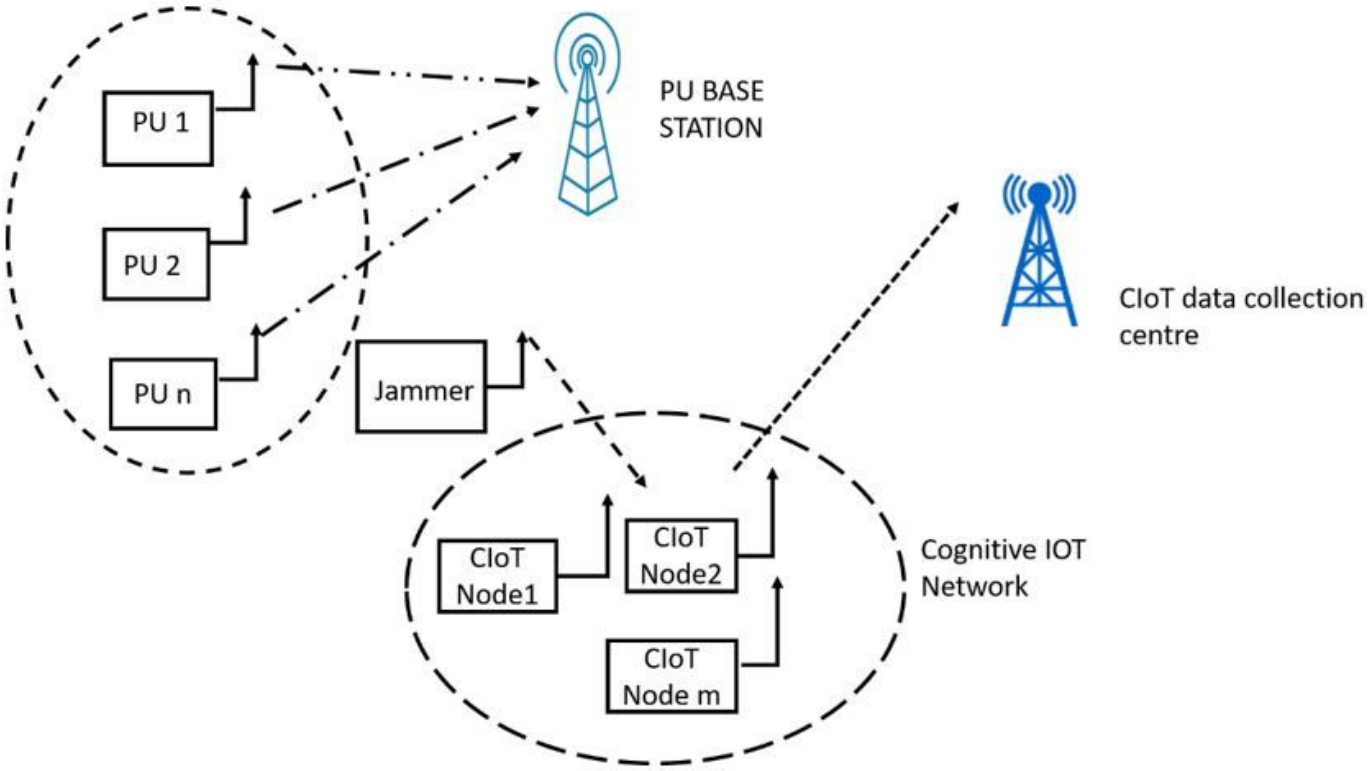


Figure 1

system model of CIoT network with jamming attack

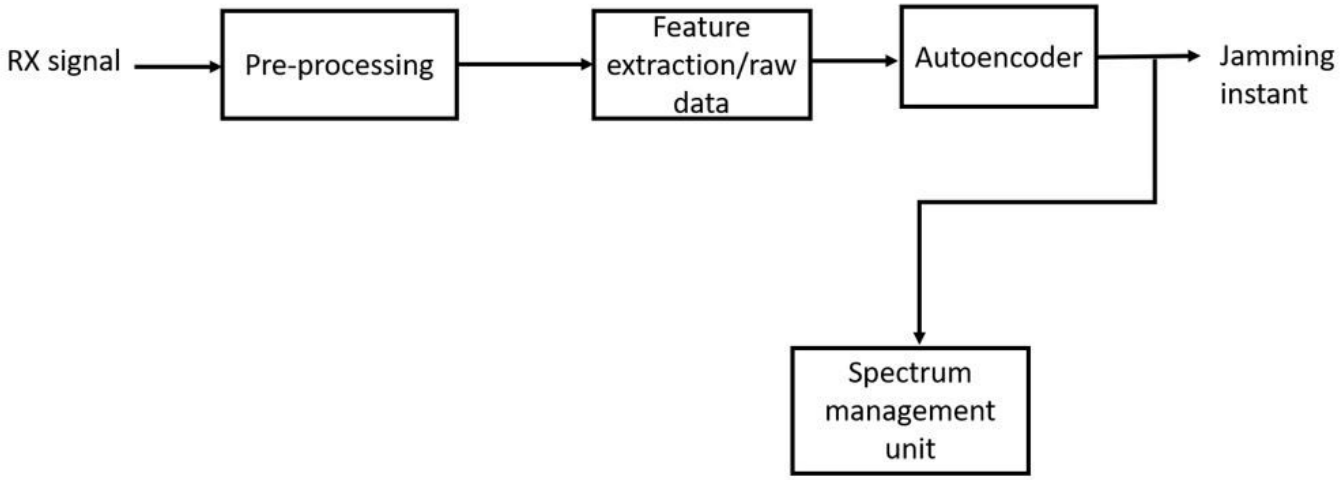


