AE-BiLSTM: Multivariate Time-Series EMI Anomaly Detection in 5G-R High-Speed Rail Wireless Communications

Yejing Fan, Li Zhang, Kang Li
School of Electronic and Electrical Engineering
University of Leeds
Leeds, United Kingdom
Email: el17yf@leeds.ac.uk, L.X.Zhang@leeds.ac.uk, K.Li1@leeds.ac.uk

***Abstract*—With the global expansion of high-speed rail (HSR) and the integration of the latest wireless communication networks into the railway system, establishing a secure bidirectional communication link between moving trains and base stations (BSs) is vital to ensure real-time control. The increasing complexity of contemporary railway systems and heightened exposure to electromagnetic interference (EMI) have led to operational disruptions and security risks. This paper introduces a real-time anomaly detection approach that utilizes a deep learning algorithm based on autoencoder (AE) and long short-term memory (LSTM). By analyzing multivariate time series characteristics, the method simultaneously examines the time and frequency domains at a finer resolution, achieving a desirable trade-off between false alarms and missed anomalies. Specifically, our approach enhances accuracy by 5%, reaching 93.24% in comparison with some state-of-the-art methods. The online detection takes 4.51 ms, meeting the security latency requirements. This highlights the potential for timely detection of unforeseen EMI incidents in diverse scenarios and at varying speeds.**

***Index Terms*—Anomaly Detection, Electromagnetic Interference, Deep Learning, High-Speed Rail Wireless Communications**

I. Introduction

The growth of High-Speed Rail (HSR) networks has profoundly improved passenger mobility. Maintaining a reliable connection between moving trains and base stations (BS) is essential for continuous data transmission with high uplink/downlink data rates and low latency [1]. Wireless networks are especially susceptible to electromagnetic interference (EMI) compared to other security threats such as eavesdropping and data fabrication [2]. Compared to other layers, the physical layer provides increased opportunities for attacks [3]. The European Project SECRET has been initiated to investigate electromagnetic risks and threats related to the railway environment [4]. The evolution of the Global System for Mobile Communications-Railway (GSM-R) to 5G-Railway (5G-R) has introduced digitized and automated services in alignment with the reliability, availability, maintenance and safety standards and specifications (RAMS) established by the International Union of Railways (UIC) [5]. Security is emerging as a big concern for the 5G-R system. Intentional EMI (IEMI) is perceived as an unpredictable threat in contemporary railway systems. Often referred to as radio jamming attacks, these interferences are closely associated with acts of terrorism and crime. Moreover, the growing complexity of the electrified railway system has raised concerns about its increased susceptibility to various EMIs [6]. Electromagnetic signals superimposed on the communication signals at the receiver side can lead to malfunctions of sensors and signaling systems, compromise the effectiveness of automatic train protection (ATP) systems, and cause errors within the radio module system, resulting in emergency braking events and potential accidents. Given the growing reliance on wireless communications, prioritizing research on anomaly detection is vital to ensure the safety of both trains and passengers against potential security attacks.

EMI can arise from natural phenomena or onboard train equipment, including lighting, relays, electric motors, and digital systems. The increasing prevalence of small and inconspicuous communication devices in the general public has increased the risk of disruptions to critical systems [7]. Four typical EMI classes affecting signal transmission in HSR are modeled [8], including transient EMI, EMI from power electronics, permanent EMI, and intentional EMI from artificial noise. Regarding IEMI, depending on its attacking strategy, jamming attacks that specifically target the Physical Layer can be classified into four types: constant jammers, periodic jammers, random jammers, and reactive jammers [2], [9]. Constant and periodic jammers continuously occupy the frequency band by producing interference signals continuously. Random jammers follow an unpredictable transmission pattern, sending jamming signals for a random duration and then turning to sleep for the rest of the time, resulting in a decreased probability of detection. The reactive jammer is unique compared to the other three active jammers. It employs a smarter and more power-efficient approach and can detect the communication channel to update its attack strategies. Therefore, manual labeling of an entire dataset for training detection and classification models is impractical, especially when normal samples significantly outnumber abnormal ones. It is imperative to devise real-time anomaly detection methods.

