With the rapid development of wireless communication, spectrum plays increasingly important role in both military and civilian fields. Spectrum anomaly detection aims at detecting emerging anomaly signals and spectrum usage behavior in the environment, which is indispensable to secure safety and improve spectrum efficiency. However, spectrum anomaly detection faces many difficulties, especially for unauthorized frequency bands. In unauthorized bands, the composition of spectrum is complex and the anomaly usage patterns are unknown in prior. In this paper, a Variational Autoencoder- (VAE-) based method is proposed for spectrum anomaly detection in unauthorized bands. First of all, we theoretically prove that the anomalies in unauthorized bands will introduce Background Noise Enhancement (BNE) effect and Anomaly Signal Disappearance (ASD) effects after VAE reconstruction. Then, we introduce a novel anomaly metric termed as percentile (PER) score, which focuses on capturing the distribution variation of reconstruction error caused by ASD and BNE. In order to verify the effectiveness of our method, we developed an ISM Anomaly Detection (IAD) dataset. The proposed PER score achieves superior performance against different type of anomalies. For QPSK type anomaly, our method increases the recall rate from 80% to 93% while keeping a false alarm rate of 5%. The proposed method is beneficial to broadband spectrum sensing and massive spectrum data processing. The code will be released at git@github.com:QXSLAB/vae_ism_ano.git.

1. Introduction

The rapid development of radio technology has resulted in a greatly enlarged demand for spectrum resources. At the same time, the risk of spectrum interference and malicious use has become increasingly serious. For example, unintentional and intentional interference to positioning service such as Global Navigation Satellite System (GNSS) has significantly increased [1, 2]. Illegal repeaters frequently affect the mobile operator’s cell planning, resulting in poor coverage and dropouts. Reliable spectrum sensing [3, 4] and spectrum anomaly detection are essential approaches to secure spectrum safety, which quickly detect the potentially threatening signal so that it can be eliminated in time.

The research of spectrum anomaly detection can be divided into authorized band anomaly detection and unauthorized band anomaly detection. Authorized bands can only be legally accessed by specific systems. The signal should be detected as anomaly spectrum if it is different from these authorized systems. Thus, authorized band anomaly detection can be well solved by signal identification, which has been well studied in recent years [5–7]. In contrast, unauthorized band anomaly detection is very challenging. In unauthorized bands, wireless systems with different physical layers coexist, which makes the unauthorized spectrum very complex. As a result, it is hard to manually identify the anomaly spectrum patterns. Besides, due to the sporadic nature of spectrum anomalies, it is hard to collect sufficient anomaly samples to train anomaly detection model. Therefore, a complete automatic feature-extracted learning model is highly required to solve this problem.

In this paper, an unsupervised deep learning method is proposed for unauthorized band spectrum anomaly detection. We convert the spectrum data into a two-dimensional spectrogram, and then use Variational Autoencoder (VAE) [8] to capture the probability distribution of spectrogram samples. Based on the theory of optimization inference, we deduced the influence of anomaly signals on VAE reconstruction. On this basis, we propose an anomaly detection metric termed as percentile (PER) score. Finally, we conduct experiments to verify the proposed method. Experimental results show that our method has superior performance for
various types of anomalies. The main contributions of this paper are as follows.

(i) The influence of anomaly signals on VAE output is deduced for the first time. It reveals that anomaly signals will introduce Background Noise Enhancement (BNE) effect and Anomaly Signal Disappearance (ASD) effect. To a certain extent, this solves the problem of insufficient prior knowledge in unlicensed frequency band anomaly detection.

(ii) A novel anomaly detection metric termed as PER score is proposed. It can effectively capture the distribution variation caused by BNE and ASD and solve the anomaly dilution problem faced by traditional anomaly scores when dealing with burst and narrow-band signals.

(iii) An ISM Anomaly Detection (IAD) dataset is developed for the study of spectrum anomaly detection. It considers four different kinds of anomalies. We believe it would foster further research on unlicensed frequency band spectrum anomaly detection.