Figure 2

Block diagram of jammer detection using an autoencoder

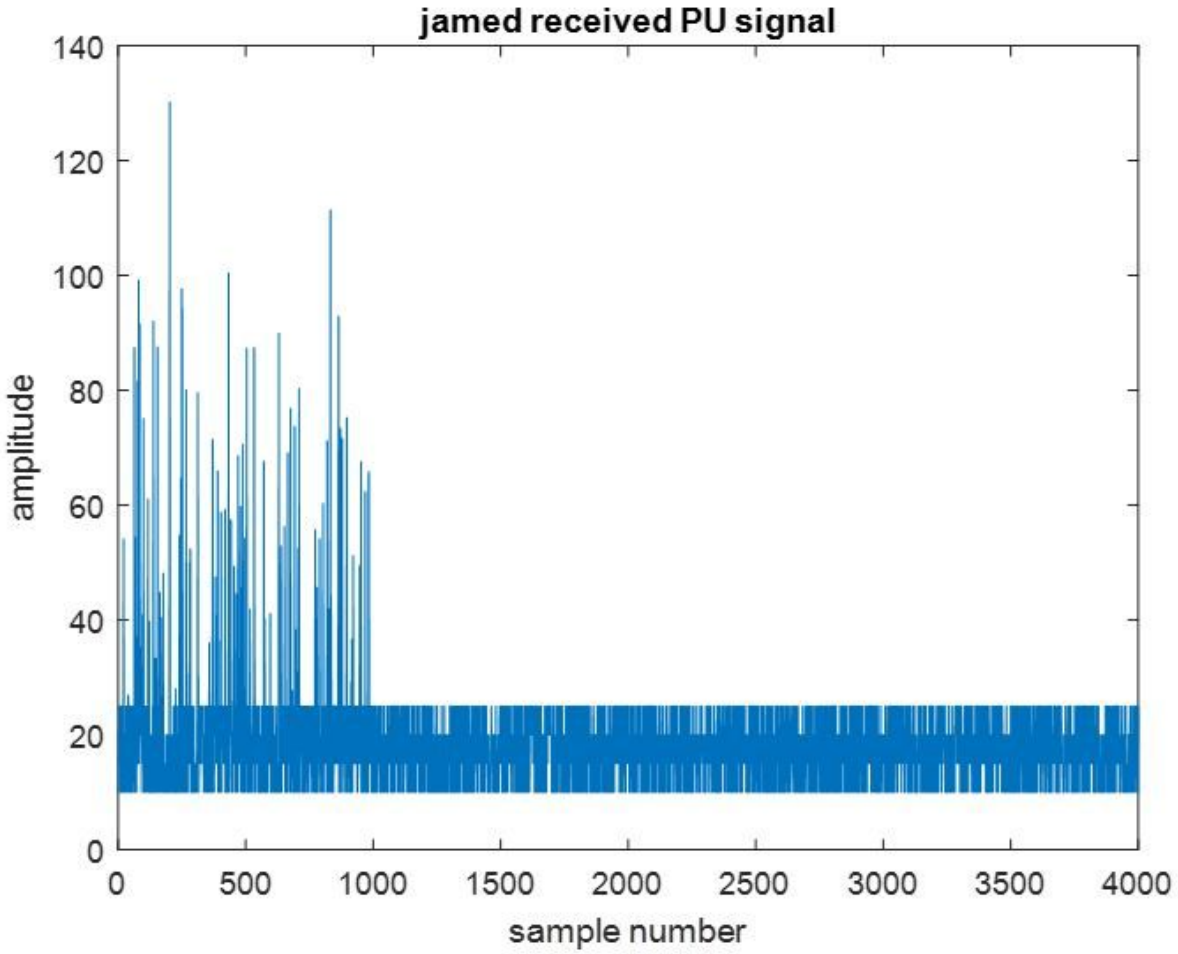


Figure 3