EMI detection methods, such as statistical approaches, have limitations in assessing multiple indicators simultaneously [10]. Recent detection techniques have employed different machine learning models, e.g., CNN [11] and SVM [12]. While the model exhibits fast data processing capabilities, their focus is limited to analyzing the spectrum solely in the frequency domain. Furthermore, they fail to address time-series features posed by dynamic HSR scenarios, including rural, cuttings, viaducts, and tunnels, which exert notable influences on signal propagation characteristics. These models neglect the time-frequency characteristics that are subject to variations in diverse and dynamic HSR scenarios, undermining their effectiveness for real-time detection.

This paper addresses the underexplored area of anomaly detection in wireless communications for HSR scenarios. We propose the multivariate time-series anomaly detection leveraging deep learning methods, specifically Long Short-Term Memory (LSTM) and Autoencoder (AE) [13], which are useful for learning long-range dependencies and effective for detecting anomalies related to unpredictable EMIs. The system model is devised for the HSR scenario, where downlink signals are captured by an onboard antenna, susceptible to potential wireless threats. The method demonstrates the effectiveness in detecting both typical and unknown EMIs by learning an extensive training dataset collected from diverse dynamic scenarios without interference. Moreover, the implementation of real-time EMI anomaly detection will instigate a fast and appropriate reaction to the threat, enhancing the efficacy of mitigation and jamming-resistance strategies [9]. The main contributions of this paper are summarized below:

- In the data pre-processing phase, multivariate features are simultaneously extracted and analyzed for time-frequency domains with finer resolution.
- Utilizing a AE-BiLSTM deep learning algorithm tailored for time-series characteristics, the system achieves real-time anomaly detection for EMI in various scenarios.
- The analysis framework can be scaled to various wireless communications in electrified transportation systems.

The rest of the paper is organized as follows. Section II gives an overview of the system model. Section III presents the AE-BiLSTM anomaly detection algorithm. Simulation results are discussed in Section IV, with the conclusion in Section V.

II. System Model

A. Overview of railway wireless communication scenarios

The high-speed train is approaching and moving away from the BS. Due to the varying distances between the train and the BS, a dynamic system model is necessary to address the rapid movement of the train and the realistic propagation of signals. The Rician fading channel model is characterized by a dominant line-of-sight (LOS) component and multiple scattered paths, making it especially suitable for dynamic landscapes such as viaducts, rural areas, cuttings, and tunnels.

$$P_r = A_1\sqrt{\frac{K}{K+1}}\cdot(P_t - PL(d_1)) + \sum_{i=2}^{N} A_i\sqrt{\frac{1}{K+1}}\cdot(P_t - PL(d_i)) \tag{1}$$

where, P_r and P_t represent the overall received signal power and BS transmitted signal power, covering both LOS and Non-Line-of-Sight (NLOS) components. The variables A_1 and K are the amplitude of the LoS component and Rician K-factor, respectively. N is the number of multipath components, and A_i is the amplitude of the i_{th} multipath component. $PL(d)$ represents the path loss at distance d, and employs the logarithmic distance model to address signal weakening over large distances [5].

$$PL(d) = PL(d_0) + 10n\log_{10}\left(\frac{d}{d_0}\right) \tag{2}$$

where, $PL(d_0)$ represents the path loss at the reference distance d_0, n is the path loss exponent, and d is the distance between BS and antenna. In Equation (1), d_1 corresponds to the first path and d_i corresponds to the NLOS paths.

