Electromagnetic Spectrum Threat Prediction via Deep Learning

Chunyan Wei[1], Lin Qi[1], Ruowu Wu[2], and Yun Lin[1](✉)

[1] College of Information and Communication Engineering,
Harbin Engineering University, Harbin 150001, China
linyun_phd@hrbeu.edu.cn

[2] State Key Laboratory of Complex Electromagnetic Environment Effects
on Electronics and Information System (CEMEE),
Luoyang 471003, Henan, China

Abstract. Nowadays, in the complex electromagnetic environment, the detection of foreign satellite, the electronic interferences and the sensing data tampering in the process of consistent spectrum situation fusion and the electronic countermeasures reconnaissance and enforcement implemented by the enemy electronic attacks all pose serious threats to the communication performance of our electronic devices and communication systems. Therefore, how to detect these electromagnetic spectrum threats effectively is very important. The generative adversarial networks was applied in this paper, which is a method in deep learning, and an unsupervised solution for the above-mentioned electromagnetic spectrum threat signal prediction problem was provided, which has achieved good results. To carry out the detection experiments, three common electromagnetic spectrum threat scenarios were simulated. The prediction performance of the model is evaluated based on the prediction accuracy of the model. The experimental results have shown that the generative adversarial networks model used in this paper has a good predictive effect on the electromagnetic spectrum threat signals of a certain intensity.

Keywords: Electromagnetic spectrum threat · Prediction · Generative Adversarial Networks

1 Data Set

1.1 Measured Data Set

The data set used in this experiment is the FM broadcast signal collected by the USRP (Universal software radio peripheral) device. The specific collection process and parameter setting interface are shown in Fig. 1.

The collected data has a center frequency of 100 MHz, a bandwidth of 2.56 MHz, and a sampling rate of 2.56 Msps. In the collection frequency range, there are a plurality of FM broadcast frequency points. 100,000 samples were collected as training data set and 4000 samples were used as test data set, where each sample was acquired through 10,240 sampling points. Since this article uses an unsupervised learning method, the samples in the training set do not need to be labeled and are considered

S. Liu and G. Yang (Eds.): ADHIP 2018, LNICST 279, pp. 433–442, 2019.
https://doi.org/10.1007/978-3-030-19086-6_48

normal samples [1]. For the 4000 samples in the test set, half of them were subjected to artificial interference processing [2], and the samples regarded as abnormal were marked as “1”; the other half were not interfered, and were regarded as normal samples, and marked as “0” [3]. The parameter description of the data set is shown in Table 1.

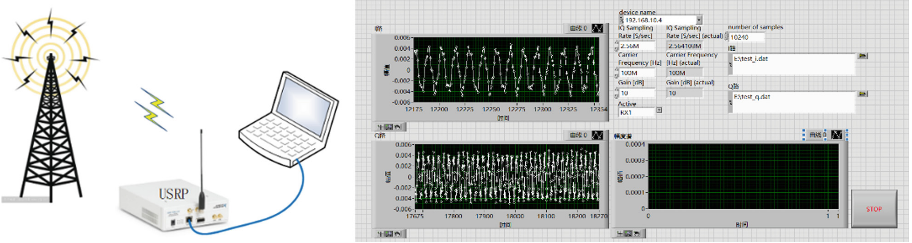

device name
192.168.10.4
IQ Sampling Rate [S/sec]
2.56M
IQ Sampling Rate [S/sec] (actual)
2.564103M
Carrier Frequency [Hz]
100M
Carrier Frequency [Hz] (actual)
100M
Gain [dB]
10
Gain [dB] (actual)
10
Active
RX1
number of samples
10240
I路
E:\test_i.dat
Q路
E:\test_q.dat

Fig. 1. Schematic diagram of data acquisition

Table 1. Dataset parameter description

Parameter	Discrimination
Acquisition frequency band	FM band
Center frequency	100 MHz
Bandwidth	2.56 MHz
Sampling frequency	2.56 Msps
The number of sampling points	10240
The number of samples in the training set	100000
The number of samples in the test set	4000

1.2 Data Preprocessing

In order to facilitate the subsequent effective analysis of the data, this paper uses the Welch estimation [4] method to preprocess the original data. It is a method of power spectral density estimation. The basic idea is to window the signal through the selection window. The power spectrum is segmented and then averaged. In this experiment, the window function selects the Hamming window, which divides the signal into 8 segments. The length of the overlap between each segment is half of the length of the truncated signal. The selected number of points is 512, which is the original dimension. The signal of 10240 was reduced to 512 dimensions after being estimated by Welch.