Cognitive radio received signal with jammer and PU signal components

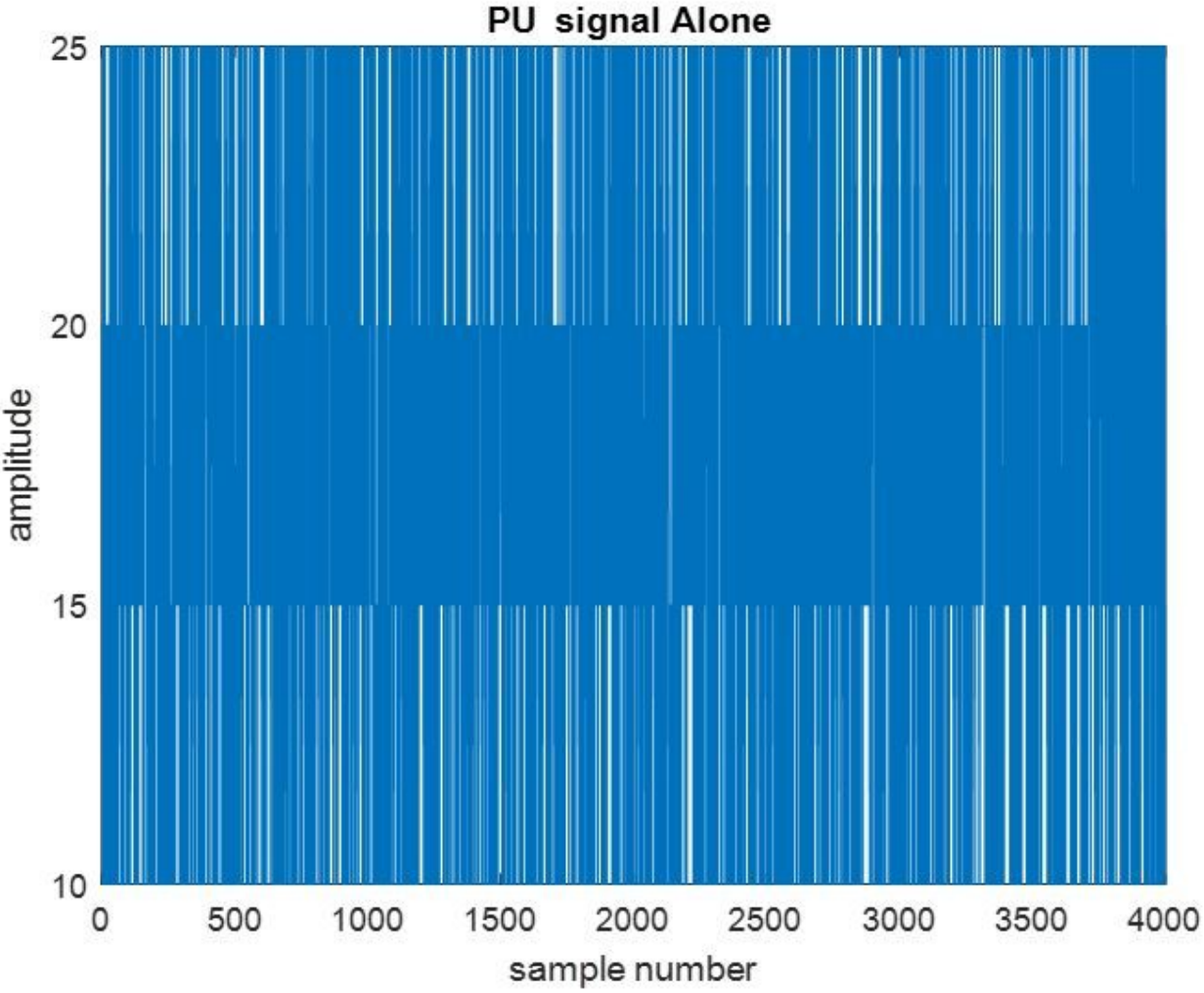


Figure 4

