Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Combinatorial Press

Low-orbit satellite signal interference detection based on fast regional convolutional network and its multidimensional evaluation method

Jieliang Zheng[1], Fenghua Xu[1], Yukun Zhu[1], Jian Zhou[1] Qiang Lv[2,✉], Rui Guo[3], Yu Chen[4]

[1] *School of Computer Science and Engineering (School of Cyber Security), University of Electronic Science and Technology of China, Chengdu, Sichuan, 611731, China*
[2] *Beijing Guodiangaoke Co., Ltd., Beijing, 100095, China*
[3] *School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan, 611731, China*
[4] *Laboratory of Space Prevention, Control and Cyber Security, Qingdao Research Institute, Sichuan University, Qingdao, Shandong, 266000, China*

ABSTRACT

To counter threats to low-orbit communication satellites from hacker attacks and spectrum interference, this study develops an adversarial sample detection model using a variational self-encoder and a fast region-based convolutional network for spectrum interference detection. The proposed model achieves 97.68% accuracy and an F1 score of 96.86% in intrusion traffic detection, with AUC values above 95% for various network attacks. For single-tone interference, it attains 98.65% accuracy, 96.21% recall, and 93.14% precision, converging within 200 iterations with an average recognition accuracy of 95.47%. These results confirm the model's ability to detect adversarial threats and interference, enhancing satellite communication security.

Keywords: low-orbit satellites, environmental threats, adversarial samples, variational self-encoders, spectral interference

1. Introduction

In LEO satellite communication systems, the ground electromagnetic spectrum environment faced by satellites is quite complex due to the low orbital altitude and fast operating speed. In practice, LEO satellite communication systems mostly use the UHF band or L band, which are now very

✉ Corresponding author.
E-mail address: lvqiang1980aa@163.com (Q. Lv).

Received 21 July 2024; Accepted 13 November 2024; Published Online 18 March 2025.

DOI: 10.61091/jcmcc124-33

crowded, and there are also unauthorized military applications, amateur radio applications and possible malicious interference [11, 5, 19, 12]. In addition to this, the actual utilization efficiency of some of the frequency bands is extremely low if the percentage of time the bands are actually occupied is defined as their utilization efficiency [2, 14]. The premise and foundation of cognitive radio lies in how to perceive and predict the complex spectrum environment. On the one hand, the communication system needs to perceive the complex spectrum environment, analyze the location of spectrum nulls, and predict the availability of nulls in the future [4, 21, 7, 6]. On the other hand, in order to verify the actual availability of the system, the actual spectrum environment needs to be simulated, and the spectrum environment is further simulated and generated by predicting the interference [8, 3, 18, 1].

Spectrum sensing can efficiently acquire spectrum posture data thus improving spectrum utilization efficiency, which makes satellite-assisted spectrum sensing an effective way to realize spectrum sensing [20, 16, 15]. However, in the complex electromagnetic environment, the spectrum signal at the receiving end will inevitably be subject to certain unknown interference, which is reflected in the spectrum as interference information [17, 10, 9]. In addition, the probability of signal interference in real scenarios is relatively large and has many reasons [13]. Therefore, in order to effectively detect the electromagnetic spectrum interference information under the condition of existing a priori information or a small amount of information is really important for the spectrum sensing results.

In this context, in order to deal with various threats and challenges facing LEO communication satellites in a more comprehensive way, the study proposes a variational self-encoder (VSE)-based adversarial sample detection model (ASDM). It also proposes a spectrum interference detection model based on fast region-based convolutional network (Fast R-CNN). To react quickly to the effects of various threat sources on the operational security of satellites, the research attempts to provide an efficient threat detection technique for low-orbit communication satellites. The study is innovative in that it uses an unbiased teacher model to train the Faster R-CNN, allowing for improved detection performance during training even with a limited sample set.