2. Related Work

Numerous researches have been conducted on spectrum anomaly detection, which can be divided into two categories with respect of their pattern extraction methods. The first kind uses manually patterns designed by experts. Liu et al. [9] converted the spectrum anomaly detection problem to a statistical significance testing problem. They leveraged the property that the received signal power (RSS) decays approximately linearly with the logarithmic distance from the source and detected the unauthorized transmitters by making use of the propagation characteristics. Greenstein et al. [10] made use of the property that transmitters at different locations would lead to different spatial distributions of the RSS and detected anomalies by comparing the current frequency band patterns with a stored spatial map of the transmitter. Yin et al. [11] obtained the historical pattern by calculating the average of seven days’ data. They calculated Mahalanobis distance between measuring spectrum and the historical pattern to detect potential anomalies.

On the other hand, considerable researches leverage data-driven learning methods to extract spectrum patterns. Feng et al. [12] and Rajendran et al. [16] used a deep autoencoder model to perform normal pattern extraction. In their papers, spectrogram was used as the input of the learning model. The anomaly score it used was mean squared error (MSE) between the amplitude across subfrequencies of the true spectrogram and the corresponding reconstructed one. Honghao et al. [13] adopted the idea of classification to detect spectrum anomalies. They used spectrum occupancy sequence as input. Normal and anomaly spectrum patterns were modeled by hidden Markov model (HMM). Therefore, the anomalies can be recognized by computing maximum log-likelihood of the data with respect to each spectrum pattern. O’Shea et al. [14] used a long short-term memory (LSTM)- based recurrent network to train a time series model and to obtain features. Firstly, it computed the difference between predicted value and true value on training set. Then, it modeled the error vector using a parametric multivariate Gaussian distribution. Finally, it computed the likelihood probability in expected error distribution on test set to distinguish anomaly. Li et al. [15] studied spectrum anomaly detection in LTE band. They built deep neural network (DNN) models to capture spectrum usage patterns and computed root mean squared error (RMSE) between the true amplitude across subfrequencies and the model prediction values.

As summarized in Table 1, most of the current researches on spectrum anomaly detection adopted MSE-type anomaly score. It should be noted that likelihood and MSE are equivalent under the premise of Gaussian distribution. The MSE score pays equal attention to every part of the spectrum, which will dilute the impact of anomalies, especially when the anomaly signal duration is short or the bandwidth is narrow. Instead of using global average error, we argue that the spectrum anomaly detection should pay more attention to the reconstruction error of the worst recovered region in the spectrogram. We will theoretically prove this point in next section.

Table 1: Deep learning-based spectrum anomaly detection.

| Pattern extraction model               | Anomaly score |
|----------------------------------------|---------------|
| Feng et al. [12]                       | Deep autoencoder | MSE |
| Honghao et al. [13]                    | Hidden Markov model | Likelihood |
| O’Shea et al. [14]                     | Long short-term memory network | Likelihood |
| Li et al. [15]                         | Long short term memory network | RMSE |

3. Principle

In this section, the VAE method is briefly described. Then, we reinterpret VAE training from the view of generation error minimization and analyze the optimal output of VAE for a given codeword. Finally, based on the property of VAE optimal output, a novel anomaly score is designed for unlicensed spectrum anomaly detection.

3.1. VAE Method. The VAE method is illustrated in Figure 1. The input $X$ is first passed through the Encoder to obtain the posterior probability $p_{\theta}(Z|X)$. Then, the codeword $Z$ is sampled from the posterior probability. At last, the output $\hat{X} = d_{\phi}(Z)$ is reconstructed by the Decoder.