PU signal alone

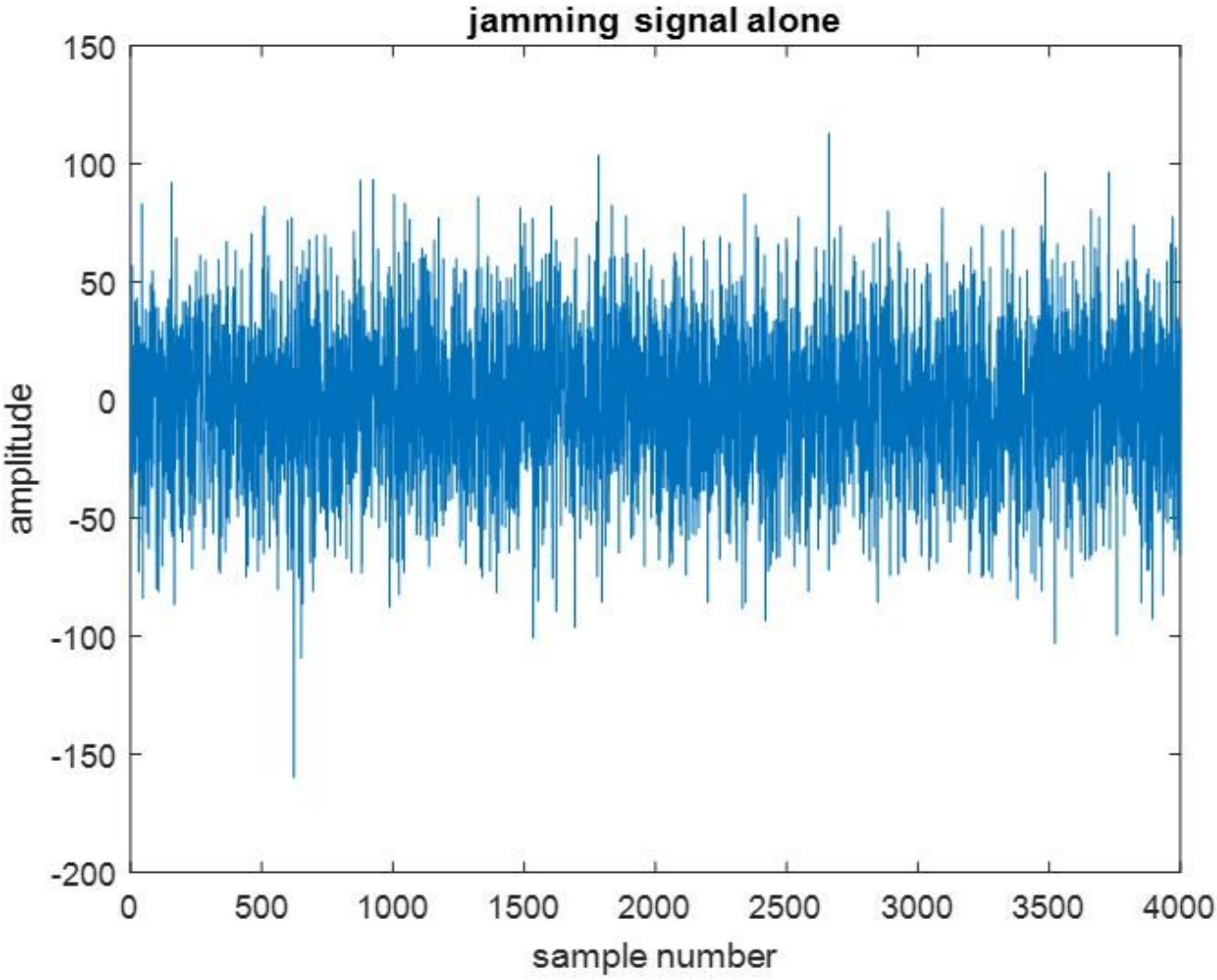


Figure 5

jammer signal alone

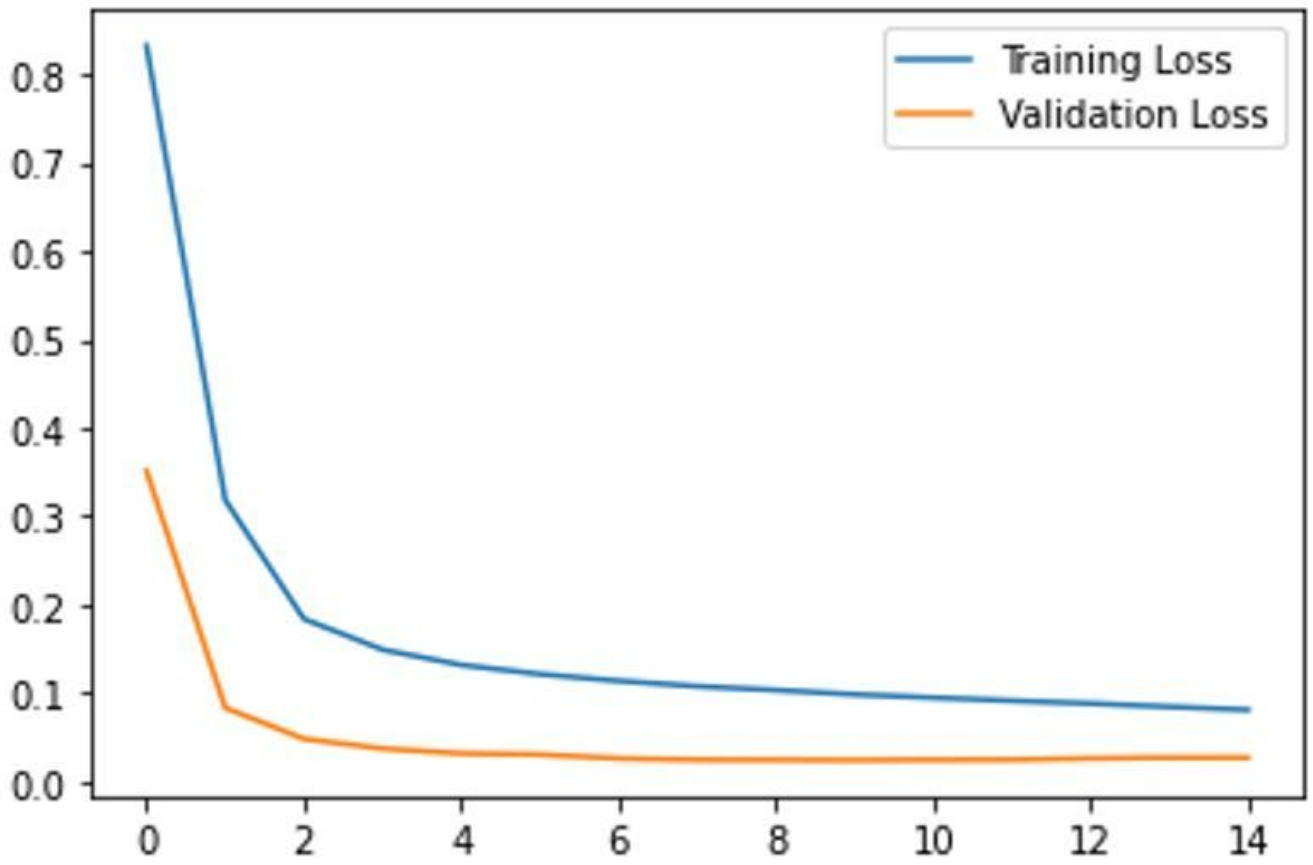