The Doppler shift effect is a frequency shift in the received antenna signal caused by the train's movement relative to the BS, commonly encountered in HSR scenarios.

$$f_d = \frac{v\cdot f_c}{c} \tag{3}$$

where, f_d denotes the Doppler shift, v is the velocity between the BS and the antenna, f_c is the carrier frequency of the transmitted signal from the BS, and c is the speed of light. This equation characterizes the maximum shift when the relative direction of the train to the transmitted signal is parallel, that is, when the angle θ is 0. This simplifies the system model without necessitating intricate geometric details or angles.

B. Flowchart of the overall framework

Fig.1 depicts the framework, comprising offline training and online detection. The deep learning model undergoes unsupervised learning using the training data in normal conditions. After that, during online detection, the newly received real-time signal is fed to the well-trained model to calculate the reconstruction loss and detect the presence of EMIs.

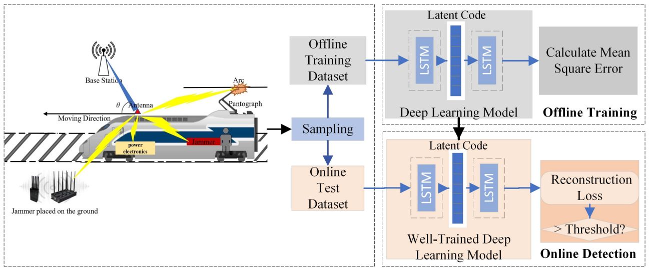

Fig. 1. Flowchart of the overall framework

In the HSR wireless communication scenarios, there are many potential attacks, including transient EMI from pantograph-catenary arcing, onboard power electronics EMI, and IEMI at two different locations: originating from a portable device in a passenger's pocket within the train and originating from a power source positioned on the ground between the BSs [8]. The macro BS operates at 1.9 GHz, transmitting signals to a train antenna receiver mounted on the train roof. The chosen frequency band aligns with the latency and reliability requirements of the 5G NR-based Future Railway Mobile Communication System (FRMCS) [14].

III. AE-BiLSTM Anomaly Detection Algorithm

A. Data Preprocessing

The procedure for extracting multivariate time series data is depicted in Fig. 2.

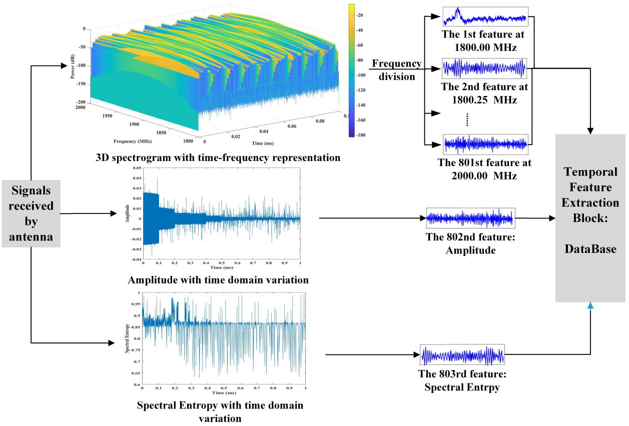
Power (dB)
Frequency (MHz)
Time (ms)
3D spectrogram with time-frequency representation
Frequency division
The 1st feature at 1800.00 MHz
The 2nd feature at 1800.25 MHz
The 801st feature at 2000.00 MHz
Signals received by antenna
Amplitude
Time (ms)
Amplitude with time domain variation
The 802nd feature: Amplitude
Temporal Feature Extraction Block:
DataBase
Spectral Entropy
Time (ms)
Spectral Entropy with time domain variation
The 803rd feature: Spectral Entrpy

Fig. 2. Flowchart of the multivariate time-series feature extraction

The initial set of time-series features captures the frequency variations over time. In signal analysis, a shorter window with superior time resolution is generally preferred for real-time detection, whereas a longer window with enhanced frequency resolution is more adept at distinguishing between different frequency components in the signal. Striking a balance between fine-time resolution and fine-frequency resolution is crucial, as achieving both simultaneously is impractical. In this study, we segment the frequency band into smaller subbands and conduct spectral analysis for each subband using a shorter window. This time-frequency decomposition approach enables simultaneous analysis of time and frequency information with finer resolution. Specifically, power levels are computed based on 3D time-frequency spectrograms, considering the variance across 801 frequency points ranging from 1800 to 2000 MHz, with a frequency resolution of 250 KHz. Combining results from all subbands creates a comprehensive time-frequency representation of the entire signal sequence, providing detailed insights into both frequency and time domain characteristics across a broad frequency range.