2. Modeling of environmental threat detection for low-orbit communication satellites

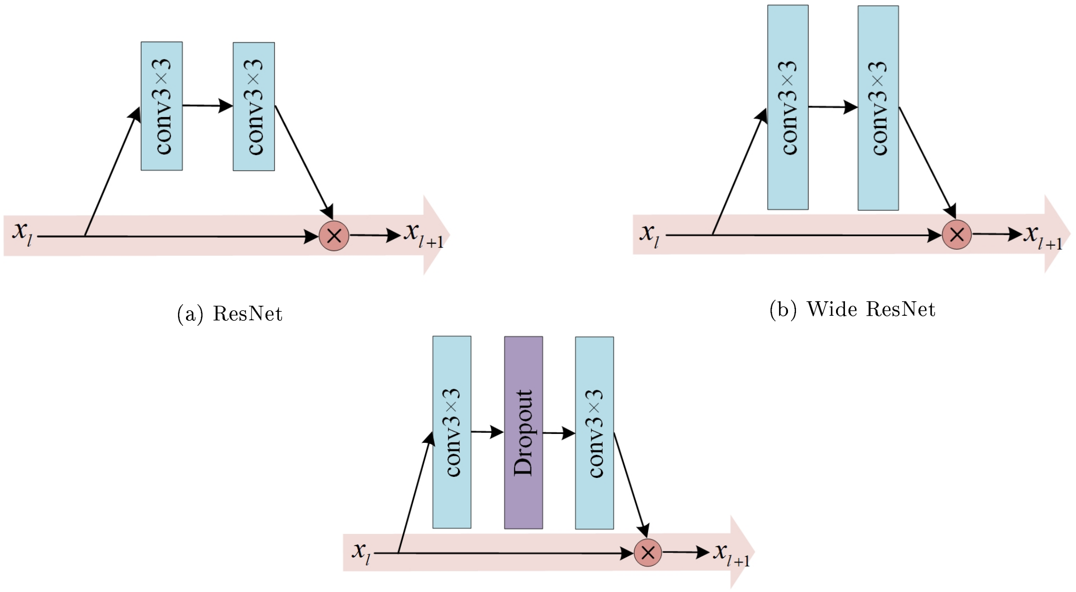
To ensure the stability and reliability of low-Earth orbit communication satellites, it is crucial to detect environmental threats. To this end, the study will combine variational autoencoders and residual networks to build an AS detection model based on variational autoencoders. And use an unbiased teacher model to train Faster R-CNN and build a spectrum interference detection model based on Faster R-CNN.

2.1. VSE-based adversarial sample detection model

Adversarial sample attack refers to the attacker modifying the data in the communication signal of a low-orbit communication satellite so that it is maliciously manipulated during transmission, thereby affecting the accuracy and security of communication. It not only affects the real time and reliability of satellite communication, but may also leak sensitive information or cause incorrect instructions to be executed, posing a serious threat to national security and social stability. The study gathers network traffic data from communication satellites during normal operation and under cyberattack, respectively, in order to identify the ASs. Depending on the volume of data, the network traffic data is transformed into picture format, and the AS generation algorithm creates the ASs in order to train the model. Eq. (1) displays the classification loss of the AS generation algorithm.

$$\max_{\|\delta\|p\leq\in} -\log\hat{D}(x+\delta)[y], \tag{1}$$

In Eq. (1), $\hat{D}$ denotes a pre-trained classifier, x denotes a clean image labeled y, δ denotes the perturbation and p usually takes the value of 1 or 2. VSE is a generative model that is able to learn potential representations of input data by combining the ideas of deep learning and probabilistic graphical models. The study employs VSE as a generator G to capture category redundant images $G(x)$. Then, category related images $x - G(x)$ are sent to the discriminator. Subsequently, the one containing category core information $x - G(x)$ is passed to the discriminator D for classification. The study uses wide residual networks (Wide ResNet) as a discriminator. ResNet is a deep convolutional neural network (CNN) structure, and its core idea is to realize a deeper network structure (NS) by introducing residual blocks. However, the jump connection of ResNet also leads to only a small number of residual blocks learned useful information, so Wide ResNet is born. Wide ResNet reduces the problem of reduced feature reuse that can occur in deep residual networks by introducing more convolutional kernels in the residual blocks and improves the training speed and performance of the model by increasing the width of the network. A comparison of the residual blocks of traditional ResNet and Wide ResNet is shown in Figure 1.



(a) ResNet

(b) Wide ResNet

(c) Wide-dropout

Fig. 1. Residual blocks of wide ResNet and traditional ResNet

In Figure 1, Figure 1a is the most basic ResNet structure. Figure 1b is the wide residual block structure. Figure 1c is the WideResNet structure with dropout layer added to the ResNet structure. The primary task of the objective function of the proposed intrusion traffic against sample detection method of the study is to reconstruct x in the generation process of VSE, as shown in Eq. (2).

$$L = \tau K\left(q_\phi(l\,|x)\,\|p(l)\right) - E_{q_\phi(l|x)}\log p_\theta(x\,|l). \tag{2}$$

In Eq. (2), l denotes the latent factor, $q_\phi(l\,|x)$ denotes the posterior distribution, $p_\theta(x\,|l)$ denotes data likelihood, τ denotes the hyperparameter, which is used to balance the reconstruction error and the regularization of the latent space, K denotes KL scatter, used to measure the difference between two probability distributions and $p(l)$ denotes prior distribution. The cross-entropy loss function (CELF) is used in the study, as shown in Eq. (3).

$$J = -\sum y \log y^*. \tag{3}$$

In Eq. (3), y represents the true category, and y^* represents the predicted category. To summarize, the flow of decoupling network intrusion traffic picture categories is shown in Figure 2.