3.2. Optimal Output of VAE. According to the theory of approximate inference [17], the log-likelihood of $X$ can be
expressed as Equation (1). \( \lambda \) represents the number of Monte Carlo samples. \( Y = [y_1, y_2, \ldots, y_p] \) and \( V = [v_1^2, v_2^2, \ldots, v_p^2] \) are the expectation and variance of the codeword, where \( \tau \) represents the dimension of codeword. \( \varphi \) and \( \theta \) are, respectively, the parameters of Encoder and Decoder.

\[
\log p_{\theta, \varphi}(X) = -m(\varphi, X) - \sum_{l=1}^{\lambda} p_{\varphi}(Z_l | X) \cdot \|X - d_\theta(Z_l)\|_2^2,
\]

\[
m(\varphi, X) = \frac{1}{2} \sum_{k=1}^{\tau} \left[ 1 + \log \left(v_k^2 - y_k^2 \right) \right]
\]

The training process of VAE aims to maximize \( \log p_{\theta, \varphi}(X) \) over the training set \( \mathcal{X} \). The objective function of VAE is defined as Equation (3).

\[
E_{X \in \mathcal{X}} \left[ \log p_{\theta, \varphi}(X) \right] = -E_{X \in \mathcal{X}}[m(\varphi, X)]

- E_{X \in \mathcal{X}} \left[ \sum_{l=1}^{\lambda} p_{\varphi}(Z_l | X) \cdot \|X - d_\theta(Z_l)\|_2^2 \right].
\]

The first item in Equation (3) can be viewed as a regularization term, and the second term can be simplified as Equation (4). We define \( g_{\varphi, \theta}(Z) \) as generation error. The physical meaning of generation error can be explained as follows. For certain Encoder output \( Z \), there exist multiple possible inputs \( X' \). Each \( X' \) will introduce a reconstruction error \( \|X' - d_\theta(Z)\|_2^2 \). Generation error represents the expectation of these reconstruction errors.

\[
E_{X \in \mathcal{X}} \left[ \sum_{l=1}^{\lambda} p_{\varphi}(Z_l | X) \cdot \|X - d_\theta(Z_l)\|_2^2 \right] = \sum_{l=1}^{\lambda} p_{\varphi}(Z_l) \cdot \|X - d_\theta(Z_l)\|_2^2,
\]

\[
g_{\varphi, \theta}(Z) = \int p_{\varphi}(X' | Z) \cdot \|X' - d_\theta(Z)\|_2^2 dX'.
\]

As can be seen in Equation (A.1), for a certain codeword \( Z \), VAE training is equivalent to generation error minimization. By differentiating \( g_{\varphi, \theta}(Z) \) with reference to \( d_\theta(Z) \) and letting the derivative equal to 0, the optimal VAE output can be derived as Equation (7). It means that the optimal output of VAE for a given codeword \( Z \) equals to the expectation of possible inputs of \( Z \).

\[
\frac{\partial g_{\varphi, \theta}(Z)}{\partial d_\theta(Z)} = -2 \int p_{\varphi}(X' | Z) \cdot \|X' - d_\theta(Z)\|_2^2 dX' = 0,
\]

\[
d_\theta^*(Z) = \int p_{\varphi}(X' | Z) \cdot X' dX',
\]

3.3. Percentile Score. For a normal spectrogram input \( X^N \), its codeword \( Z^N \) should be located near the center of the posterior probability \( p_{\varphi}(Z | X^N) \), while at the edge of posterior probability \( p_{\varphi}(Z | X'), X' \neq X^N \). Assuming that the prior distribution \( p(X) \) is approximately uniform, Equation (7) can be approximated as Equation (9). As a result, the VAE output approximates the input origin \( X^N \), and the reconstruction error should be small.

\[
p_{\varphi}(X^N | Z^N) \approx p_{\varphi}(X' | Z^N), X' \neq X^N,
\]

\[
d_\theta^*(Z^N) = X^N.
\]

For an anomaly spectrogram input \( X^A \) with anomaly signal \( A \), according to Equation (7), VAE would reconstruct it by weighted summation of normal inputs \( X' \)'s that are distinct from \( X^A \). This will bring about two effects.

(i) Background Noise Enhancement (BNE) Effect. The noise level in the background region of the spectrogram will be raised, since many signals that are presented \( X^A \) but not in \( X^N \) would be superimposed on the reconstructed output

(ii) Anomaly Signal Disappearance (ASD) Effect. The anomaly signal \( A \) would disappear in the reconstruction output, since \( A \) is not presented in \( X^A \).