The second set of time-series features illustrates the amplitude variations in the signals received by the antenna, stemming from the dynamic train movement. The third set of time series features is linked to spectral entropy, a concept derived from Shannon information theory that gauges the uncertainty and randomness of signal power distributed across different frequencies.

In total, 803 multivariate time series features are obtained and subsequently input into the deep-learning network. The duration of the entire time is evenly divided for each time window length τ for anomaly detection.

B. Auto-encoder (AE) basis

AE is a type of unsupervised neural network used to learn latent representations by reconstructing input data. It consists of an encoder network that transforms the input into a lower-dimensional representation known as latent code and a decoder network that reconstructs the original input as shown in Fig. 3 [13]. After training, When interference is introduced to the spectra, communication will be significantly impacted. Identifying anomalies is possible by comparing reconstruction errors to a predefined threshold due to the changes in the signal spectra received by the antenna. AE is useful for anomaly detection, especially when dealing with unforeseen abnormal data [15].

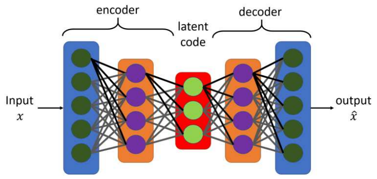

Fig. 3. Illustration of an AE architecture

C. Long short-term memory (LSTM) basis

The LSTM network represents an enhanced version of recurrent neural networks (RNNs) designed to overcome challenges related to vanishing and exploding gradients [16], [17]. This improvement is achieved through the incorporation of forgotten gates, input gates, and output gates shown in Fig. 4, which significantly enhance the network's ability to selectively retain important information while discarding irrelevant information. In the context of 5G-R signal detection, particularly when dealing with a carrier frequency of 1.9GHz, the task becomes challenging. To address this, a practical sampling frequency of 5GHz is employed, aligning with Nyquist theory requirements. Given the need to process long time-series data within the signal detection window duration τ, the LSTM network is seamlessly integrated into our algorithm to effectively capture features based on long-range dependencies.

D. AE-BiLSTM Anomaly Detection Algorithm Structure

The structure of the AE-BiLSTM anomaly detection algorithm, as illustrated in Fig. 5, includes both the encoder and decoder, each comprising two BiLSTM layers. These layers capture temporal dependencies bidirectionally by incorporating LSTM. The BiLSTM layer is pivotal, facilitating the

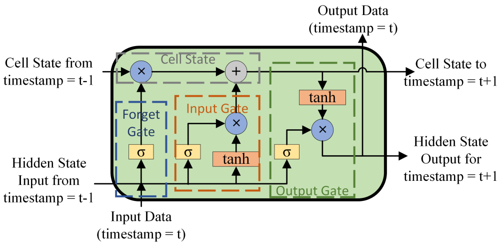

Fig. 4. Illustration of an LSTM cell

integration of forward and backward information flow within the LSTM layers at each time step. In the encoding phase, utilizing both forward and backward LSTM layers, the encoder transforms the input data X into a latent code y. Conversely, the decoder's role is to reconstruct the input from the latent representation y back into the original data space, generating an output denoted as $\hat{X}$. The loss function for the decoder involves calculating the mean squared error (MSE) using the formula (6), quantifying the discrepancy between the input and the reconstructed output. During this unsupervised training process, the objective is to minimize the reconstruction error, enabling the model to learn accurate reconstruction of normal data. This approach equips the model to precisely reconstruct inputs, closely mirroring the inherent trends of the signal without relying on labeled data.

