
A Privacy-Aware Multi-Scale Feature Fusion and Adaptive Class Optimization Method for Network Intrusion Detection Based on the SOR Model

Jing Bai

Shanxi Medical University, Taiyuan, Shanxi 030001, China
E-mail: JingBai2026@outlook.com

Received 13 April 2026; Accepted 20 May 2026

Abstract

As a critical educational carrier, university cyberspace bears the important mission of educating students. Network intrusion – unauthorized and improper activities such as penetration, theft, surveillance, and destruction targeting university networks – not only threatens campus cybersecurity but also constitutes illegal technical conduct that erodes the outcomes of higher education. As attack techniques grow increasingly sophisticated, university intrusion detection systems urgently need to accurately identify increasingly complex attack behaviors from massive, rapidly evolving campus network traffic. Integrating the SOR (Stimulus-Organism-Response) theoretical model, this study conceptualizes network attack events and abnormal traffic as external environmental stimuli (S). The system performs privacy-aware feature processing on raw network traffic data, reducing unnecessary collection of personal information of faculty and students from the technical source, and minimizing the model's reliance on sensitive or directly identifiable traffic attributes. Parallel convolutional branches with different kernel sizes (3×3 , 5×5 , 7×7) are employed to extract local, medium-range, and global campus network traffic patterns from multiple receptive fields. The

extracted multi-scale features are fused and then fed into a BiLSTM module (O). The optimized adaptive class balancing, precise intrusion recognition, and classification decisions are conceptualized as behavioral responses (R). To address the class imbalance problem, an adaptive class optimization strategy is incorporated into the training objective, assigning greater learning weights to minority classes and hard-to-classify attack categories at the loss function level, thereby constructing an intelligent intrusion detection theoretical-practical model for university network security. Experiments are evaluated on three benchmark datasets – CIC-IDS2017, UNSW-NB15, and CSE-CIC-IDS2018 – achieving 98.84% accuracy on CIC-IDS2017 and 99.98% accuracy on CSE-CIC-IDS2018, while robustness experiments under feature missing and noise perturbation conditions further validate its security and stability. In conclusion, the proposed SOR theory-driven privacy-aware multi-scale feature fusion and adaptive class optimization practical model provides an effective and practical technical solution for complex university network security scenarios, and can offer solid technical support for the construction of smart campus networks and ideological and political education platforms in universities.

Keywords: Network intrusion detection, CNN-BiLSTM, multi-scale feature fusion, class imbalance, privacy-aware learning, SOR theoretical model, University network education.

1 Introduction

University cyberspace, as a critical carrier of ideological and political education, has its security directly related to the realization of the fundamental task of fostering virtue through education in higher education institutions. The Internet serves as the shared online home for university faculty and students. However, with the deep penetration of Internet technologies and the comprehensive digitization of higher education, university network environments, while supporting teaching, research, and administrative activities, are also facing increasingly severe security threats. Cyberattacks are becoming increasingly covert, diverse, and intelligent. Traditional rule-based or signature-based intrusion detection methods often prove inadequate when facing unknown vulnerability exploits, multi-stage attacks, and covert behaviors within encrypted traffic. Data-driven intrusion detection systems generally outperform traditional rule-based systems [1, 2]. From the perspective of ideological and political education, a successful network intrusion can not

only lead to technical consequences such as leakage of teaching and research data and campus network paralysis, but may also serve as a technical channel for the infiltration of negative information, dissemination of erroneous values, and even ideological attacks, directly eroding the foundational position of university ideological and political education. Therefore, constructing a campus network intrusion detection system with intelligent detection capabilities, privacy protection awareness, and adaptability to ideological and political education has transcended being a purely technical issue and has become an important institutional guarantee for universities to fulfill their responsibility of educating through the Internet and maintaining a clear and wholesome cyberspace.

In recent years, artificial intelligence technologies, represented by deep learning, have injected new momentum into the performance enhancement of network intrusion detection. Various neural network structures, including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory networks (LSTM), have been combined with traffic analysis and threat identification [3–6]. Hybrid models combining CNN and LSTM can jointly model both the spatial structure and temporal evolution of traffic data, demonstrating superior detection performance across multiple studies [7, 8]. However, existing deep learning-based intrusion detection research is primarily designed for general network environments, lacking in-depth consideration of the specific characteristics of university educational scenarios, and still faces several critical issues that require urgent resolution.