The BNE effect will cause large reconstruction errors in certain background regions. It will lead to more large outliers in the reconstruction error. As a result, the probability distribution of reconstruction error will have a longer tail, and the percentile will be lifted. In the same way, the ASD effect will increase the percentile of the reconstruction error in the signal region.
On this basis, we propose a percentile (PER) score for anomaly spectrum detection. Different from MSE and MAE scores, PER score focuses on reconstruction errors of badly recovered region in spectrogram. The PER score is shown in Equation (10). We segment the spectrogram $X$ into signal region and background region. The first item represents the $\xi$th percentile of pixel-level reconstruction errors in background region. The second item represents the $\eta$th percentile of pixel-level reconstruction errors in signal region.

$$q_\xi(x)$$ measures the value corresponding to the $\xi\%$ point in the cumulative distribution of scalar $x$. $r_{a_y}(X)$ represent the mask for background region, which is implemented by a max-pooling function with kernel size of $y$ and a step activation with threshold of $a$. $1 - r_{a_y}(X)$ represents the mask for signal region. $f_\gamma$ represents min-pooling function with kernel size $\gamma$ and is used to reliably detect the noise floor variation. Symbol $\circ$ is used to represent Hadamard product between matrices. $\| \|$ represents pixel-level absolute value operation. The definition of operator $q_\xi, f_\gamma,$ and $r_{a_y}$ are shown in see the appendix.

$$\text{PER}(X, \hat{X}) = \beta \cdot q_\xi \left( f_\gamma (|X - \hat{X}|) \circ r_{a_y}(X) \right) + q_\eta \left( f_\gamma (|X - \hat{X}|) \circ \left[ 1 - r_{a_y}(X) \right] \right). \quad (10)$$

In Equation (10), $\alpha, \beta, \gamma, \xi,$ and $\eta$ are hyperparameters and can be tuned according to application scenarios. In this paper, the kernel size $\gamma$ of max-pooling and min-pooling function is set to 3. In order to balance the difference in the absolute value of the reconstruction error between the signal region and the background, the weight of background error percentile is set to 2. The threshold of step activation is set to 0.05. The percentage parameters $\xi$ and $\eta$ are, respectively, set as 90 and 99.

4. Experimental Results

4.1. Dataset. In order to verify the effectiveness of our method, we developed a dataset for ISM frequency band anomaly detection, termed as ISM Anomaly Detection (IAD) dataset. Similar to the approaches taken in the literature [12, 14, 16, 18], we collect ISM spectrum data in the laboratory environment as normal spectrogram samples and construct anomaly spectrogram samples by artificially sending specific types of signals to the environment. The experiment setup for data acquisition is shown in Figure 2. Two Universal Software Radio Peripherals (USRPs) are, respectively, used as transmitter and receiver. Both USRPs use the VERT2450 omnidirectional antenna. The receiver USRP is used to collect spectrum data. The center frequency is set to be 2.432 GHz and the bandwidth is set to be 20 MHz. The receiving frequency band includes WiFi and Bluetooth signals. The duration of each acquisition is set to 100 ms. The collected I/Q data is transformed into spectrogram with size of $256 \times 256$ by Short-Time Fourier Transform (STFT). Then, the spectrogram is down-sampled with a factor of 4. The final size of spectrogram sample is $64 \times 64$. The transmitter USRP is used to send anomaly signal to the environment. Anomaly signal with four different types of modulations are considered, namely QPSK, 16QAM, GMSK, and CHIRP. The signal bandwidth varies randomly from 1 MHz to 5 MHz, and the transmission duration is 20 ms. The frequency tuning speed of the CHIRP signal is 20 KHz per second. The transmitter USRP is turned on during anomaly spectrogram sample collection, and it is turned off when collecting normal spectrogram samples. Examples of the normal and anomaly spectrogram samples are shown in Figure 3.