After completing training, the detector can compute the loss of reconstruction, which measures the deviation between the test signal and its reconstruction. It identifies a signal as anomalous when the reconstruction error exceeds the specified threshold. Consequently, the detector can flag anomalies whenever the patterns deviate from the learned normal patterns. The EMI detection approach proposed in this paper is set to find abnormal signals in a duration τ of 100 µs. In other words, the detector can determine whether the train communication network is tolerant to incoming EMI and consider the signal in the time window as anomalous.

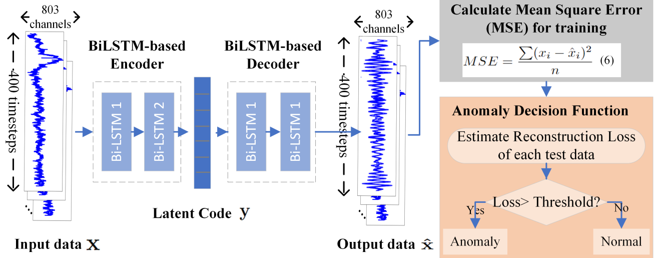

Fig. 5. Flowchart of the AE-BiLSTM Anomaly Detection Algorithm

IV. Simulation Results and Analysis

The model of the HSR wireless communication system, incorporating Rician fading, Doppler shift, path loss, and ambient noise, offers a realistic framework to assess anomaly detection systems in dynamic scenarios. Data is gathered as the train approaches and departs from the BS at varying speeds. The distance between the train and the BS ranges from 100 to a maximum of 2500 meters, all within the coverage range of a single BS. In the simulation, three different train speeds (250, 350, 450 km/h) and four typical HSR scenarios featured by different Rician fading K-factors and path loss exponents are considered. Parameters are shown in TABLE I [18], [19]. The ambient noise model AWGN with SNR 20 dB. The simulations are performed with a detection sampling interval of 100 µs every 1 second, covering a 20-second duration of train operation. The encoder consists of layers with 64 and 32 units, while the decoder mirrors this structure. Training involves a maximum of 100 epochs with a batch size of 32, utilizing the Adam optimizer with a learning rate of 0.001. A dataset without EMI, totaling 1920 samples, is gathered and subsequently divided into an 80% training set and a 20% testing set.

TABLE I
Simulation Parameters for Four Different Scenarios

Parameter	Rural	Viaduct	Tunnel	Cutting
Rician K-Factor	6	3.66	2.33	1.88
Path Loss Exponent n	2.53	3.5	4.5	4.3
Maximum Doppler Shift	792 Hz	792 Hz	792 Hz	792 Hz

A. *Anomaly Decision Threshold*

After training the model with unsupervised learning, the proposed detector reconstructs each signal on normal conditions and computes a reconstruction loss. Using a threshold of a maximum loss of 2.2001×10^{-6}, the detector categorizes any test signal exceeding this limit as anomalous. This criterion ensures heightened sensitivity to deviations from learned normal scenarios, enhancing its capability to flag potential anomalies in real-world scenarios.

B. *Test with Typical EMI Models*

In this paper, two typical time-varying IEMIs are investigated and presented as follows for the testing phase.

a) Frequency sweeping IEMI: Typically, 5G-R wireless communications offer multiple channels and frequency bands. To overcome hardware limitations, a low-cost jammer employs frequency-sweeping jamming attacks, exploiting a broad frequency range with high ADC sampling rates and broadband power amplifiers [2]. This jamming technique involves transmitting continuous high-power noise that sweeps across channels, repeating the process over time [6]. The jammer can be represented as a cosine wave with a random amplitude A sweeping over a frequency band $[f1, f2]$ within a period T. In this model, the interference signal sweeps frequencies around [1800,2000] MHz for 10 µs as depicted in Fig. 6. The intentional design of this jammer aims to disrupt the 1900 MHz frequency band of 5G-R.