Figure 6

training and validation losses

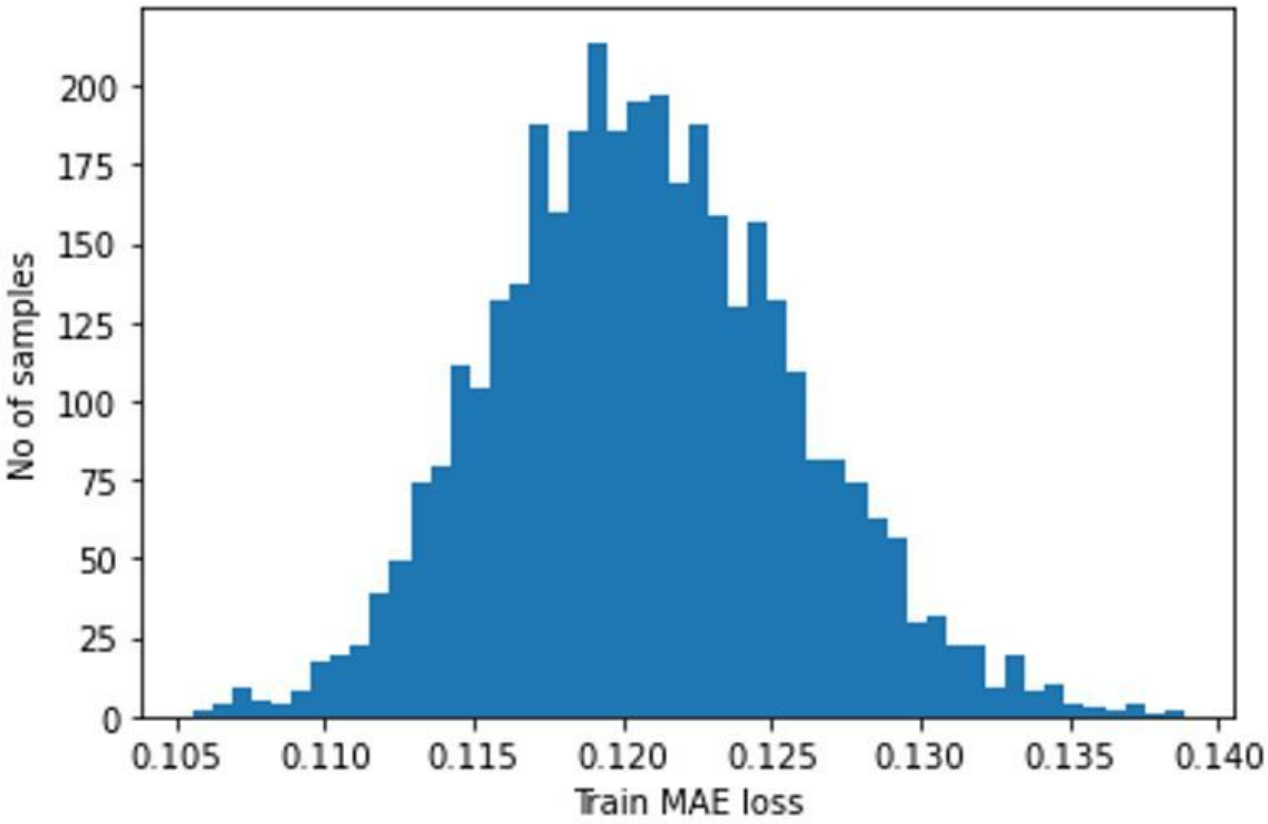


Figure 7

Histogram of the training mean absolute error