The normal spectrogram samples are randomly split into two parts. The first part contains 4388 samples and is used to construct training set $\%$. The second part is used to construct test sets. In order to evaluate the performance of
anomaly scores against different anomalous signals, we constructed four test sets. The constitution of different test sets is shown in Table 2. For example, Testset 1 contains 788 normal spectrogram samples and 774 anomaly spectrogram samples with QPSK signal. Testset 1, Testset 2, Testset 3, and Testset 4 are, respectively, used to evaluate the detection ability for QPSK type, 16QAM type, GMSK type, and CHIRP type anomalies.

| SetNumber | Type | Normal | QPSK | 16QAM | GMSK | CHIRP |
|-----------|------|--------|------|-------|------|-------|
| Testset 1 |      | 788    | 774  | 0     | 0    | 0     |
| Testset 2 |      | 788    | 0    | 774   | 0    | 0     |
| Testset 3 |      | 788    | 0    | 0     | 774  | 0     |
| Testset 4 |      | 788    | 0    | 0     | 0    | 774   |

Table 2: Constitution of different test sets.

4.2. VAE Network. In our study, two different VAE networks are adopted to investigate the performance of proposed PER anomaly detection score. The first is Convolutional VAE (Conv-VAE) network. The architecture of Conv-VAE network is shown in Figure 4(a). It uses convolution operation to extract hierarchical features from the original spectrogram, then uses dense layers to generate codeword at the bottleneck, and finally uses transposed convolution (ConvT) to gradually restore the spectrogram. Each feature map consists of C planes. Each plane is with shape of $H \times W$ and represents the prominence of a certain feature on two-dimensional time-frequency plane, where $H$ and $W$ represent the scale of time and frequency dimensions. The second is Fully Connected VAE (FC-VAE) network. Its architecture is shown in Figure 4(b). In FC-VAE network, the 2-dimensional (2D) original spectrogram sample is firstly reshaped into 1-dimensional (1D) feature. Then, dense layers are used for feature compression and recovery. At last, the recovered 1D feature is reshaped to generate a spectrogram with the same size as the input. Both VAE networks are implemented in PyTorch and are trained by only normal samples in an unsupervised approach. We use Adam optimizer with a learning rate of $10^{-4}$. The batch size is set to be 64.

4.3. Results. After training, the input and output of Conv-VAE network on Testset 1 are shown in Figure 3. The results are similar for FC-VAE network and Testset 2, Testset 3, and Testset 4. The first and second rows are the input and output of Conv-VAE network. As can be seen, for anomaly spectrogram samples, QPSK-modulated anomaly signals are disappeared in the reconstructed output. At the same time, the background noise floor of the anomaly spectrogram has been risen. The third row represents the mask used to filter signal region in spectrogram. The fourth and fifth rows are the reconstruction errors in signal region and background. The results confirm that spectrogram anomalies indeed cause ASD and BNE effects.

The distribution of pixel reconstruction errors is shown in Figure 5(a). The ASD and BNE effects cause large pixel reconstruction errors. Compared with normal spectrogram, the probability distribution of the pixel reconstruction error for the anomaly spectrogram has a longer tail. As a result, anomaly spectrogram samples have larger reconstruction
error percentiles than normal spectrogram samples. 99th percentiles of signal reconstruction error are illustrated in Figure 5(b).

The performance of PER score is evaluated by Receiver Operating Characteristic (ROC) test. ROC curve examines the variation of true positive rate (TPR) with false positive rate (FPR). TPR equals the ratio of anomaly samples that are detected as anomaly. It represents the recall rate of all anomaly samples and reflects the level of missed detection. FPR equals the ratio of normal samples that are detected as anomaly, which is the false alarm rate. The Area Under Curve (AUC) metric measures the area under ROC curve and reflects the performance of the anomaly detection. AUC closer to 1 indicates better detection performance.