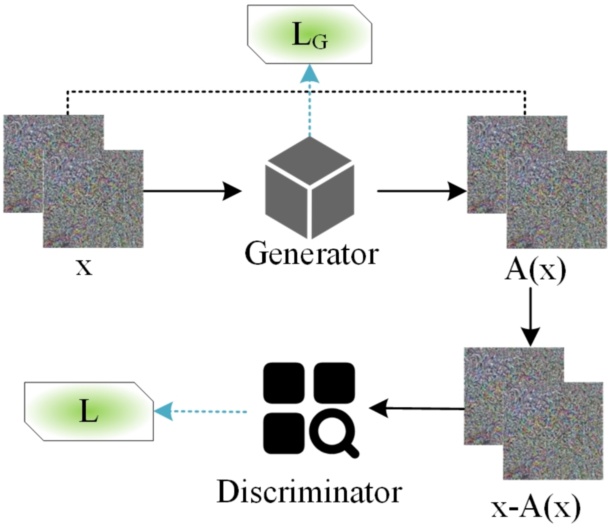


Fig. 2. Flowchart for decoupling traffic images

In Figure 2, category decoupling achieves the recovery of the original image by separating the input ASs into $A(x)$ and $x - A(x)$. Among them, $A(x)$ contains category-related information useful for classification. The adversarial perturbations generated by the network attack are mainly concentrated on $x - A(x)$, revealing the main image region of interest for the classifier. The proposed VSE-based ASDM first extracts the feature map (FM) of $x - A(x)$ using category decoupling. and computes the multiple local intrinsic dimensions between the FMs of the ASs and the normal samples, denoted as matrix m. The multiple local intrinsic dimensions are a further development of the local intrinsic dimensions. Let the continuous space of a nonnegative distance function d be R. The distribution of distances between any point c and other points in R is a random variable $D \in [0, +\infty)$. If the cumulative density function $C(d)$ of d is positive and continuously differentiable when d is greater than 0, then the intrinsic dimension of the point c, as shown in Eq. (4).

$$ID_D(d) \triangleq \lim_{\varepsilon \to 0} \frac{\log C_D\left((1+\varepsilon)d\right) - \log C_D(d)}{\log(1+\varepsilon)}. \tag{4}$$

Finally, matrix m is utilized to train random forest (RF) and the analysis results of different intrinsic dimensions are fed into the RF model for binary classification. RF is a machine learning algorithm that refers to a classifier that utilizes multiple trees to train and predict samples. Figure 3 displays the RF model's schematic diagram.

The proposed VSE-based ASDM decouples clean samples and ASs by category during the training process. Moreover, the decoupled samples are used to train the RF model to realize the detection of ASs.

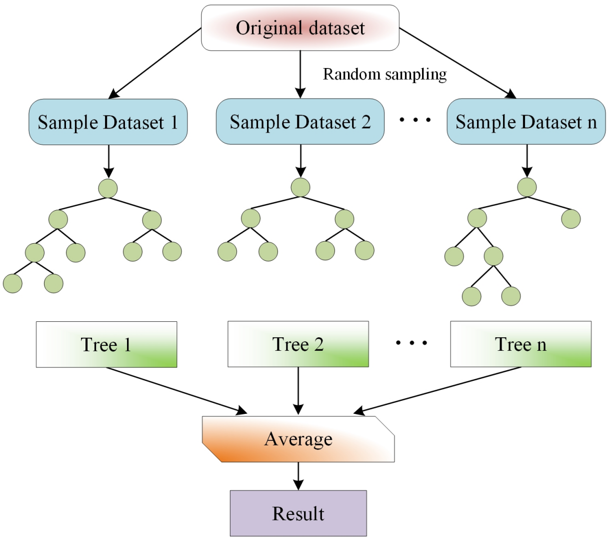


Fig. 3. Schematic diagram of RF model

2.2. *Faster R-CNN-based model for spectrum interference detection*

In addition to cyber-attacks, spectrum interference is also an important factor that threatens the normal operation of LEO communication satellites. Therefore, the research will build the spectrum interference detection model. Faster R-CNN is a deep neural NS for object detection, and the main innovation is the faster object detection speed achieved by adding region proposal network (RPN), which enables Faster R-CNN to be trained end-to-end. Therefore, the study uses Faster R-CNN for spectrum interference detection. The NS of Faster R-CNN consists of four main components: shared neural network (SNN), RPN, region of interest (RoI) and classification. Figure 4 depicts Faster R-CNN's core architecture.

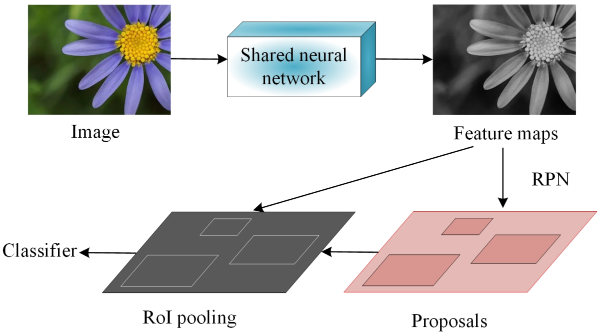


Fig. 4. Structure diagram of Faster R-CNN

Figure 4 displays the FM of the picture extracted by the SNN, which consists of 4 pooling layers, 13 relu levels, and 13 conv layers. Using Softmax to ascertain whether the anchor points are foreground or background, RPN is utilized to create the target region. To determine the target FMs, ROI gathers and compares the input FMs and target regions. to maximize the model's prediction accuracy by modifying the Faster R-CNN model's parameters and weights. The study uses the unbiased teacher model to train the Faster R-CNN. The unbiased teacher model is a deep learning model training framework that can be seamlessly inserted into existing deep learning workflows, effectively mitigating potential biases in the model. Figure 5 depicts the unbiased instructor model's organizational structure.