2 Generative Adversarial Networks

The Generative Adversarial Networks (GAN) [5] is a generative neural networks model based on the differentiable generator networks proposed by Goodfellow et al. in 2014. The GAN consists of a generator networks and a discriminator networks.

The task of the generator (G) is to capture the distribution of the sample data x, and use the input noise vector to simulate the training data to generate samples. The sample generated by G in this article is called a fake sample. The a priori variable of the input noise is represented by $p_z(z)$. The mapping of data space is represented by $G(z;\theta_g)$, where G is a differentiable function represented by a multilayer perceptron with parameter θ_g. The discriminator (D) is a two-classifier whose task is to correctly distinguish the true samples from the training set and the fake samples as possible. The multi-layer perceptron $D(x;\theta_d)$ is defined to output a single scalar, where $D(x)$ represents the probability that input x is from a real sample, and we train D to maximize the probability of correctly classifying samples. We train G to minimize the $\log(1 - D(G(z)))$ at the same. In short, the training process of D and G can be described as the following formula, which is a minimax game with function $V(G, D)$:

$$\min_G \max_D V(D,G) = E_{x \sim p_{data}(x)}[\log D(x)] + E_{z \sim p_z(z)}[\log(1 - D(G(z)))] \tag{1}$$

Therefore, the model will converge according to the following formula,

$$g^* = \arg \min_g \max_d v(g,d) \tag{2}$$

When the model is converged, the real sample and the fake sample generated by the generator are indistinguishable, and the discriminator outputs $\frac{1}{2}$ everywhere. At this time, the discriminator has reached its best discriminating ability, and it can be used to predict the threatening of electromagnetic signals.

According to the generative adversarial networks model built in this paper, the actual training process diagram is shown as Fig. 2.

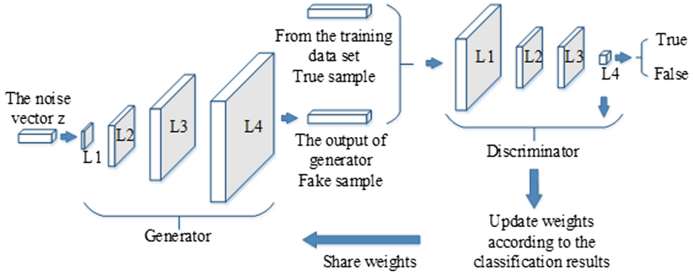

The noise vector z
L1
L2
L3
L4
Generator
From the training data set True sample
The output of generator Fake sample
L1
L2
L3
L4
True
False
Discriminator
Update weights according to the classification results
Share weights

Fig. 2. The training process diagram of generative adversarial networks

In Fig. 2, the generator consists of a four-layer neural networks with 64, 128, 256, and 512 nodes. The generator takes the noise vector as input, the 512-dimensional vector is generated by simulating the real sample according to the layer-by-layer mapping, and that is the fake sample. The true and fake samples are mixed together as the discriminator input. The discriminator in this paper consists of four layers of neural networks, each with 256, 128, 128 and 1 node. The final layer outputs the discrimination result of the input sample, and the discriminator will update the networks weight according to this and share the updated weights with the generator. The generator generates a fake sample again based on the updated weights, and mixes it with the true sample, inputs the discriminator, and then the foregoing process will be repeated. The above process will be repeated until the preset number of trainings is reached. At this time, the discriminator has reached a great discriminating ability and can be used to predict the unknown input. The predicting process is shown in Fig. 3.