b) Transient IEMI: Transient EMI pertains to brief electromagnetic disturbances within the radio frequency spectrum, stemming from various sources during train operation such as pantograph-catenary arcing, lightning strikes, and onboard

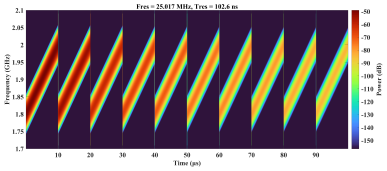

Fig. 6. Time-frequency representation of the frequency-sweeping interference

power electronic equipment, among others [20]. Transient IEMI intentionally mimics the damped sinusoidal signal characteristics of transient EMI to disrupt wireless communication systems.

$$V_{trans(t)} = A\left(e^{\frac{-t}{t_{rise}}} - e^{\frac{-t}{t_{hold}}}\right) \cdot sin(2\pi f_c t) \cdot \mu(t) \tag{4}$$

In the time domain, these signals display a swift rise time, while in the frequency domain, they feature a wide spectrum overlapping the spectrum of the center frequency f_c of the useful signal. The characteristics of two consecutive transient IEMIs, including amplitude A, rise time t_{rise}, duration t_{hold}, unit step function $\mu(t)$, and interval can be randomly set up. Compared to frequency sweep IEMI, the behavior of this type of jammer is more unpredictable and conserves energy by alternating between active and idle states [9]. Fig. 7 shows the two consecutive transient interferences separated by a similar amplitude and duration with variable time intervals.

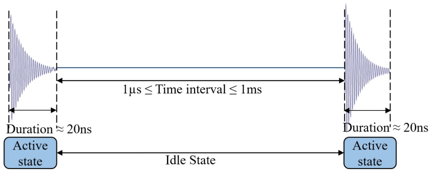

Fig. 7. Time representation of the transient IEMI model

C. Anomaly Threshold Evaluation

Considering the unpredictability of IEMI, data with two anomalous instances are also collected from four typical HSR scenarios.

To validate the choice of threshold, the test data comprises an equal number of abnormal data and the normal test dataset. The loss distribution of reconstruction in the test data with cumulative distribution function (CDF) and histogram is shown in Fig. 8. As expected, the detector can adequately reconstruct the normal signals within the threshold, and the reconstruction losses of the anomalous data are much larger than that of the normal data. The chosen threshold effectively separates the normal and anomalous groups. For the two typical IEMI models, the frequency-sweeping IEMI and transient IEMI are both random jammers with time-varying amplitude, duration, and repetition rates, thus the reconstruction loss shows a large variation.

Although the reconstruction loss of the training data is derived from the train operating under normal conditions, a few normal data points exceed the threshold in Fig. 8. These observations indicate that the receiver signal varies due to the dynamic scenario of the HSR. If the reconstruction loss is greater than the threshold, the detector will identify it as an anomaly, even if the signal disruption is caused by scenario variation rather than EMI, leading to false alarm problems.

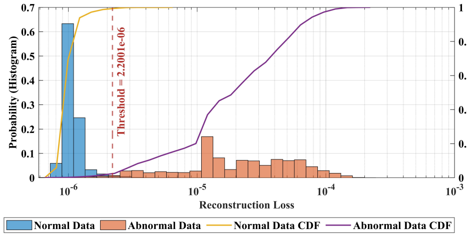

Fig. 8. Histogram and CDF of Test Reconstruction Loss Distribution

D. Performance Comparison with State-of-the-Art Methods

a) Index Performance: To assess the proposed method's effectiveness, we utilized anomaly evaluation metrics, including accuracy, precision, recall (sensitivity), and F1-measure. Accuracy indicates the ratio of samples with test results matching the actual type to the total samples. Precision signifies the ratio of samples correctly identified as positive to the total positively identified samples. Recall represents the ratio of samples correctly identified as positive to the total positive samples. F1-measure provides a comprehensive assessment by considering both precision and recall. Higher metric values indicate superior detection performance. The positive class denotes the target class as an anomaly, while the negative class signifies the normal class.