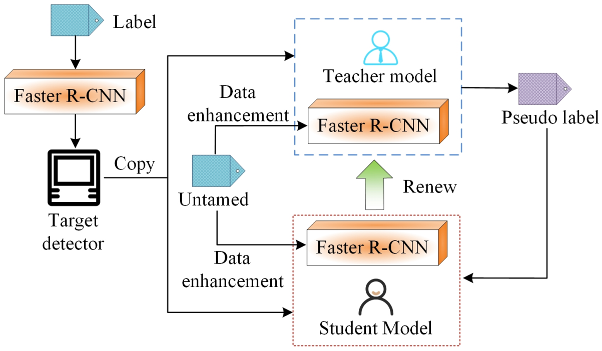


Fig. 5. The structure of unbiased teacher model

The study set the RPN's loss to the CELF, but the RPN simply filtered out target frames that are judged to be background. With less training data, the CELF causes the prediction results to be biased towards a larger number of target categories. Therefore, the study sets the loss of RoI to Focal Loss. To help to enable the model to focus more on the difficult-to-split samples, focal Loss is a loss function (LF) that was created to address the issues of positive and negative sample imbalance as well as hard and easy sample imbalance in the target identification task. Focal loss is shown in Eq. (5).

$$F = -(1-P)^{\delta}\log(P). \tag{5}$$

In Eq. (5), P denotes the probability of predicting a particular category and δ denotes the hyperparameter. In Eq. (5), when the P of the target sample is larger, $(1-P)$ is close to 0, then the weight of this target is smaller when calculating the loss, and vice versa, the weight is not affected. The larger the hyperparameter δ is the greater the degree of change. When it is 0, Focal loss is equivalent to the CELF. The Fast R-CNN model's total loss consists of the following: regression losses for RPN reference frames, RPN classification, RoI target frames, and RoI classification. using Fast R-CNN by reducing the multi-task loss objective function. Eq. (6) illustrates the image's LF.

$$Loss(P_a, y_a) = \frac{1}{N_c}\sum_a Loss_c(P_a, P_a^*) + \kappa\frac{1}{N_r}\sum_a P_a^* Loss_r(y_a, y_a^*). \tag{6}$$

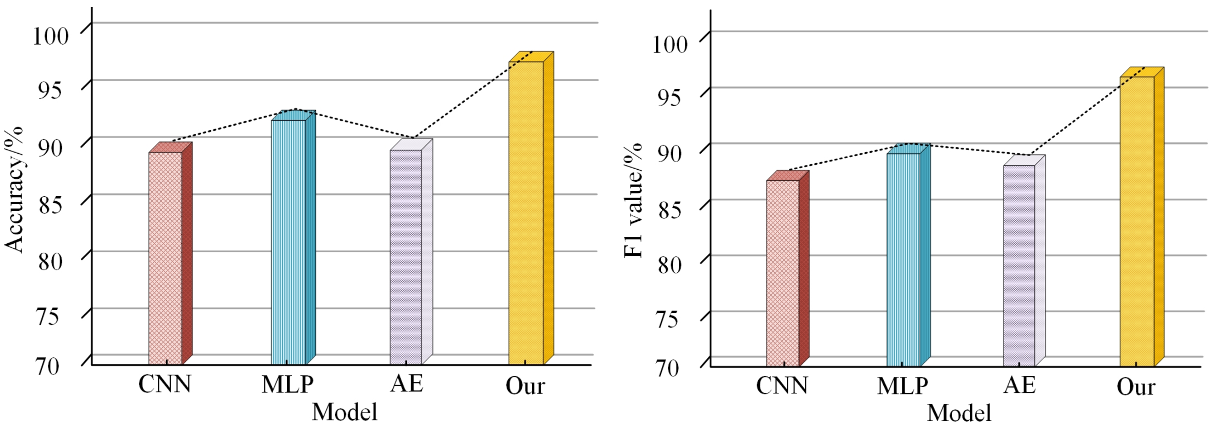
In Eq. (6), a denotes the index of the anchor, P_a denotes the predicted probability that anchor is a target, $Loss_c$ denotes classification loss, κ represents the parameter, $P_a^* Loss_r$ denotes regression loss, y_a denotes coordinate parameter, y_a^* denotes the information associated with having a target anchor and P_a^* is 0 if the anchor is not a target and 1 if it is a target. Therefore, the final loss of Fast R-CNN model training is the sum of RPN loss and RoI loss. The final optimization goal of the model is to minimize the final loss.