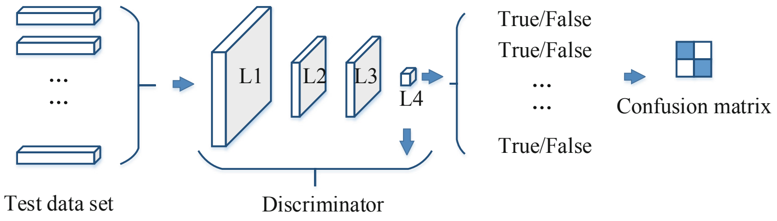


Fig. 3. Schematic diagram of generative adversarial networks prediction

When using the trained model to predict the output of test data, the test data set which contains 2000 normal samples and 2000 abnormal samples is input into the discriminator networks, and the discriminator predicts and outputs the confusion matrix. In this paper, the prediction accuracy is calculated based on the confusion matrix to evaluate the classification performance of the model.

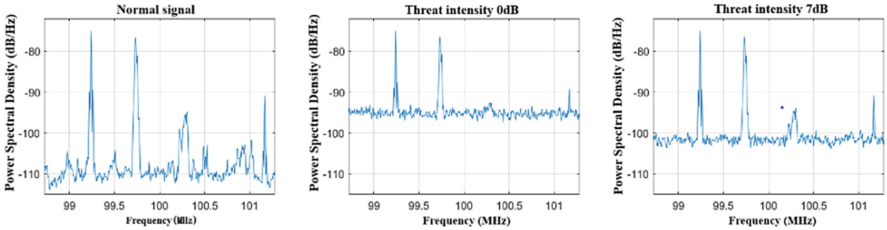
3 Experiment Implement

In this section three common electromagnetic spectrum threats will be simulated: abnormal channel environment threats, band illegal occupancy threats, and broadband signal interference threats. The experiment was designed to use the above-mentioned generative adversarial networks model to carry out the electromagnetic spectrum threat prediction experiment, and we will evaluate the prediction performance of the model according to the experimental results.

3.1 Abnormal Channel Environment Threat Prediction

Threat Situation and Its Data Set. In the wireless communication system, there are situations such as channel environment changes, noise enhancement, etc. [6], and the abnormality caused to the communication by these is called the channel environment abnormal threat [7]. In order to simulate this threat, we superimposes a certain intensity of Gaussian white noise, and the threat intensity is reflected by the signal-to-noise ratio. At the same time, in order to study the prediction performance of the proposed method for different intensity threat signals, Gaussian noise with signal-to-noise ratio of 0 dB–7 dB is added in steps of 1 dB, and threat prediction experiments are carried out.

Figure 4 shows the power spectral density of a data sample before and after the noise is added. Figure 4(a) shows the sample signal without the addition of Gaussian white noise, and Fig. 4(b) and (c) are the power spectral density estimates of the sample signal with the signal-to-noise ratio of 0 dB and 7 dB Gaussian noise, respectively.



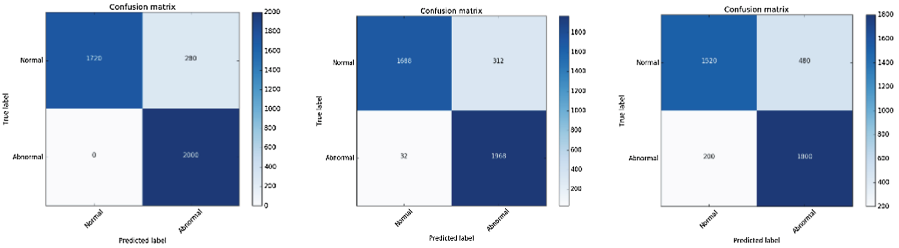
(a) Normal signal (b) SNR=0dB (c) SNR=7dB

Fig. 4. Power spectral density estimation of sample signals under different channel environmental anomalies

As can be seen from Fig. 4, when Gaussian white noise is added, part of the original signal is submerged by noise, and the lower the signal-to-noise ratio, the higher the noise, the more parts of the signal are flooded.

Prediction Results. During the training process, the model automatically performs feature learning on the data samples in the training data set to minimize the error of generative adversarial networks, and a threat prediction model based on GAN can be obtained. Then, we use the test data set to test the model and evaluate its prediction performance based on the classification result on the entire test data set [8].

Figure 5 shows part of the predicted confusion matrix for a trained generative adversarial networks model for data samples in test data sets with different intensities of Gaussian white noise.



(a)SNR=0dB (b)SNR=3dB (c)SNR=7dB

Fig. 5. The predictive confusion matrix output by the generative adversarial networks of abnormal channel environment threat of different intensity.