TABLE II
ANOMALY DETECTION INDEX PERFORMANCE COMPARISON

Algorithms	Accuracy	Precision	Recall	F1-measure
AE-BiLSTM	**0.9324**	0.9722	**0.9041**	**0.9379**
AE-CNN	0.8806	**0.9750**	0.8192	0.8912
AE	0.865	0.894	0.845	0.869
SVM	0.8475	0.95	0.8529	0.8982

The anomaly detection performance of AE-BiLSTM is compared with existing deep learning and conventional machine learning methods, including AE-CNN, AE, and SVM. Based on the test results shown in Table II, AE-LSTM outperforms other algorithms in accuracy, recall rate, and F1 measure. The accuracy achieves 93.24% enhanced by 5% compared to AE-CNN, the highest state-of-art. Precision and recall (sensitivity) of AE-BiLSTM are 0.9722 and 0.9041, respectively, indicating that the choice of threshold provides a trade-off between false alarms and missed anomalies. This underscores the significance of the AE-BiLSTM deep network structure to learn temporal information over long-range dependencies in normal conditions. The AE-CNN model, on the other hand, employs convolutional neural networks (CNNs) for feature extraction, followed by AE for reconstruction. This architecture exihibited competitive performance, capturing local patterns in the data using convolutional filters. The AE model represents a simpler architecture, serving as a baseline for comparison with more complex models, demonstrating respectable performance with the efficacy of AE-based representations for the task. In previous research based on SVM, power level data was collected from 801 frequency points within each spectrum [12]. However, it focused solely on the frequency domain, neglecting the frequency variance over time. Consequently, its anomaly detection performance deteriorates with unpredictable IEMI, different train speeds, and diverse scenarios, potentially posing security concerns.

TABLE III
COMPUTATION TIME COMPARISON OF DIFFERENT METHODS

Method	Online detection (ms)	Offline training (s)
AE-BiLSTM	4.51	906
AE-CNN	2.35	516
AE	1.95	200
SVM	1.41	109

b) Real-time Detection Analysis: Table III presents the computation time results for three different methods. The online detection time is measured in milliseconds, while the training time is measured in seconds. Our methods result in longer training and online detection times. This disparity arises from the fact that convolution operations can be parallelized by GPU, whereas LSTM cannot. Despite our model incurring the longest online detection time, it only takes 4.51 milliseconds to process a single input data, which falls within the tolerance of 3GPP critical data communications latency requirements of 10 ms [14]. The interval is established based on triggering the emergency brake in case of signal loss and considering the tolerance of signal variance during the movement of the train. Consequently, our proposed AE-BiLSTM deep learning method effectively responds to interference when real-time anomaly detection against security attacks is paramount.

V. CONCLUSION

In this paper, a wireless communication model is developed for a future 5G-R intelligent HSR system, considering the dynamic train movements, the signal propagation characteristics, and potential threats to operational security. The AE-BiLSTM anomaly detection algorithm utilizes AE and the bidirectional LSTM layers to capture signals during normal operations, incorporating multivariate features from time and frequency domains. Simulations show that the model achieves improvements in balancing false alarms and missed anomalies, with higher accuracy by 5% to reach 93.24% compared to three other approaches. It performs effectively in various scenarios and train speeds, particularly excelling in detecting unpredictable IEMIs. Furthermore, the online detection only takes 4.51 ms, indicating that the proposed anomaly detection method enables the design of real-time responses to threats, ensuring security. The approach can be applied to a wide range of electrified transportation systems.

REFERENCES

[1] J. Moreno, J. M. Riera, L. d. Haro, and C. Rodriguez, "A survey on future railway radio communications services: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 10, pp. 62–68, 2015.

[2] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 24, no. 2, pp. 767–809, 2022.