3. Result

3.1. Effectiveness analysis of the adversarial sample detection model

To exam the performance of VSE based ASDM, the study is tested using CIC-IDS2017 dataset. The CIC-IDS2017 dataset is created by the Canadian Institute of Cybersecurity and is a network intrusion detection dataset that includes benign and the latest common attacks, similar to real-world data. The collection period starts on Monday, July 3rd, 2017 and ends on Friday, July 7th, 2017, totaling 5 days. Monday only includes normal traffic, while the other days include network attacks such as brute force FTP, brute force SSH, DoS, Heartbleed, web attacks, penetration, botnets, and

DDoS. The experiments are conducted in Windows 11 environment with Intel(R) Xeon(R) Gold 6226R processor and 64GB of RAM. The proposed model is compared with three common intrusion traffic detection models, namely, CNN, multilayer perceptron (MLP) and auto-encoder (AE). The results of accuracy and F1 value comparison of the four models in intrusion traffic detection are shown in Figure 6. In Figure 6a, the proposed ASDM has the highest detection accuracy of 97.68% compared to the other three models. This is followed by the MLP model with a detection accuracy of 92.51%. In Figure 6b, the proposed ASDM still has the highest F1 value of 96.86%. The findings demonstrate that the suggested ASDM performs better in terms of intrusion traffic detection.

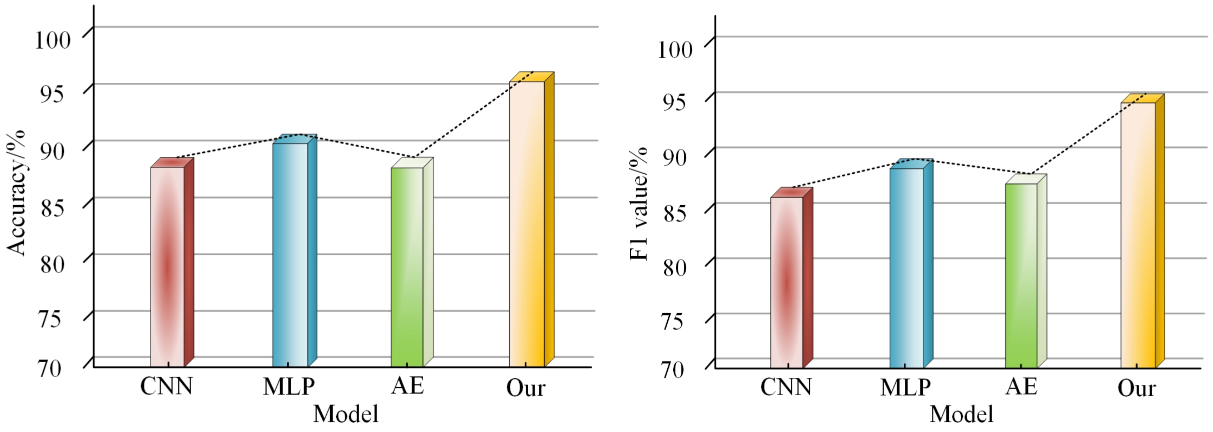


(a) Accuracy

(b) F1 value

Fig. 6. Comparison of detection performance of four models in intrusion traffic

The detection accuracies and F1 values of the above four models in normal traffic are shown in Figure 7. In Figure 7a, the detection accuracy of the proposed antagonistic sample detection model is still higher than the other three models, which is 95.63%. In Figure 7b, the proposed ASDM has the highest F1 value of 95.87%. The outcomes exhibit that the VSE-based ASDM still has a good detection effect in the normal flow detection task.