In order to describe the prediction performance of the model on different intensity threat signals more intuitively, we calculate the prediction accuracy of the model under each SNR based on the confusion matrix obtained by the experiment, as shown in Table 2.

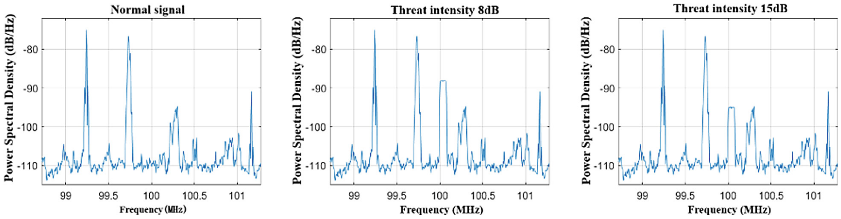
Table 2. The predictive accuracy of the generative adversarial networks on anomaly channel environment threat of different intensity

Signal to noise ratio	True positive	True negative	Prediction accuracy
0 dB	1720	2000	93.00%
1 dB	1718	1998	92.90%
2 dB	1707	1987	92.35%
3 dB	1688	1968	91.40%
4 dB	1661	1941	90.05%
5 dB	1623	1903	88.15%
6 dB	1576	1856	85.80%
7 dB	1520	1800	83.00%

As can be seen in Table 2, for signals with a signal-to-noise ratio of 1–4 dB Gaussian noise, the prediction accuracy of the model can reach more than 90%. As the intensity of the anomaly channel environment threat is weakened, the average prediction accuracy of the model decreases, but for the anomaly signal with a signal-to-noise ratio of 7 dB, the prediction accuracy can still be higher than 80%.

3.2 Band Illegal Occupation Threat Prediction

Threat Situation and Its Data Set. During communication, if the band is occupied by an unknown narrowband signal, the signal received can be anomaly, which can be a threat to the communication [9]. This situation is called a band illegal occupation threat. In order to simulate this threat situation, we artificially superimposed an FM interference signal with a signal-to-interference ratio of 8–15 dB in a step of 1 dB at 100 MHz which is an idle frequency of the signal. The power spectral density map before and after noise addition of a data sample is shown as Fig. 6.

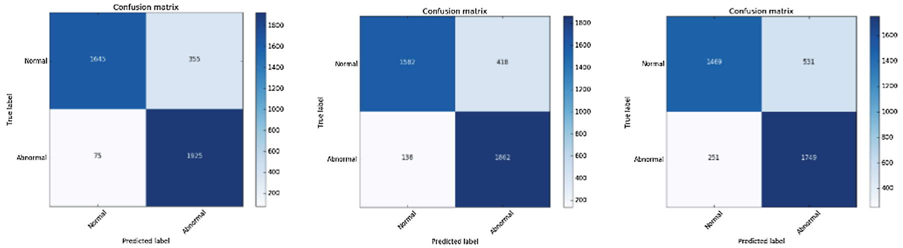


(a) Normal signal (b)SIR=8dB (c)SIR=15dB

Fig. 6. The power spectral density estimation of the sample signal under the band illegal occupation threat of different intensity

As shown in Fig. 6, compared with the normal signal, the signal added the FM interference signal has a spike at the frequency of 100 MHz, that is, the interference signal. The lower the signal-to-interference ratio, that is, the greater the interference intensity, the more the spike high.

Prediction Results. Similarly, we use the test data set to test the model and evaluate its prediction performance according to the classification result. Figure 7 shows part of the predicted confusion matrix for the trained data generative adversarial networks model for data samples in test data sets with different intensities of chirped interference signals.



(a)SIR=8dB (b)SIR=11dB (c)SIR=15dB

Fig. 7. Prediction confusion matrix output by generative adversarial networks for band illegal occupation threats of different intensity.

We calculate the prediction accuracy of model based on the confusion matrix obtained by experiment, as shown in Table 3.