[3] S. Sullivan, A. Brighente, S. A. P. Kumar, and M. Conti, "5g security challenges and solutions: A review by osi layers," *IEEE Access*, vol. 9, pp. 116 294–116 314, 2021.

[4] V. Deniau, "Overview of the european project security of railways in europe against electromagnetic attacks (secret)," *IEEE Electromagnetic Compatibility Magazine*, vol. 3, no. 4, pp. 80–85, 2014.

[5] B. Ai, A. F. Molisch, M. Rupp, and Z.-D. Zhong, "5g key technologies for smart railways," *Proceedings of the IEEE*, vol. 108, no. 6, pp. 856–893, 2020.

[6] J. Villain, V. Deniau, and C. Gransart, *Jamming Detection in Electromagnetic Communication with Machine Learning: A Survey and Perspective*, ser. Machine Learning and Probabilistic Graphical Models for Decision Support Systems. CRC Press, 10 2022.

[7] S. Mili, V. Deniau, D. Sodoyer, M. Heddebaut, and S. Ambellouis, "Jamming detection methods to protect railway radio communication," *International Journal of Engineering and Innovative Technology - IJEIT*, vol. 4, no. 7, p. 7p, Jan. 2015.

[8] Y. Fan, L. Zhang, and K. Li, "Emi and iemi impacts on the radio communication network of electrified railway systems: A critical review," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 8, pp. 10 409–10 424, 2023.

[9] T. Erpek, Y. E. Sagduyu, and Y. Shi, "Deep learning for launching and mitigating wireless jamming attacks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 1, pp. 2–14, 2019.

[10] A. Marttinen, A. M. Wyglinski, and R. Jäntti, "Statistics-based jamming detection algorithm for jamming attacks against tactical manets," in *2014 IEEE Military Communications Conference*, 2014, pp. 501–506.

[11] C. Yin, S. Zhang, J. Wang, and N. N. Xiong, "Anomaly detection based on convolutional recurrent autoencoder for iot time series," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 1, pp. 112–122, 2022.

[12] J. Villain, V. Deniau, E. P. Simon, C. Gransart, A. N. de São José, F. Valenti, and N. Becuwe, "Detection and classification of interference affecting lorawan communications in railway environment," in *2022 3rd URSI Atlantic and Asia Pacific Radio Science Meeting*, 2022, pp. 1–4.

[13] H. Liu, H. Zhao, J. Wang, S. Yuan, and W. Feng, "Lstm-gan-ae: A promising approach for fault diagnosis in machine health monitoring," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–13, 2022.

[14] E. , "White paper on 5g-powered future railway mobile communication system (frmcs)," www.ericsson.com, 03 2022.

[15] N. Japkowicz, C. Myers, and M. Gluck, "A novelty detection approach to classification," in *Proceedings of the 14th International Joint Conference on Artificial Intelligence - Volume 1*, ser. IJCAI'95. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1995, p. 518–523.

[16] K. Greff, R. K. Srivastava, J. Koutník, B. R. Steunebrink, and J. Schmidhuber, "Lstm: A search space odyssey," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 28, no. 10, pp. 2222–2232, 2017.

[17] X. Wang, Z. Yu, and S. Mao, "Deepml: Deep lstm for indoor localization with smartphone magnetic and light sensors," in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1–6.

[18] C.-X. Wang, A. Ghazal, B. Ai, Y. Liu, and P. Fan, "Channel measurements and models for high-speed train communication systems: A survey," *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 974–987, 2016.

[19] L. Liu, C. Tao, J. Qiu, H. Chen, L. Yu, W. Dong, and Y. Yuan, "Position-based modeling for wireless channel on high-speed railway under a viaduct at 2.35 ghz," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 4, pp. 834–845, 2012.

[20] W. Radasky, C. Baum, and M. Wik, "Introduction to the special issue on high-power electromagnetics (hpem) and intentional electromagnetic interference (iemi)," *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, pp. 314–321, 2004.