(a) Accuracy

(b) F1 value

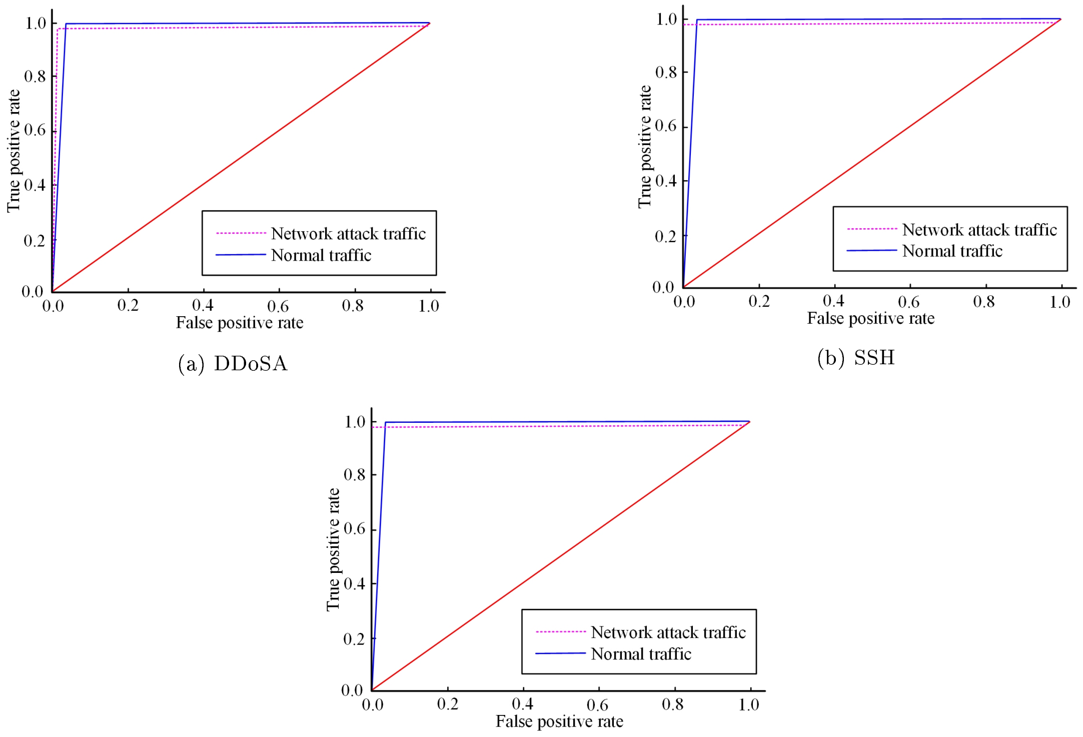
Fig. 7. Comparison of detection performance of four models in normal traffic

The detection accuracy of the above four models under the four antagonistic sample generation methods of fast gradient symbolic method (FGSM), basic iterative method (BIM), projection gradient descent (PGD) and Carlini-Wagner (CW) attack are shown in Table 1. Compared with the other three models, the proposed ASDM has the highest detection accuracy under all four AS generation methods, FGSM, BIM, PGD, and CW, which are 90.16%, 89.65%, 96.84%, and 94.62%, respectively. The outcomes display that the ASDM has higher discrimination accuracy in AS attacks.

Table 1. Comparison of adversarial sample detection results using different attack methods

Model	Adversarial sample generation method			
	FGSM	BIM	PGD	CW
CNN	85.93%	83.64%	88.46%	86.57%
MLP	87.95%	85.39%	90.16%	89.95%
AE	85.98%	83.49%	89.65%	86.98%
Our	90.16%	89.65%	96.84%	94.62%

To verify the practical application effect of the VSE-based ASDM, the study collects a total of 94,025 network attack traffic samples in a low-orbit satellites communication network. It contains three typical network attacks, DDoSA, secure shell (SSH) blasting and port scanning, and 22,138 normal traffic samples as experimental data. Based on an 8:2 ratio, it is split into training and test sets. The receiver operating characteristic (ROC) curves of the proposed model under different network attacks are shown in Figure 8. The proposed ASDM has better detection results in all three typical network attacks, and the area under the curve (AUC) for detecting both normal and intrusion traffic is above 95%. The outcomes demonstrate the practical applicability of the VSE-based ASDM.



(a) DDoSA

(b) SSH

(c) port scanning

Fig. 8. ROC curves of models under different network attacks

3.2. Effectiveness analysis of spectrum interference detection model

For validating the performance of the proposed Fast R-CNN based spectrum interference detection model, the study uses the dataset constructed for testing. The learning rate, teacher model parameter retention rate, iterations, epoch, and the reference frame threshold is set to 0.01, 0.9996, 1000, 300, and 0.7. The detection effectiveness of the proposed model in different interference types is shown in Table 2. The proposed spectrum interference detection model has the best detection effect in single tone interference detection. The detection accuracy, recall and evaluation precision are 98.65%, 96.21%, and 93.14%, respectively.

Table 2. The detection performance of the model in different types of interference

Interference type	Precision/%	Recall/%	Average precision/%
Tone interference	98.65	96.21	93.14
Polyphonic interference	92.24	90.49	85.15
Linear sweep interference	99.95	97.66	98.67
Pulse interference	87.34	86.17	83.65
Partial noise interference	91.38	90.35	84.98

The detection accuracy curve of the proposed Fast R-CNN-based spectrum interference detection model on the test set is shown in Figure 9. The proposed spectrum interference detection model converges at about 200 iterations, and the average recognition accuracy is 95.47%. The outcomes display that the Fast R-CNN-based spectrum interference detection model has high recognition accuracy and convergence efficiency, which is feasible and effective.