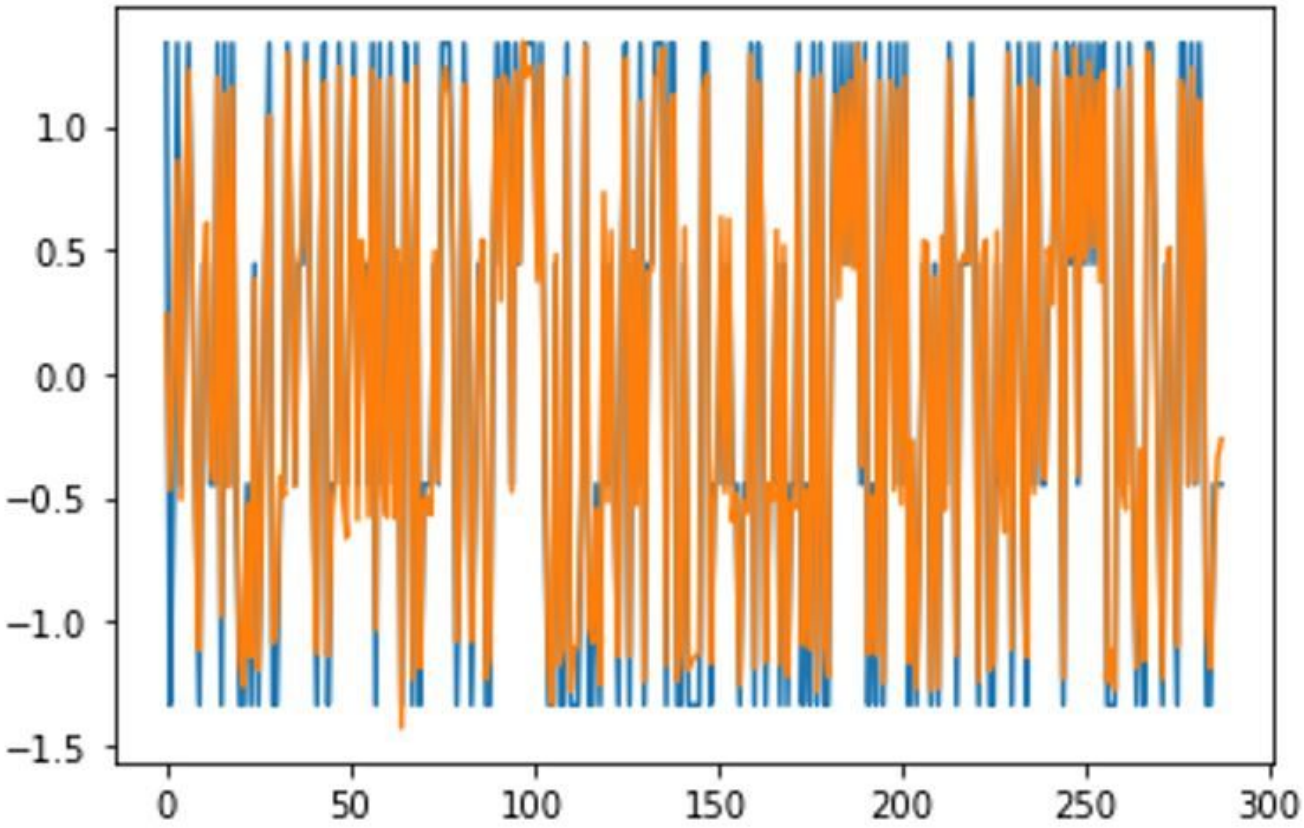


Figure 8

PU signal and decoded PU signal

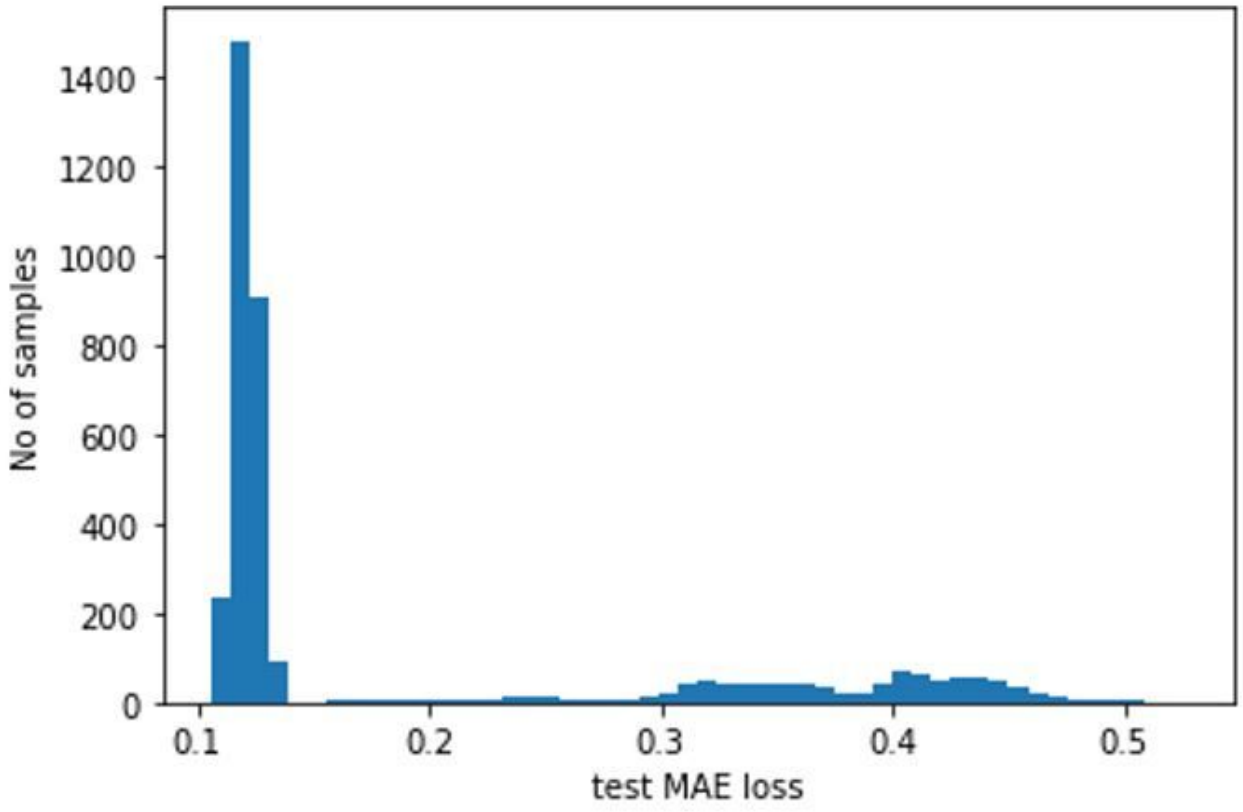