Table 3. The prediction accuracy of the generative adversarial networks of the band illegal occupation threat of different intensity

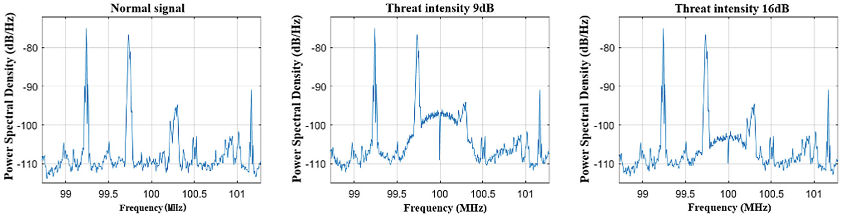
Signal to interference ratio	True positive	True negative	Prediction accuracy
8 dB	1645	1925	89.25%
9 dB	1626	1906	88.30%
10 dB	1601	1881	87.05%
11 dB	1582	1862	86.10%
12 dB	1557	1837	84.85%
13 dB	1529	1809	83.45%
14 dB	1497	1777	81.85%
15 dB	1469	1749	80.45%

As can be seen from Table 3, the prediction accuracy of the model can reach more than 85% for signals with 8–11 dB signal to interference ratio. As the intensity of the threat weakens, the prediction accuracy of the model has decreased, however, for 8 dB–15 dB abnormal signals, there is still a prediction accuracy higher than 80%.

3.3 Wideband Signal Interference Threat Prediction

Threat Situation and Its Data Set. In a wireless communication system, the signal transmitted by the authorized transmitter sometimes can encounters an interference caused by an unknown wideband signal [3]. At this time, the signal of the authorized transmitter is often aliased by the wideband signal, causing the signal received to be anomaly or even to be severely distorted after demodulation [10]. We call that threats to the communication broadband signal interference threat.

In order to simulate this threat, a wideband DSQPSK signal with a signal-to-interference ratio of 9 dB–16 dB is artificially superimposed on the signal in 1 dB steps [11]. Since the wideband DSQPSK is wideband, it can affect all frequency components in a certain frequency band in the sample signal [12]. Figure 8 shows the power spectral density of a data sample before and after noise addition.



(a) Normal signal (b) SIR=9dB (c) SIR=16dB

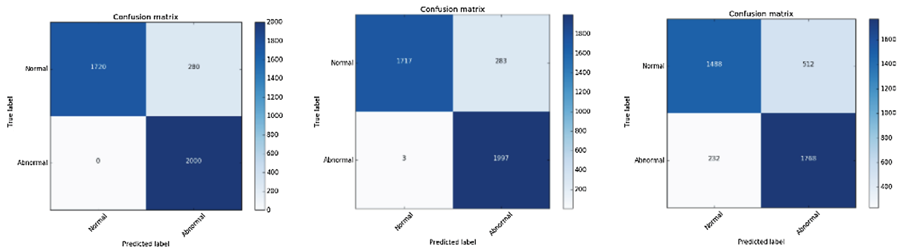
Fig. 8. Estimation of power spectral density of sample signals under different bandwidth broadband signal interference threats

As can be seen from Fig. 8, when the broadband DSQPSK interference signal is added, the spectrum of the signal in the original signal with a frequency of around 100 MHz is superimposed with the interference signal [13]. The lower the signal-to-interference ratio, that is, the greater the interference signal strength, the signal is, the greater the partial power spectral density of the superposition.

Prediction Results. The model is tested by the test data set added the DSQPSK interference signal, and part of the obtained confusion matrix is shown in Fig. 9.

In order to describe the prediction effect of the model on different intensity threat signals more intuitively, we calculate the prediction accuracy of model based on the confusion matrix obtained by experiment, as shown in Table 4.

It can be seen from Table 4 that the model used in this paper can correctly predict the broadband signal interference threat of 9 dB–11 dB, and can achieve the prediction accuracy of 92% or more. As the threat intensity of wideband signal interference decreases, the average prediction accuracy of the model decreases, but the prediction accuracy of more than 80% can still be obtained for the abnormal signal of 9 dB–16 dB.



(a) SIR=9dB (b) SIR=12dB (c) SIR=16dB

Fig. 9. Prediction confusion matrix output by the generative adversarial networks for broadband signal interference threats of different intensity.