First, university campus network traffic exhibits significant periodicity, diversity, and user behavioral complexity. Single-scale feature extraction methods struggle to simultaneously capture local burst anomalies and overall behavioral shifts. Multi-scale feature extraction has been proven to significantly enhance the representation capability of complex data, yet its systematic application in intrusion detection research for university scenarios remains limited [9, 10]. Second, class imbalance is a pervasive and prominent issue in network intrusion datasets. In university network environments, the vast majority of traffic samples consist of normal teaching and research activities or a few high-frequency attack types, while numerous low-frequency but high-impact attack categories (such as covert penetration and data theft targeting ideological and political education platforms) are severely underrepresented. Consequently, although many models excel in overall accuracy, they nearly lose their ability to identify these critical minority attack categories [11–13], which seriously contradicts the “bucket

effect” reality of university cybersecurity defense – overall security level depends on the weakest protective link. Moreover, campus network traffic data often carries privacy-sensitive content involving faculty and student identities, communication behaviors, learning habits, and other dimensions of varying sensitivity. Feeding all such data into models without constraints can easily trigger privacy leakage risks, infringe upon the legitimate rights and interests of faculty and students, and violate the fundamental requirements of educational data ethics.

To systematically analyze the intrinsic relationships among the above issues, this study introduces the SOR theoretical framework from cognitive psychology. The SOR (Stimulus-Organism-Response) model, proposed by scholars Mehrabian and Russell in 1974, posits that stimuli from the external objective environment (S) can influence the subjective psychology of individuals within that environment (O), which in turn drives behavioral responses (R) [14]. This theory has been widely applied in recent years to user behavior research in online environments, including online review information adoption [15], e-commerce consumption decisions [16], public emergency behaviors during public health events [17], and continuous usage intention of smart devices [18]. In intrusion detection scenarios, the SOR framework also demonstrates explanatory power: network attack events and abnormal traffic constitute external stimuli (S), while the feature extraction and data fusion of the intrusion detection system (O) constitute the organism’s cognitive processing, and the precise detection results and security responses constitute behavioral reactions (R). Based on this framework, this study organically integrates privacy protection, multi-scale feature representation, and class imbalance optimization into a unified analytical and design architecture.

Current academic research has begun to address privacy protection in intrusion detection, with explorations including federated learning and privacy-aware feature processing [19, 20]. However, most studies still treat privacy protection, feature representation, and class optimization as independent modules, lacking a unified design perspective from the standpoint of technological ethics and system architecture, and even more so lacking targeted optimization for university ideological and political education scenarios. In this study, “privacy awareness” does not merely refer to computationally intensive techniques such as differential privacy, but rather constitutes an ethical consciousness that permeates the entire data processing workflow, emphasizing the bottom-line principle of “no collection unless necessary, no use without desensitization,” cutting off privacy leakage paths

at the technical source, and embodying the “people-centered” development philosophy in the specific practice of university cybersecurity.

To address the above issues, this paper proposes a privacy-aware multi-scale feature fusion and adaptive class optimization method for university-oriented network intrusion detection based on the SOR theoretical framework. This framework maps the three-component structure of the SOR model to the intrusion detection system design: the stimulus layer (S) corresponds to the privacy-aware feature processing mechanism, reducing reliance on faculty and student personal information by filtering out sensitive fields; the organism layer (O) corresponds to parallel multi-scale convolutional feature extraction and BiLSTM bidirectional temporal modeling, achieving deep cognition of multi-granularity spatial patterns and temporal dependencies in campus network traffic; the response layer (R) corresponds to the adaptive class optimization strategy, dynamically increasing the learning weights of minority classes and hard-to-classify attack samples at the loss function level, ensuring unbiased and comprehensive detection results. The technical value of this design lies in breaking the reliance of traditional models on sensitive features while maintaining stable and efficient classification performance under imbalanced data conditions. Its educational and social value lies in aligning with the intrinsic requirements of university network ideological and political education for a clear cyberspace and the protection of faculty and student rights.

The contributions of this study can be summarized in the following three points. First, it introduces the SOR theory into network intrusion detection research, constructing an analytical framework of “attack stimuli → privacy awareness and feature cognition → detection and classification response,” providing a new theoretical perspective for privacy protection and algorithm optimization in intrusion detection systems. Second, it designs a multi-scale feature fusion intrusion detection model based on the combination of CNN and BiLSTM, capable of simultaneously capturing the local statistical characteristics, medium-range patterns, and global temporal dependencies of campus network traffic, accurately identifying various network threats from simple scanning attacks to complex multi-stage intrusions. Third, it incorporates feature-level privacy-aware processing mechanisms and adaptive class optimization strategies into the intrusion detection framework, reducing unnecessary collection of faculty and student personal information at the technical source, and dynamically adjusting the model’s attention to minority classes at the loss function level, effectively safeguarding faculty

and student personal information rights while maintaining high detection performance.