Figure 9

Test Mean Absolute error histogram

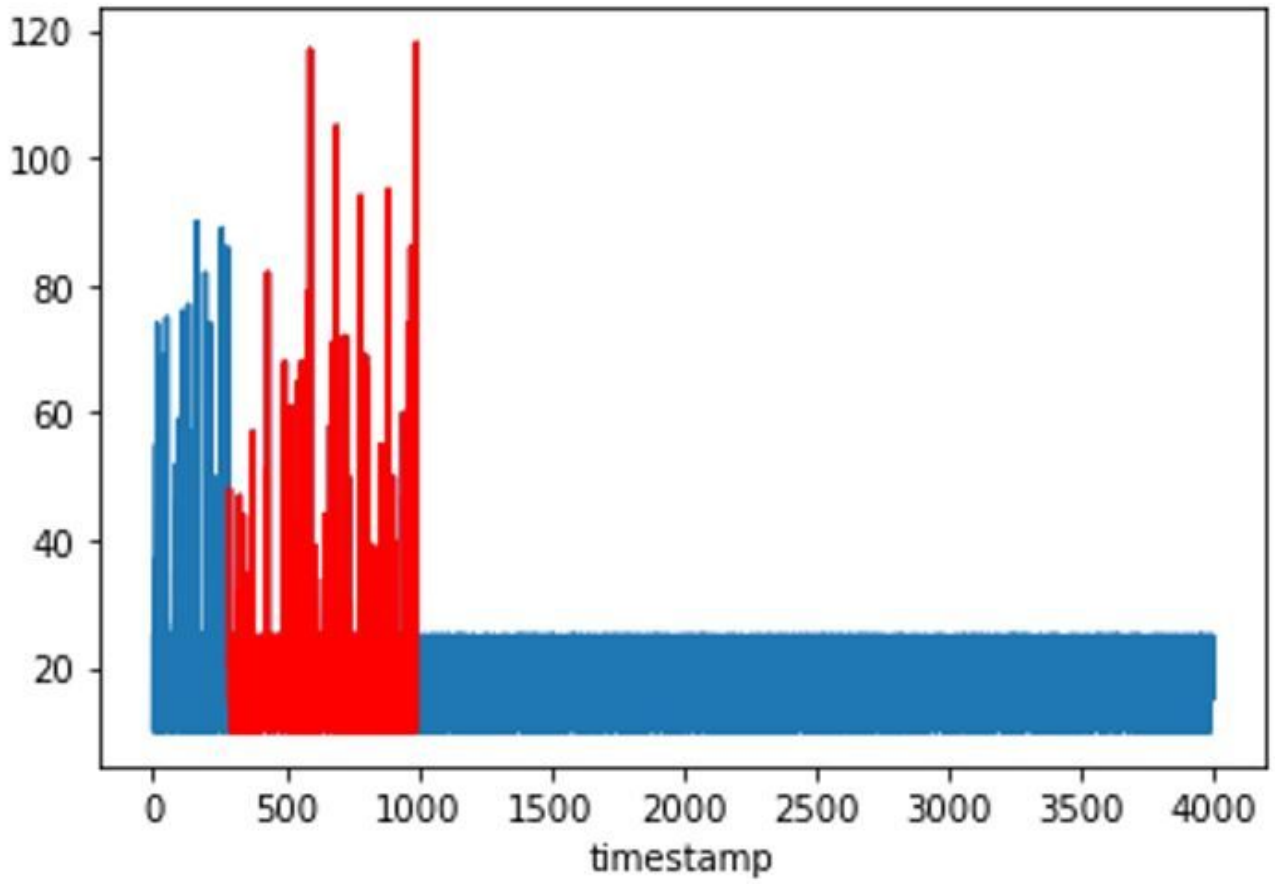


Figure 10

Detected jammer with time stamp information