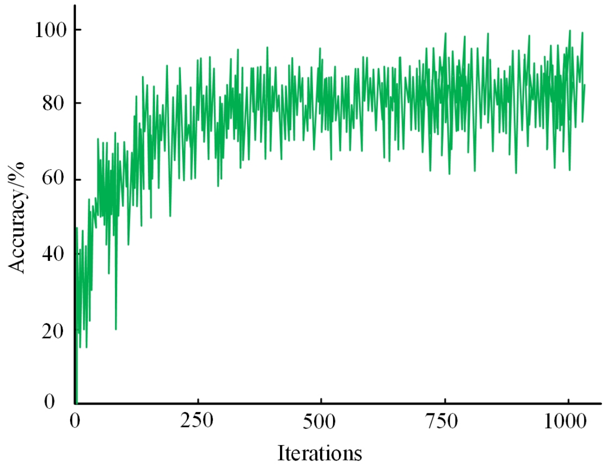
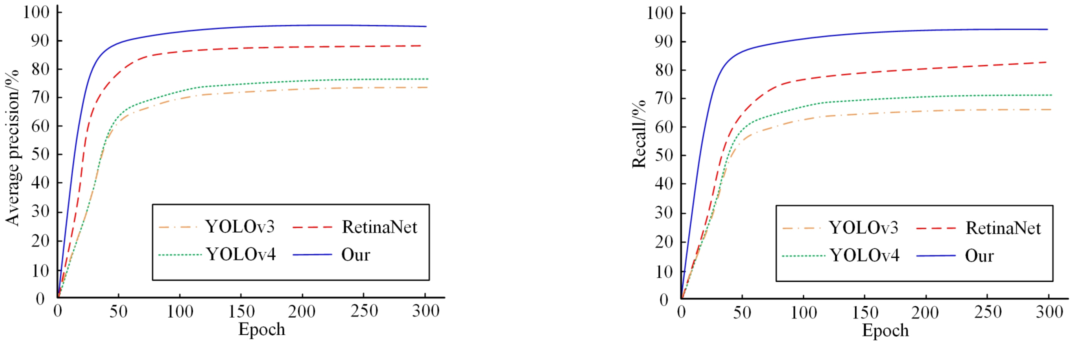


Fig. 9. Detection accuracy curve

The average precision and recall of the suggested model are compared with those of the YOLOv3 model, YOLOv4 model, and RetinaNet model with the goal to confirm the superiority of the suggested spectrum interference detection model. Figure 10 presents the findings. In Figure 10a, the average precision rate of the proposed spectrum interference detection model is the highest with 95.68% compared to the other three models. This is followed by the RetinaNet model and the YOLOv3 model has the lowest average accuracy rate. In Figure 10b, the proposed antisample detection model still outperforms the other three models in the recall metric, with a recall rate of 91.94%. The outcomes displays that the proposed spectrum interference detection model of the study has better interference detection precision and demonstrates certain superiority.



(a) Average precision

(b) Recall

Fig. 10. Comparison of average accuracy and recall of four models

4. Conclusions

Aiming at the environmental threats to the space signals of low-orbit communication satellites, the study constructed an ASDM based on VSE and a spectrum interference detection model based on Fast R-CNN. In the intrusion traffic detection test, the findings showed that the suggested ASDM had the maximum detection accuracy of 97.68% with an F1 value of 96.86%. This was followed by the MLP model with a detection accuracy of 92.51%. In the normal traffic detection task, the proposed ASDM had a detection accuracy of 95.63% and an F1 value of 95.87%. The detection accuracy of the proposed ASDM was 90.16%, 89.65%, 96.84% and 94.62% under four AS generation methods, namely FGSM, BIM, PGD and CW, respectively. Its AUC values in three typical network attacks were above 95%. The proposed spectrum interference detection model had the best detection effect in single tone interference detection. The detection accuracy, recall and evaluation precision were 98.65%, 96.21% and 93.14%, respectively. It converged at about 200 iterations with an average recognition accuracy of 95.47%. The proposed spectrum interference detection model had the highest average precision rate and recall rate of 95.68% and 91.94%, respectively. In summary, the ASDM and spectrum interference detection model built by the research have better detection performance. However, the detection model built by the research can only take relevant measures after being threatened, which has a certain lag. Therefore, in the future research, the satellite environment security should be further predicted to help the development of defense schemes.

References

[1] R. A. D. S. Araujo, L. B. D. Silva, W. A. D. SANTOS, and M. L. D. O. E. Souza. Mitigating interferences on leo satellite downlinks of earth exploration services by cognitive radio, adaptive modulation and coding techniques. *Anais da Academia Brasileira de Ciencias*, 96(suppl 1):e20230487, 2024. https://doi.org/10.1590/0001-3765202420230487.

[2] X. Chen and Z. Luo. Asynchronous interference mitigation for leo multi-satellite cooperative systems. *IEEE Transactions on Wireless Communications*, 23(10):14956–14971, 2024. https://doi.org/10.1109/TWC.2024.3422101.

[3] C. Duan, Y. Li, W. Wang, and J. Li. Leo-based satellite constellation for moving target detection. *Remote Sensing*, 14(2):403, 2022. https://doi.org/10.3390/rs14020403.

[4] R. He, X. Zhang, Q. Cui, and X. Tao. Doppler interference analysis for otfs-based leo satellite system. *IEEE Journal on Selected Areas in Communications*, 43(1):75–89, 2024. https://doi.org/10.1109/JSAC.2024.3460058.