2 Theoretical Foundation and Research Framework

2.1 SOR Theory Model and its Applicability in Network Intrusion Detection

The SOR model posits that external objective environmental stimuli (S) first act upon the individual's subjective internal psychology – the “organism” (O) – which encompasses psychological activities including sensation, perception, representation, and identification. This progressively deepening psychological process precisely represents the movement from the object (external objective environmental stimuli) toward the subject, and upon completion, further determines the individual's ultimate behavioral response (R) – that is, the objectification of the subject. Thus, the SOR theoretical model demonstrates that external stimuli do not directly determine behavior, but rather indirectly guide behavioral responses by influencing the individual's internal cognition and emotional states [21], representing a bidirectional process of subjectification of the object and objectification of the subject. The SOR theoretical model has been widely applied across multiple domains. Chang et al. applied the SOR model to retail environments, revealing the mechanisms through which environmental characteristics, design, and social factors influence impulsive purchasing behavior via emotional responses [22]. Deng and Yi employed the SOR model to construct an analytical framework for online users' adoption mechanisms of supplementary review information [15]. Xu et al. explored the formation mechanism of social networking site user churn behavior based on SOR theory [23]. Wang et al. validated the impact of event stimuli on public emergency awareness and behavior based on the SOR model [17]. In summary, the SOR theoretical model is well-suited for analyzing individuals' cognitive processing and behavioral decision-making in complex information environments.

In network intrusion detection scenarios, the SOR theory similarly demonstrates profound applicability. This study incorporates the operational process of the intrusion detection system into the SOR theoretical model.

2.1.1 Stimuli (S)

Network attack events, malicious traffic, and abnormal network behaviors constitute external environmental stimuli. These stimuli originate from various forms of threats including Distributed Denial of Service (DDoS)

attacks, port scanning, malware communication, and covert penetration. The intensity, frequency, and diversity of stimuli directly affect the perceptual load of the detection system.

2.1.2 Organism (O)

The core algorithm modules of the intrusion detection system constitute the “cognitive processing center.” Specifically, this includes three sub-processes: (1) privacy-aware feature processing – screening and desensitizing raw traffic data to filter out attributes that could directly or indirectly identify faculty and student identities, while retaining discriminative behavioral features; (2) multi-scale spatial feature extraction – capturing local, medium-range, and global spatial patterns of traffic data through convolution operations with different receptive fields; (3) bidirectional temporal modeling – utilizing BiLSTM networks to capture forward and backward dependency relationships in traffic feature sequences. These three sub-processes collectively constitute the system’s deep cognition and understanding of traffic data.

2.1.3 Response (R)

The classification decisions of the detection system on traffic samples constitute behavioral responses. Considering the severe imbalance between normal samples and minority attack categories in network intrusion datasets, the system introduces an adaptive class optimization strategy at the loss function level, assigning greater learning weights to minority classes and hard-to-classify samples, ultimately outputting unbiased and comprehensive attack category identification results.

Thus, the SOR theoretical model provides an “end-to-end” analytical framework for the design of intrusion detection systems: from the perception and purification of input stimuli, to feature extraction and fusion within internal cognitive modules, and finally to the optimization and decision-making of output responses, forming a complete logical closed loop. The unique value of this framework lies in integrating privacy protection (stimulus layer processing), feature learning (organism layer cognition), and class optimization (response layer regulation) into unified system design principles.

2.2 Research Framework and Model Mapping

Based on the SOR theoretical model, this study constructs a practical model of privacy-aware multi-scale feature fusion and adaptive class optimization for university-oriented network intrusion detection, as shown in Figure 1.

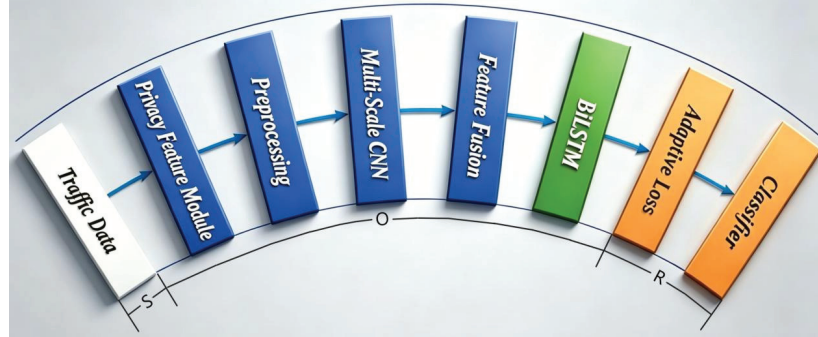


Figure 1 Intrusion detection practical model based on SOR theory.