We compare PER score with traditional anomaly scores in Figure 6. Conv-VAE network and Testset 1 are used here. MSE and MSE score are defined in Equation (A.9) and Equation (A.8). In addition, we take the codeword from Conv-VAE network as the input feature and use Local Outlier Factor (LOF) [19], One Class SVM (OCS) [20], Elliptic Envelope (EE) [21], and Isolation Forest (IF) [22] methods for spectrogram anomaly detection. These methods are commonly used to detect anomalies in low dimensional data in the field of machine learning [23]. As can be seen, the proposed PER score achieves higher anomaly detection performance under same false alarm rates. Compared with the MSE score, the PER score increases the recall rate from 80% to 93% when the false alarm rate equals 5%.

We further compare the detection performance of PER score against different anomaly signals. The results are shown in Table 3. For all anomaly types, the PER score
achieves the highest detection performance. When the
abnormal type is GMSK, the improvement brought by the
PER score is relatively small. We guess this is because there
is a GMSK-modulated Bluetooth signal in the observation
frequency band, which makes it more difficult to detect
GMSK anomaly.
Finally, we study the dependence of the detection ability on network architecture. We perform experiments on the FC-VAE network, and the experimental results are shown in Table 4. As can be seen, PER score outperforms all other methods.

### Appendix

#### A. Derivation of Generation Error

The detailed derivation of Equation (4) is shown in Equation (A.1).

\[
E_{\text{EX}} \left[ \sum_{l=1}^{L} p_{\phi}(Z_l | X) \cdot \|X - d_{\theta}(Z_l)\|_2^2 \right] = \int p(X) \cdot \sum_{l=1}^{L} p_{\phi}(Z_l | X) \cdot \|X - d_{\theta}(Z_l)\|_2^2 \, dX \\
= \sum_{l=1}^{L} \int p(X) \cdot p_{\phi}(Z_l | X) \cdot \|X - d_{\theta}(Z_l)\|_2^2 \, dX \\
= \sum_{l=1}^{L} \int p_{\phi}(Z_l, X) \cdot \|X - d_{\theta}(Z_l)\|_2^2 \, dX \tag{A.1} \\
= \sum_{l=1}^{L} p_{\phi}(Z_l) \cdot g_{\phi, \theta}(Z_l) \\
= \sum_{l=1}^{L} p_{\phi}(Z_l) \cdot \sum_{i,j} g_{\phi, \theta}(x_{ij})
\]

The definition of percentile operator \(q_{\xi}\), min-pooling operator \(f_{\gamma}\), and max-pooling operator \(r_{\alpha, \gamma}\) are shown in Equation (A.4), Equation (A.2), and Equation (A.7). We use \(\odot\) to denote compound mapping. \(x_{ij}\) represents the pixel value at \(i\)th row and \(j\)th column in \(X\).

### 5. Conclusions

In this paper, an unsupervised deep learning method is proposed for unsupervised spectrum anomaly detection in unauthorized bands, which leverages VAE to capture the spectrum data distribution and detects anomalies by selectively comparing the difference between spectrogram and its VAE reconstruction counterparts. We have theoretically proved and experimentally verified that the anomaly spectrum usage will introduce Background Noise Enhancement (BNE) effect and Anomaly Signal Disappearance (ASD) effect. On this basis, the PER score is proposed for spectrum anomaly detection, which focuses on capturing the distribution changes of pixel reconstruction errors caused by ASD and BNE effects. The experimental results show that PER score achieves the superior detection performance against different anomaly signals at ISM band. For QPSK-type anomalies, the PER score increases the recall rate from 80% to 93% while keeping a false alarm rate of 5%. The proposed anomaly detection method is beneficial to guide spectrum sensing system to quickly filter out the high-value information from a large amount of spectrum data and automatically invest more computing and storing resources for time-frequency window containing threatening signals.