Table 4. The prediction accuracy of the generative adversarial networks of the band broadband signal interference threats of different intensity

Signal to interference ratio	True positive	True negative	Prediction accuracy
9 dB	1720	2000	93.00%
10 dB	1720	2000	93.00%
11 dB	1720	2000	93.00%
12 dB	1717	1997	92.85%
13 dB	1690	1970	91.50%
14 dB	1635	1915	88.75%
15 dB	1572	1852	85.60%
16 dB	1488	1768	81.40%

4 Conclusion

In this paper, through the analysis of electromagnetic signals in the background of complex electromagnetic environment, an unsupervised deep learning method, generative adversarial networks, is used to implement experiment to predict the threats caused by the anomalies and interference signals. This unsupervised learning method can automatically learn the features of data through neural networks, eliminating the cumbersome task of tagging large amounts of data. The experiment uses the FM signal collected by USRP equipment, and simulates three common electromagnetic spectrum threats. The results show that the electromagnetic spectrum threat prediction system designed by generative adversarial networks can solve the prediction problem of threat samples in the electromagnetic environment. It provides a new idea for solving the electromagnetic spectrum threat prediction problem in complex electromagnetic environment.

Acknowledgment. This work is supported by the National Natural Science Foundation of China (61771154) and the Fundamental Research Funds for the Central Universities (HEUCFG201830). This paper is also funded by the International Exchange Program of Harbin Engineering University for Innovation-oriented Talents Cultivation. Meantime, all the authors declare that there is no conflict of interests regarding the publication of this article. We gratefully thank of very useful discussions of reviewers.

References

1. Feng, Q., Dou, Z., Li, C., Si, G.: Anomaly detection of spectrum in wireless communication via deep autoencoder. In: Park, J.J.(Jong Hyuk), Pan, Y., Yi, G., Loia, V. (eds.) CSA/CUTE/UCAWSN-2016. LNEE, vol. 421, pp. 259–265. Springer, Singapore (2017). https://doi.org/10.1007/978-981-10-3023-9_42
2. Wen, Z., Luo, T., Xiang, W., et al.: Autoregressive spectrum hole prediction model for cognitive radio systems. In: IEEE International Conference on Communications Workshops, ICC Workshops, pp. 154–157. IEEE (2008)
3. Guan, Q., Yu, F.R., Jiang, S., et al.: Prediction-based topology control and routing in cognitive radio mobile ad hoc networks. IEEE Trans. Veh. Technol. **59**(9), 4443–4452 (2010)
4. Acharya, P.A.K., Singh, S., Zheng, H.: Reliable open spectrum communications through proactive spectrum access (2006). 5
5. Goodfellow, I.J., Pouget-Abadie, J., Mirza, M., et al.: Generative adversarial nets. In: International Conference on Neural Information Processing Systems, pp. 2672–2680. MIT Press (2014)
6. Tumuluru, V.K., Wang, P., Niyato, D.: A neural networks based spectrum prediction scheme for cognitive radio. In: IEEE International Conference on Communications, pp. 1–5. IEEE (2010)
7. Li, H.: Reconstructing spectrum occupancies for wideband cognitive radio networks: a matrix completion via belief propagation. In: IEEE International Conference on Communications, pp. 1–6. IEEE (2010)
8. Kim, S.J., Giannakis, G.B.: Cognitive radio spectrum prediction using dictionary learning. In: Global Communications Conference, pp. 3206–3211. IEEE (2014)
9. Yin, S., Chen, D., Zhang, Q., Li, S.: Prediction-based throughput optimization for dynamic spectrum access. IEEE Trans. Veh. Technol. **60**(3), 1284–1289 (2011)
10. Tu, Y., Lin, Y., Wang, J., et al.: Semi-supervised learning with generative adversarial networks on digital signal modulation classification. CMC-Comput. Mater. Continua **55**(2), 243–254 (2018)
11. Zhou, J.T., Zhao, H., Peng, X., et al.: Transfer hashing: from shallow to deep. IEEE Trans. Neural Netw. Learn. Syst. **PP**(99), 1–11 (2018)
12. Zheng, Z., Sangaiah, A.K., Wang, T.: Adaptive communication protocols in flying ad-hoc networks. IEEE Commun. Mag. **56**(1), 136–142 (2018)
13. Zhao, N., Richard Yu, F., Sun, H., Li, M.: Adaptive power allocation schemes for spectrum sharing in interference-alignment-based cognitive radio networks. IEEE Trans. Veh. Technol. **65**(5), 3700–3714 (2016)