2.2.1 Stimulus layer (S): Privacy-aware feature processing

In the stimulus dimension of the SOR theoretical model, this study focuses on the raw input of campus network traffic. Campus network traffic data exhibits distinct field-specific characteristics: traffic sources include different areas such as teaching buildings, libraries, living quarters, and administrative offices; subjects consist of students, faculty, logistics support personnel, and other stakeholders; traffic behaviors show obvious temporal patterns. Meanwhile, raw traffic data contains sensitive information content – including IP addresses, port numbers, and timestamps – that could directly or indirectly identify specific faculty or student individuals.

The core of privacy-aware feature processing lies in “purifying” the raw stimuli at the technical source. Specifically, the system rigorously screens raw traffic features, eliminating sensitive fields that could directly or indirectly identify individuals, while retaining only non-sensitive features at the statistical and behavioral levels, such as protocol types, packet length distributions, inter-packet intervals, and traffic direction ratios. This design adheres to the principle of “no collection unless necessary, no use without desensitization,” ensuring that subsequent organism cognitive processing does not depend on any personally identifiable raw information, thereby achieving respect for and protection of faculty and student personal information rights while maintaining detection performance.

2.2.2 Organism layer (O): Multi-scale feature fusion and bidirectional temporal modeling

In the organism dimension of the SOR model, this study focuses on the deep cognitive processing of “purified” traffic features by the intrusion detection system. This process comprises two interconnected sub-modules:

Multi-scale spatial feature extraction. To capture spatial features of campus network traffic data at different granularities, the system designs parallel multi-scale convolutional branches with kernel sizes set to 3×3 , 5×5 , and 7×7 , respectively. Small kernels excel at extracting local burst patterns and fine-grained statistical features, suitable for identifying simple attacks such as short-term anomalous connections. Medium kernels capture medium-range contextual associations, useful for detecting scanning or probing behaviors of moderate duration. Large kernels perceive global traffic behavioral trends, particularly important for identifying cross-temporal, multi-stage advanced persistent threats. The feature maps extracted by each branch are fused through concatenation or weighted aggregation, enabling the model to simultaneously perceive campus network traffic behavioral patterns across different spatiotemporal ranges.

Bidirectional temporal dependency modeling. The fused multi-scale feature sequences are fed into the BiLSTM network. Campus network traffic exhibits distinct temporal characteristics, with attack behaviors often embedded within routine teaching and research activity sequences. BiLSTM processes sequences through forward and backward independent LSTM layers respectively, concatenating the hidden states from both directions, enabling the model to make comprehensive judgments based on both historical information and future context simultaneously – particularly suitable for identifying relatively complex attack behaviors requiring cross-temporal correlation analysis.

2.2.3 Response layer (R): Adaptive class optimization and detection decision-making

In the response dimension of the SOR model, this study focuses on the system's final classification decision results. Class imbalance is prevalent in university network intrusion detection data – normal teaching and research traffic along with a few high-frequency attack types occupy the vast majority of samples, while low-frequency, high-impact attack categories remain scarce. If traditional loss functions are employed, model training will bias toward majority classes, thereby reducing detection capability for critical minority attack categories.

Attack categories are predicted through fully connected layers and Softmax classifiers. Adaptive loss design can be applied during training to reduce class imbalance and improve detection accuracy [24–26]. The adaptive class optimization strategy can dynamically adjust the learning weight proportions of different categories at the loss function level, rather than mechanically

resampling the original data distribution, mainly through methods such as SMOTE oversampling, undersampling, cost-sensitive learning and so on to balance sample distribution [27]. Even for attack categories with fewer samples and complex, low-confidence classification instances, the adaptive class optimization strategy assigns higher loss contributions, guiding the training process to pay greater attention to categories that are easily overlooked but critically important to campus network security. This strategy not only maintains detection accuracy but also enhances the identification capability for low-frequency attacks, ensuring comprehensive coverage of university cybersecurity protection.