Future research should consider how to transfer the anomaly detection model between different scenarios. This will enable the spectrum anomaly detection model to be quickly deployed to unfamiliar scenes. Few-shot learning and transfer learning may play an important role in this topic. At the same time, a multiscenario spectrum anomaly detection dataset should be developed.
\[ f_y(X) = \begin{cases} \min_{m \in \mathbb{Z}} \max_{n \in \mathbb{Z}} \left( x_{i+m,j+n} \right) & X_{i,j} \in X \end{cases} \] (A.2)

\[ h_y(X) = \begin{cases} \max_{m \in \mathbb{Z}} \min_{n \in \mathbb{Z}} \left( x_{i+m,j+n} \right) & X_{i,j} \in X \end{cases} \] (A.3)

\[ q_{\xi}(X) = \arg\min_{\epsilon} \left| p_{\xi,\epsilon}(x_i < \epsilon) = \xi/100 \right| \] (A.4)

\[ \omega_a(X) = \left\{ \begin{array}{cl} u(a - x_{ij}) | x_{ij} \in X, \\ 1, & x \geq 0 \\ 0, & \text{else} \end{array} \right. \] (A.5)

\[ r_{a,j}(X) = \omega_a \odot h_{a,j}(X). \] (A.7)

The definitions of MAE and MSE are shown in Equation (A.8) and Equation (A.9). X and \( \bar{X} \) are original input and reconstructed output. Operator \( \| \cdot \|_1 \) and \( \| \cdot \|_2 \) represent 1-norm and 2-norm of matrix.

\[ \text{MAE}(X, \bar{X}) = \|X - \bar{X}\|_1, \] (A.8)

\[ \text{MSE}(X, \bar{X}) = \|X - \bar{X}\|_2^2. \] (A.9)

**Data Availability**

The data and code used to support the findings of this study have been deposited in the git@github.com:QXSLAB/vae_ism_ano.git repository.

**Additional Points**

**Notation.** Capital letters such as \( X, \bar{X} \), and \( Z \) are used to denote matrices or vectors. Hollow capital letters such as \( \bar{X} \) are used to represent data distribution. Lowercase letters such as \( x, k, \text{ and } l \) are used to denote scalar values. Bold lowercase letters such as \( p, q, g, \) and \( d \) are used to represent functions. Lowercase Greek letters such as \( \alpha, \beta, \gamma \) are scalars, which denote the hyperparameters of neural network. Bold lowercase Greek letters such as \( \varphi \) and \( \theta \) represent the weight and bias terms in neural networks.

**Conflicts of Interest**

The authors declare that there is no conflict of interests.

**Authors’ Contributions**

Yu Tian and Haihuia Liao contributed equally to this work.

**Acknowledgments**

We would like to thank all authors for their work in theoretical analysis, experimental verification, and manuscript drafting and revision. The details of contributions of authors are listed as follows. Dr. Yu Tian accomplished the theoretical derivation of PER score, the code development of deep learning model, the statistical analysis of experimental results, and drafting of the manuscript. Haihuia Liao accomplished the setup of the experimental platform and the development of IAD dataset. Jing Xu accomplished the investigation of related works. Ya Wang and Shuai Yuan participated in data processing and manuscript revision.

Professor Naijin Liu provided the equipment needed for real-world case study. Haihua Liu accomplished the setup of the experimental platform and the development of IAD dataset. Jing Xu accomplished the statistical analysis of experimental results, and drafting of the manuscript. The IAD dataset will be released at git@github.com:QXSLAB/vae_ism_ano.git. We hope it would foster further research on unlicensed frequency band spectrum anomaly detection.

**References**

[1] S. Thombre, M. Z. H. Bhuiyan, P. Eliardsson et al., “Gnss threat monitoring and reporting: past, present, and a proposed future,” The Journal of Navigation, vol. 71, no. 3, pp. 513–529, 2018.

[2] M. Strohmeier, “On perception and reality in wireless air traffic communication security,” IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 6, pp. 1338–1357, 2016.

[3] I. Dey, D. Ciuonzo, and P. S. Rossi, “Wideband collaborative spectrum sensing using massive MIMO decision fusion,” IEEE Transactions on Wireless Communications, vol. 19, no. 8, pp. 5246–5260, 2020.