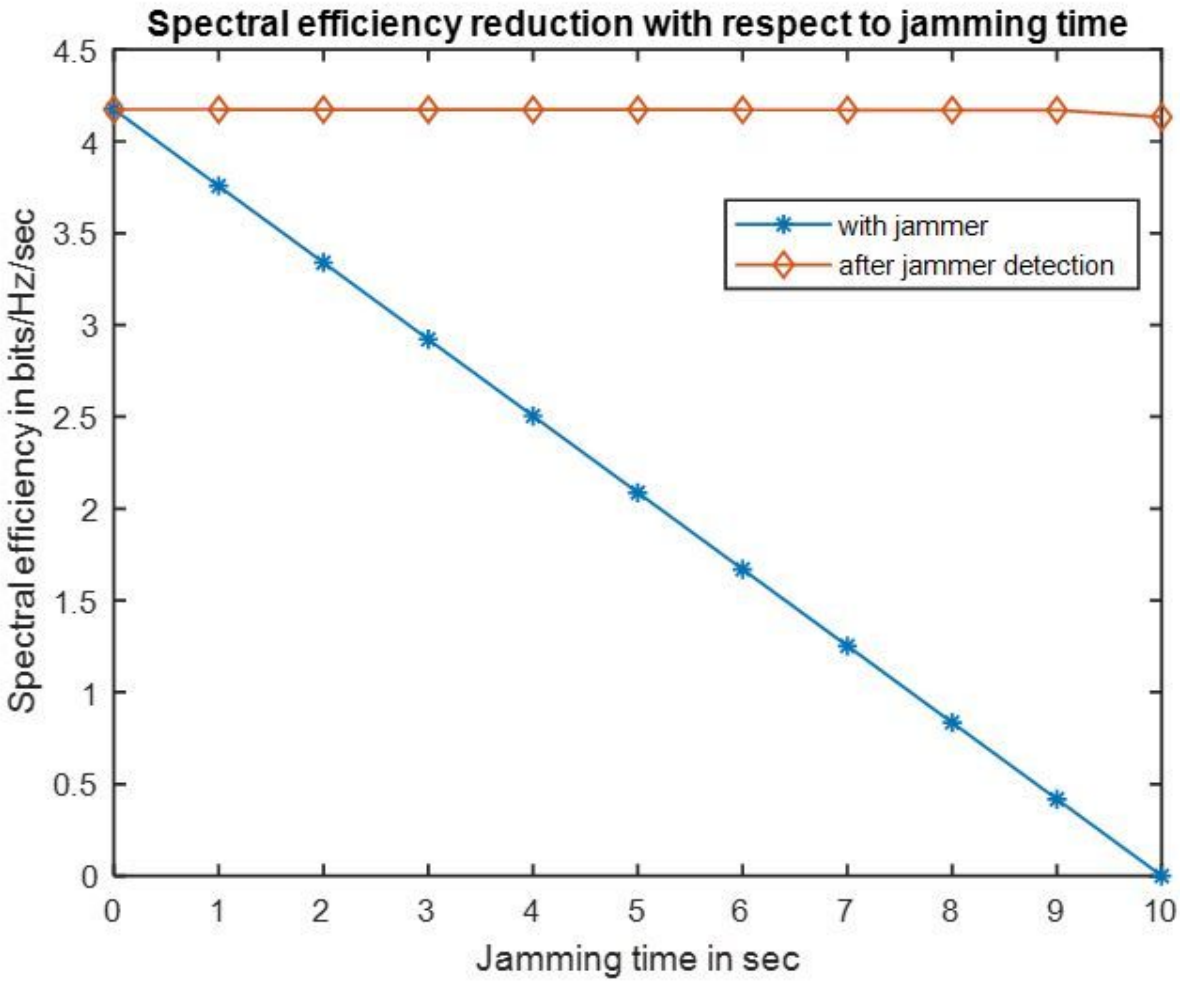


Figure 11

spectral efficiency with a jammer and after jammer detection