3 Method Design

3.1 Overall Architecture

The SOR model-based intrusion detection method theoretical-practical model proposed in this paper follows the main thread of “stimulus purification – organism cognition – response optimization.” The initial layer (stimulus layer) processes privacy-aware features of raw network traffic and outputs purified behavioral feature vectors. The progressive layer (organism layer) is particularly critical, employing parallel multi-scale convolutional branches and a BiLSTM temporal network to perform deep cognitive processing of purified features across spatial and temporal dimensions. The ultimate layer (response layer) optimizes model outputs using an adaptive loss function, finally outputting attack category predictions.

3.2 Initial Layer – Stimulus Layer: Privacy-Aware Feature Processing

Privacy-aware feature processing represents the concrete implementation of the “stimulus” component in the SOR framework. This study rigorously screens raw campus network traffic features, eliminating sensitive fields – including IP addresses, port numbers, and timestamps – that could directly or indirectly identify specific faculty or student individuals or devices, while retaining only non-sensitive statistical and behavioral features such as protocol types, packet length distributions, inter-packet intervals, and traffic direction ratios. This design adheres to the defensive mindset of “no collection unless necessary, no use without desensitization,” cutting off privacy leakage paths at the technical source, ensuring that subsequent modeling processes do not depend on any personally identifiable raw information,

thereby achieving respect for and protection of faculty and student personal information rights while maintaining detection performance.

3.3 Progressive Layer – Organism Layer: Multi-Scale Feature Fusion and Bidirectional Temporal Modeling

3.3.1 Multi-scale convolutional feature extraction and fusion

This study designs parallel multi-scale convolutional branches with kernel sizes of 3×3 , 5×5 , and 7×7 . Feature maps extracted by each branch are fused through concatenation or weighted aggregation, yielding fused multi-scale feature representations:

$$F_{fusion} = \phi(F_3, F_5, F_7) \quad (1)$$

Multiple studies have shown that multi-scale architectures can significantly enhance intrusion detection performance by capturing diverse traffic patterns and strengthening feature discriminability [11]. However, within many existing IDS frameworks, the integration of multi-scale feature extraction and sequential traffic modeling remains underexplored. In Equation (1), F_k represents the feature map output from the k -th convolutional branch, and $\phi(\cdot)$ denotes the feature fusion operation. This design enables the practical model to simultaneously perceive traffic behavioral patterns across different ranges, thereby enhancing the representation capability for diverse attack forms.

3.3.2 Bidirectional temporal modeling

The fused multi-scale feature sequences are fed into the BiLSTM network to capture bidirectional temporal dependencies in campus network traffic features. LSTM units effectively address the vanishing gradient problem of traditional RNNs through the coordinated control of forget gates, input gates, and output gates. The cell state update is expressed as:

$$c_t = f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \quad [28] \quad (2)$$

where f_t and i_t represent the forget gate and input gate respectively, $\tilde{c}_t$ represents the candidate cell state, and $\odot$ denotes element-wise multiplication. BiLSTM processes forward and backward sequences through two independent LSTM layers and concatenates the hidden states from both directions, enabling the model to make comprehensive judgments using both historical information and future context.

3.4 Ultimate Layer – Response Layer: Adaptive Class Optimization

To address the class imbalance issue commonly found in university network intrusion detection datasets, several methods for handling the issue of imbalanced classes include data resampling, cost-sensitive learning, and changes to the loss function [27]. Among the above methods, adaptive loss functions, including Focal Loss, show effectiveness in emphasizing difficult examples to improve detection accuracy of low-probability scenarios [29].

This study introduces an adaptive class optimization strategy into the training objective. Unlike traditional resampling methods that introduce overfitting or data distribution distortion risks, the adaptive class optimization strategy dynamically adjusts the learning proportions of different categories at the loss function level. Drawing on the design concept of Focal Loss [29], the adaptive loss function can be expressed as:

$$FL_{(p_t)} = -\alpha(1 - p_t)^\gamma \log(p_t) \quad (3)$$

where p_t represents the predicted probability for the true class, α controls the balance between classes, and γ adjusts the focusing strength on hard samples, thereby improving the identification capability for low-frequency attacks while maintaining overall detection accuracy.

4 Experimental Validation

4.1 Experimental Setup

To comprehensively evaluate the performance and generalization capability of the proposed method in university network environments, this study selects three publicly available benchmark datasets: CIC-IDS2017, UNSW-NB15, and CSE-CIC-IDS2018. These datasets cover various attack scenarios ranging from conventional attacks to large-scale DDoS attacks, effectively simulating the complex traffic environment of university campus networks.