[4] P. S. Rossi, D. Ciuonzo, and G. Romano, “Orthogonality and cooperation in collaborative spectrum sensing through mimo decision fusion,” IEEE Transactions on Wireless Communications, vol. 12, no. 11, pp. 5826–5836, 2013.

[5] C. Salcedo Coloma and A. Garcia Armada, “Signal detection and identification for OFDM cognitive radio,” [M.S. thesis.], Universidad Carlos III de Madrid, 2010.

[6] A. Ebrahimzadeh and S. A. Seyedin, “Digital signal types identification using a hierarchical SVM-based classifier and efficient features,” in 2007 International Conference on Computing: Theory and Applications (ICCTA’07), pp. 521–525, Kolkata, India, 2007.

[7] A. Gorcin and H. Arslan, “Template matching for signal identification in cognitive radio systems,” in MILCOM 2012 - 2012 IEEE Military Communications Conference, pp. 1–6, Orlando, FL, USA, 2012.

[8] D. P. Kingma and M. Welling, “Auto-encoding variational bayes,” 2013, https://arxiv.org/abs/1312.6114.

[9] S. Liu, Y. Chen, W. Trappe, and L. J. Greenstein, “Aldo: An anomaly detection framework for dynamic spectrum access networks,” in IEEE INFOCOM 2009, pp. 675–683, Rio de Janeiro, Brazil, 2009.

[10] S. Liu, L. J. Greenstein, W. Trappe, and Y. Chen, “Detecting anomalous spectrum usage in dynamic spectrum access networks,” Ad Hoc Networks, vol. 10, no. 5, pp. 831–844, 2012.

[11] S. Yin, S. Li, and J. Yin, “Temporal-spectral data mining in anomaly detection for spectrum monitoring,” in 2009 5th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1–5, Beijing, China, 2009.
Q. Feng, Y. Zhang, C. Li, Z. Dou, and J. Wang, "Anomaly detection of spectrum in wireless communication via deep auto-encoders," *The Journal of Supercomputing*, vol. 73, no. 7, pp. 3161–3178, 2017.

W. Honghao, J. Yunfeng, and W. Lei, "Spectrum anomalies autonomous detection in cognitive radio using hidden Markov models," in *2015 IEEE advanced information technology, electronic and automation control conference (IAEAC)*, pp. 388–392, Chongqing, China, 2015.

T. J. O’Shea, T. C. Clancy, and R. W. McGwier, "Recurrent neural radio anomaly detection," 2016, https://arxiv.org/abs/1611.00301.

Z. Li, Z. Xiao, B. Wang, B. Y. Zhao, and H. Zheng, “Scaling deep learning models for spectrum anomaly detection,” in *Proceedings of the Twentieth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 291–300, Catania, Italy, 2019.

S. Rajendran, W. Meert, V. Lenders, and S. Pollin, “Unsupervised wireless spectrum anomaly detection with interpretable features,” *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 3, pp. 637–647, 2019.

I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*, MIT press, 2016.

S. Rajendran, V. Lenders, W. Meert, and S. Pollin, "Crowd-sourced wireless spectrum anomaly detection," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 2, pp. 694–703, 2020.

M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "LOF: identifying density-based local outliers," in *Proceedings of the 2000 ACM SIGMOD international conference on Management of data*, pp. 93–104, Dallas Texas, USA, 2000.

B. Schölkopf, R. C. Williamson, A. J. Smola, J. Shawe-Taylor, and J. C. Platt, "Support vector method for novelty detection," in *NIPS*, vol. 12, pp. 582–588, Citeseer, 1999.

P. J. Rousseeuw and K. V. Driessen, "A fast algorithm for the minimum covariance determinant estimator," *Technometrics*, vol. 41, no. 3, pp. 212–223, 1999.

F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation-based anomaly detection," *ACM Transactions on Knowledge Discovery from Data (TKDD)*, vol. 6, no. 1, pp. 1–39, 2012.

A. Gramfort and A. Thomas, "Comparing anomaly detection algorithms for outlier detection on toy datasets," *scikit-learn 0.20*, vol. 3, pp. 2–5, 2019.