[5] N. Heydarishahreza, T. Han, and N. Ansari. Spectrum sharing and interference management for 6g leo satellite-terrestrial network integration. *IEEE Communications Surveys & Tutorials*:1–1, 2024. https://doi.org/10.1109/COMST.2024.3507019.

[6] C. Li, L. Zhu, and Z. Zhang. For leo satellite networks: intelligent interference sensing and signal reconstruction based on blind separation technology. *China Communications*, 21(2):85–95, 2024. https://doi.org/10.23919/JCC.fa.2023-0371.202402.

[7] S. Meng, M. Jia, Q. Guo, and X. Gu. Inter satellite link interference detection and analysis of ngso satellite system. In *International Conference on Wireless and Satellite Systems*, pages 1–11. Springer, 2021. https://doi.org/10.1007/978-3-030-93398-2_1.

[8] M. J. Murrian, L. Narula, and T. E. Humphreys. Characterizing terrestrial gnss interference from low earth orbit. In *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, pages 3239–3253, 2019. https://doi.org/10.33012/2019.17065.

[9] M. J. Murrian, L. Narula, P. A. Iannucci, S. Budzien, B. W. O'Hanlon, M. L. Psiaki, and T. E. Humphreys. First results from three years of gnss interference monitoring from low earth orbit. *Navigation*, 68(4):673–685, 2021. https://doi.org/10.1002/navi.449.

[10] A. Patil, R. E. Phelts, T. Walter, and S. Thoelert. Detecting and localizing space based interference on gnss signals using machine learning. In *Proceedings of the 2024 International Technical Meeting of The Institute of Navigation*, pages 532–545, 2024. https://doi.org/10.33012/2024.19559.

[11] A. Saifaldawla, F. Ortiz, E. Lagunas, A. B. Adam, and S. Chatzinotas. Genai-based models for ngso satellites interference detection. *IEEE Transactions on Machine Learning in Communications and Networking*, 2:904–924, 2024. https://doi.org/10.1109/TMLCN.2024.3418933.

[12] A. Saifaldawla, F. Ortiz, E. Lagunas, and S. Chatzinotas. Convolutional autoencoders for non-geostationary satellite interference detection. In *2024 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1334–1339. IEEE, 2024. https://doi.org/10.1109/ICCWorkshops59551.2024.10615457.

[13] V. Saiko, V. Nakonechnyi, T. Narytnyk, M. Brailovskyi, and S. Toliupa. Increasing noise immunity between leo satellite radio channels. In *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, pages 442–446. IEEE, 2020. https://doi.org/10.1109/TCSET49122.2020.235471.

[14] S. K. Sharma, S. Chatzinotas, and B. Ottersten. In-line interference mitigation techniques for spectral coexistence of geo and ngeo satellites. *International Journal of Satellite Communications and Networking*, 34(1):11–39, 2016. https://doi.org/10.1002/sat.1090.

[15] J. R. van der Merwe, D. Contreras Franco, J. Hansen, T. Brieger, T. Feigl, F. Ott, D. Jdidi, A. Rügamer, and W. Felber. Low-cost cots gnss interference monitoring, detection, and classification system. *Sensors*, 23(7):3452, 2023. https://doi.org/10.3390/s23073452.

[16] Y. Wang, X. Ding, and G. Zhang. A novel dynamic spectrum-sharing method for geo and leo satellite networks. *IEEE Access*, 8:147895–147906, 2020. https://doi.org/10.1109/ACCESS.2020.3015487.

[17] K.-B. Wu, Y. Morton, S. T. Dittmann, and H. Chang. Gnss signal disturbance detection and classification based on leo satellite measurements. In *Proceedings of the 2024 International Technical Meeting of The Institute of Navigation*, pages 417–425, 2024. https://doi.org/10.33012/2024.19481.

[18] X. Xie, X. Ding, and G. Zhang. Interference mitigation via beamforming for spectrum-sharing leo satellite communication systems. *IEEE Systems Journal*, 17(4):5822–5830, 2023. https://doi.org/10.1109/JSYST.2023.3286117.

[19] T. Yousif, B. Wadsworth, P. Christopher, and P. Blunt. A novel gnss rf interference detection and geolocation algorithm for leo satellites. In *Proceedings of the 37th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2024)*, pages 3375–3389, 2024. https://doi.org/10.33012/2024.19771.

[20] P. Yue, J. An, J. Zhang, J. Ye, G. Pan, S. Wang, P. Xiao, and L. Hanzo. Low earth orbit satellite security and reliability: issues, solutions, and the road ahead. *IEEE Communications Surveys & Tutorials*, 25(3):1604–1652, 2023. https://doi.org/10.1109/COMST.2023.3296160.

[21] L. Zhang, Z. Chen, C. Jiang, and L. Yin. Covert communication in ultra-dense leo satellite systems with interference uncertainty. In *ICC 2024-IEEE International Conference on Communications*, pages 1255–1260. IEEE, 2024. https://doi.org/10.1109/ICC51166.2024.10622920.