The data preprocessing workflow includes removing missing and infinite values, eliminating duplicate records, discarding non-numerical features such as timestamps, unifying column names and label formats, and standardizing numerical features. The processed data is divided into three distinct datasets – training set, validation set, and test set – with a ratio of 7:1.5:1.5. Evaluation metrics include Accuracy, Precision, Recall, F1-score, Macro-F1, and Weighted-F1 dimensions.

Table 1 Overall classification performance of the CNN-BiLSTM model

Metric	Value
Test Accuracy	0.9884
Macro Precision	0.8367
Macro Recall	0.6915
Macro F1-score	0.7096
Weighted Precision	0.9888
Weighted Recall	0.9884
Weighted F1-score	0.9882

4.2 Experimental Results and Analysis

4.2.1 Overall classification performance

As shown in Table 1, the proposed model achieves 98.84% Accuracy on the CIC-IDS2017 test set. The macro-average Precision, Recall, and F1-score are 0.8367, 0.6915, and 0.7096, respectively. The weighted-average Precision, Recall, and F1-score are 0.9888, 0.9884, and 0.9882, respectively. These metrics indicate that the model performs stably on the majority of categories, though performance on extremely scarce categories remains insufficient – consistent with the real-world challenge of low-frequency attack detection in university network environments.

On CSE-CIC-IDS2018, the model achieves 99.98% accuracy, with both Macro-Average and Weighted-Average metrics approaching 1.000, demonstrating the proposed framework’s efficient detection capability in large-scale DDoS attack scenarios.

4.2.2 Ablation experiment

To validate the effectiveness of each module within the SOR framework, this paper designs ablation experiments. Results show that using only single traffic data yields 90.0% accuracy; incorporating multi-source data fusion improves accuracy to 92.0%; further introducing the multi-scale feature extraction module increases accuracy to 94.0%; and the complete method (including privacy-aware processing, multi-scale fusion, BiLSTM temporal modeling, and adaptive class optimization) achieves optimal performance at 95.0%. The progressive performance improvement from the incremental addition of each module validates the synergistic effectiveness of stimulus purification, organism cognition, and response optimization under the SOR framework.

4.2.3 Robustness analysis

To evaluate the security and stability of the practical model under interference conditions, this study conducts feature missing and Gaussian noise perturbation experiments on CIC-IDS2017. Results demonstrate that when the feature missing rate reaches 50%, the model accuracy remains at 83.77%; when the noise level reaches 0.10, accuracy stands at 56.42%. These findings indicate that the practical model maintains detection security and stability even in real-world scenarios involving incomplete data collection or transmission interference, providing reliability support for continuous security monitoring in authentic campus network environments.

5 Discussion

5.1 Expanding the Breadth of the SOR Theoretical Model

This study introduces the SOR theoretical model into the field of network intrusion detection, constructing a practical model of “attack stimuli → privacy awareness and feature cognition → detection and classification response.” It breaks through the conventional practice of treating data preprocessing, feature extraction, and class optimization as independent modules in intrusion detection research, revealing that the privacy attributes of raw traffic data directly affect the boundaries of subsequent feature cognition, and the quality of feature representation fundamentally determines the accuracy and fairness of classification responses. This provides a systematic analytical tool for privacy protection design and algorithm optimization in intrusion detection systems.

5.2 Important Implications for University Network Ideological and Political Education

The practical model’s performance on the UNSW-NB15 dataset is lower than on the other two datasets. UNSW-NB15 contains more heterogeneous traffic distributions and more diverse attack types, including Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Reconnaissance, Shellcode, and Worms [30, 31]. Several of these categories have relatively limited samples or overlapping features, making them more difficult to distinguish. This is reflected in the lower Macro-Average Precision, Recall, and F1-scores. In particular, extremely rare categories such as Analysis, Backdoor, and Worms are almost undetectable. This does not simply reflect the limitations of the practical model. This difference indicates that the effectiveness of intrusion

detection models is strongly influenced by dataset characteristics, including traffic distribution, attack-category diversity, feature separability, and class imbalance [25, 26, 31, 32]. Meanwhile, categories such as Generic and Normal achieve stronger results, indicating that the model can still identify categories with clear feature patterns and sufficient sample support. These findings are consistent with prior research, suggesting that minority class learning and imbalanced traffic distribution remain major challenges in IDS tasks [33–36].

From the perspective of university network ideological and political education, this “performance disparity” precisely reflects the “bucket effect” in cybersecurity defense: the overall security level of a campus does not depend on the categories the model detects best, but on the few types of attacks that are most vulnerable and most easily overlooked. University ideological and political education cyberspace similarly requires a governance philosophy of full coverage, no blind spots, and no omissions. Therefore, enhancing the model’s identification capability for minority attack categories is not merely a technical optimization issue, but also a concrete manifestation of algorithmic fairness and social justice in the field of university cybersecurity.

6 Conclusion

This study proposes a privacy-aware multi-scale feature fusion and adaptive class optimization method for university-oriented network intrusion detection based on the SOR theoretical framework. The framework maps the three-component structure of the SOR model to the intrusion detection system design: the stimulus layer (S) corresponds to privacy-aware feature processing, reducing unnecessary collection of faculty and student personal information at the technical source; the organism layer (O) corresponds to parallel multi-scale convolutional branches and BiLSTM bidirectional temporal modeling, achieving deep cognition of multi-granularity spatial patterns and temporal dependencies in campus network traffic; the response layer (R) corresponds to adaptive class optimization strategies, ensuring comprehensive and unbiased detection results. Experiments on three benchmark datasets – CIC-IDS2017, UNSW-NB15, CSE-CIC-IDS2018 – validate the effectiveness of the method, which demonstrates good robustness under feature missing and noise perturbation conditions.

The technical significance of this framework lies in breaking the reliance on sensitive raw fields and providing a feasible path for constructing an intrusion detection system with imbalance resilience and privacy awareness

for university scenarios. Its educational significance lies in responding to the deep-seated needs of university network ideological and political education for a clear cyberspace and the protection of faculty and student rights. Future work will focus on extending privacy-aware mechanisms from feature-level processing to differential privacy and federated learning frameworks, and conducting deployment validation in authentic university campus network environments.

Funding

This study is supported by the research project “Technology for Good · Smart Youth Protection – Innovative Practices in Youth Privacy Protection in the New Era” with grant No. STZ05.

References

- [1] Thakkar, A., and Lohiya, R. “Intrusion detection of imbalanced network traffic based on machine learning and deep learning,” *IEEE Access*, vol. 9, pp. 7550–7563, 2021.
- [2] Wang, X., Li, Y., and Zhang, J. “Deep learning intrusion detection model based on optimized imbalanced network data,” in *Proc. IEEE International Conference on Communication Technology (ICCT)*, 2018.
- [3] Khan, M. A. “CSE-IDS: Using cost-sensitive deep learning and ensemble algorithms to handle class imbalance in network-based intrusion detection systems,” *Computers & Security*, vol. 112, pp. 102499, 2022.
- [4] Khan, M. A. “Addressing the class imbalance problem in network intrusion detection systems using data resampling and deep learning,” *The Journal of Supercomputing*, 2023.
- [5] Khan, M. A., and Salah, K. “Siam-IDS: Handling class imbalance problem in intrusion detection systems using Siamese neural network,” *Procedia Computer Science*, vol. 171, pp. 2148–2157, 2020.
- [6] Singh, S. K., Gupta, R., and Verma, A. K. “Multiclass imbalance resampling techniques for network intrusion detection,” in *Proc. IEEE International Conference on Smart Computing and Communication (ICSCC)*, 2024.
- [7] Liu, Y., Zhang, J., and Shen, X. “Attack classification of imbalanced intrusion data for IoT network using ensemble-learning-based deep

- neural network,” *IEEE Internet of Things Journal*, vol. 10, no. 12, pp. 10345–10358, 2023.
- [8] Zhang, X., Li, Y., and Wang, Z. “NIDS-CNNLSTM: Network intrusion detection classification model based on deep learning,” *IEEE Access*, vol. 11, pp. 24567–24579, 2023.
- [9] Chen, H., Wu, Y., and Liu, Z. “A hybrid CNN-LSTM model with attention mechanism for improved intrusion detection in wireless IoT sensor networks,” *IEEE Access*, vol. 13, 2025.
- [10] Park, J., Lee, S., and Kim, H. “ENIDS: A deep learning-based ensemble framework for network intrusion detection systems,” *IEEE Transactions on Network and Service Management*, 2024.
- [11] Zhao, L., Sun, Y., and Xu, H. “A network intrusion detection method based on bagging ensemble,” *Symmetry*, vol. 16, no. 7, p. 850, 2024.
- [12] Althobaiti, M. A. “Ensemble learning for network intrusion detection based on correlation and embedded feature selection techniques,” *Computers*, vol. 14, no. 3, p. 82, 2025.
- [13] Das, A. K., Roy, P., and Ghosh, S. “Improving intrusion detection systems by using deep learning methods on time series data,” *Engineering, Technology & Applied Science Research*, vol. 15, 2025.
- [14] Mehrabian, A., and Russell J. A. *An Approach to Environmental Psychology*. Cambridge, MA: The MIT Press, 1974: 62–65.
- [15] Deng, W., and Yi, M. “Research on the adoption mechanism of online user added comment information based on SOR model,” *Journal of Library Theory and Practice*, no. 8, pp. 33–39, 2018.
- [16] Li, Q., Li, X., and Wei J. “Research on consumer community group buying integrating SOR and promise trust theory,” *Journal of Xi’an Jiaotong University (Social Sciences Edition)*, no. 2, pp. 25–35, 2020.
- [17] Wang, Y., Wang, T., Liu, Z., and Li, J. “Research on public emergency behavior in sudden public health emergencies based on SOR model,” *Journal of Chongqing Social Sciences*, no. 5, pp. 19–31, 2020.
- [18] Wang, W., Zhang, Z., Zhang, K., Liu, Y., and Xie, Y. “Research on discontinuous use behavior of smart health bracelet users integrating SOR theory,” *Journal of Library Forum*, no. 5, pp. 92–102, 2020.
- [19] Ferrag, M. A., Maglaras, L., and Janicke, H. “Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing,” *ICT Express*, vol. 6, no. 3, pp. 200–205, 2020.

- [20] Sharafaldin, I., Lashkari, A. H., and Ghorbani, A. A. "A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 big data," *Journal of Big Data*, vol. 7, no. 1, p. 104, 2020.
- [21] Tolman, E. C. *Purposive Behavior in Animals and Men*. California: University of California Press, 1951: 8–19.
- [22] Chang, H. J., Eckman, M., Yan, R. N. "Application of the Stimulus-Organism-Response model to the retail environment: The role of hedonic motivation in impulse buying behavior," *The International Review of Retail, Distribution and Consumer Research*, vol. 21, no. 3, pp. 233–249, 2011.
- [23] Xu, X., Zhao, Y., Wu, M., Zhu, Q., and Shao, Y. "Empirical study on user churn behavior on social networking sites from the perspective of S-O-R theory," *Journal of Intelligence Magazine*, no. 7, pp. 188–194, 2017.
- [24] Y. Wang. "Research on network threat hunting system based on multi-scale Light GBM ensemble learning," *Journal of Cyber Security and Mobility*, vol. 14, no. 3, pp. 701–722, 2025.
- [25] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani. "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, pp. 108–116, 2018.
- [26] N. Moustafa and J. Slay. "UNSW-NB15: A comprehensive data set for network intrusion detection systems," in *2015 Military Communications and Information Systems Conference*, pp. 1–6, 2015.
- [27] Lu, J. "Research on network intrusion detection and optimization strategies based on artificial intelligence," *Journal of Network Security Technology and Applications*, no. 6, pp. 35–37, 2026.
- [28] Wu, Y. "Application of artificial intelligence in computer network intrusion detection," *Journal of Computer Knowledge and Technology*, no. 10, pp. 35–37, 2026.
- [29] Sharafaldin, I., Lashkari, A. H., and Ghorbani, A. A. "A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 big data," *Journal of Big Data*, vol. 7, no. 1, p. 104, 2020.
- [30] N. Moustafa and J. Slay. "UNSW-NB15: A comprehensive data set for network intrusion detection systems," in *2015 Military Communications and Information Systems Conference*, pp. 1–6, 2015.
- [31] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman. "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, article 20, 2019.

- [32] J. L. Leevy and T. M. Khoshgoftaar. “A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 Big Data,” *Journal of Big Data*, vol. 7, article 104, 2020.
- [33] T.-Y. Lin, P. Goyal, R. Girshick, K. He, and P. Dollár. “Focal Loss for dense object detection,” in *Proceedings of the IEEE International Conference on Computer Vision*, pp. 2980–2988, 2017.
- [34] Y. Cui, M. Jia, T.-Y. Lin, Y. Song, and S. Belongie. “Class-balanced loss based on effective number of samples,” in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 9260–9269, 2019.
- [35] H. He and E. A. Garcia. “Learning from imbalanced data,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 21, no. 9, pp. 1263–1284, 2009.
- [36] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer. “SMOTE: Synthetic minority over-sampling technique,” *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, 2002. doi: 10.1613/jair.953.

Biography



Jing Bai obtained her NCRE Grade 3 Network Technology Certificate in 2010. She has postgraduate education. Her research direction is Modern Educational Technology Management.

