






Machine-learning-based optical spectrum feature analysis for DoS attack detection in IP over optical networks

XIAOXUE GONG,^{1,2}  YANG LEI,^{1,2} QIHAN ZHANG,^{1,2}  LU GAN,³
XU ZHANG,^{1,2,4}  AND LEI GUO^{1,2}

¹*School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*

²*Institute of Intelligent Communications and Network Security, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*

³*Dept. of Electronic and Electrical Engineering, Brunel University, London UB8 3PH, UK*

⁴*zhangxu@cqupt.edu.cn*

Abstract: In this paper, we introduce a novel approach for detecting Denial of Service (DoS) attacks in software-defined IP over optical networks, leveraging machine learning to analyze optical spectrum features. This method employs machine learning to automatically process optical spectrum data, which is indicative of network security status, thereby identifying potential DoS attacks. To validate its effectiveness, we conducted both numerical simulations and experimental trials to collect relevant optical spectrum datasets. We then assessed the performance of three machine learning algorithms XGBoost, LightGBM, and the BP neural network in detecting DoS attacks. Our findings show that all three algorithms demonstrate a detection accuracy exceeding 97%, with the BP neural network achieving the highest accuracy rates of 99.55% and 99.74% in simulations and experiments, respectively. This research not only offers a new avenue for DoS attack detection but also enhances early detection capabilities in the underlying optical network through optical spectrum data analysis.

© 2024 Optica Publishing Group under the terms of the [Optica Open Access Publishing Agreement](#)

1. Introduction

With the booming development of various emerging network services, future-proof IP over optical networks is facing unprecedented opportunities and challenges [1–3]. Typically, IP over optical networks integrate IP and optical network technologies, where IP protocols are used to encapsulate data, while optical fiber is employed as a transmission medium to achieve high-speed transmission and exchange of data. Although IP over optical networks provides convenient service to users, they also suffer from serious network security threats. DoS attacks have become one of the main threats to network security due to their simple and crude attack mode, as well as diverse attack methods [4,5]. In general, the defense approaches for DoS attacks include three aspects: DoS attack detection, DoS attack source tracking, and DoS attack packet filtering. Among them, DoS attack detection is the foundation and premise of attack source tracking and attack packet filtering. Given the rising prevalence of transient DoS attacks, the need for fast and accurate detection methods has become an urgent priority in the field of network security research.

Current DoS attack detection strategies primarily focus on packet-level analysis in the IP network layer [6–8], examining network traffic or highly processed packet datasets. While these methods, which analyze network traffic characteristics and packet contents, aid in detecting DoS attacks, they suffer from slow detection speeds. This sluggishness stems from their reliance on data obtained through photoelectric conversion, hindering their effectiveness against transient DoS attacks. Moreover, as IP and optical networks continue to merge and evolve rapidly, shifting

more network functions to the optical layer via software-defined approaches is emerging as a trend. This shift aims to alleviate the burden at the IP level and enhance overall network efficiency, marking a new direction in the development of IP over optical networks [9–11]. With the application of machine learning in assisting fault management in optical networks, it has become a feasible scheme for attack detection and received great attention from researchers [12–15].

Therefore, in this paper, we explore the feasibility of implementing DoS attack detection at the optical layer in IP over optical networks by proposing a DoS attack detection scheme based on optical spectrum feature analysis. Taking into account that the security state information of the optical network is hidden in the correlation of the optical spectrum data, the proposed scheme can determine whether the network is under DoS attack by using machine learning algorithms to automatically mine and process the correlation among the optical spectrum data. To evaluate the performance of the proposed method, both numerical simulations and experimental validations are undertaken. In simulations, different types of DoS attack traffic data and normal traffic data are first acquired from a typical DARPA 1998 dataset [16]. Then the acquired data are pre-processed and converted into an optical signal for spectrum data collection. Finally, the performance of three machine learning algorithms including the backpropagation (BP) neural network [17], XGBoost (eXtreme Gradient Boosting) [18] and LightGBM (Light Gradient Boosting Machine) [19] on DoS attack detection is evaluated based on the characteristics of the optical spectrum information collected under different attack types. The results show that the detection accuracy of the three algorithms is above 97%, and the accuracy of the BP neural network reaches 99.55%. In the experiment, the DoS attack is launched by the host, and the optical spectrum information on the optical fiber link is monitored in real time by using an optical spectrum analyzer. The performance of the above three machine learning algorithms is evaluated by extracting the optical spectrum information at regular intervals. The results also demonstrate that the detection accuracy of the three algorithms is above 99%, and the accuracy of the BP neural network detection reaches 99.74%. Therefore, the feasibility and reliability are verified by using optical spectrum data features for high-precision detection of DoS attacks. Our work can extract the data information much earlier in the optical domain without the need for photoelectric conversion in traditional methods, which can achieve faster detection of DoS attacks.

The rest of this paper is organized as follows. Section 2 presents the proposed framework for DoS attack detection using optical spectrum features. Section 3 describes the simulation setup and analysis of synthetically generated data. Section 4 details the experimental configuration and results for measurements on a practical system. Finally, Section 5 concludes the paper with a summary of key findings.

2. Proposed framework for DoS attack detection

2.1. System overview

Figure 1 illustrates the proposed framework for DoS attack detection based on optical spectrum feature analysis in IP over optical networks. When a DoS attack occurs, the attacker sends a large amount of malicious traffic and requests at the network nodes, which are transmitted to the attack target through the optical network together with normal traffic. In traditional IP over optical networks, the IP layer is responsible for DoS attack detection and the optical layer is only responsible for the transparent transmission of optical signals. In the software-defined optical network scenario, the optical layer is equipped with the attack detection system to achieve DoS attack detection. In addition, the optical spectrum characteristics of the attacked signal will be different from the ordinary data signal when the data is finally transmitted in the optical fiber after electro-optic conversion, due to the load regularity, the randomly generated IP address of the attack signal, and the bit difference from normal communication. Therefore, the optical spectrum data can be used as a feature of DoS attack detection.

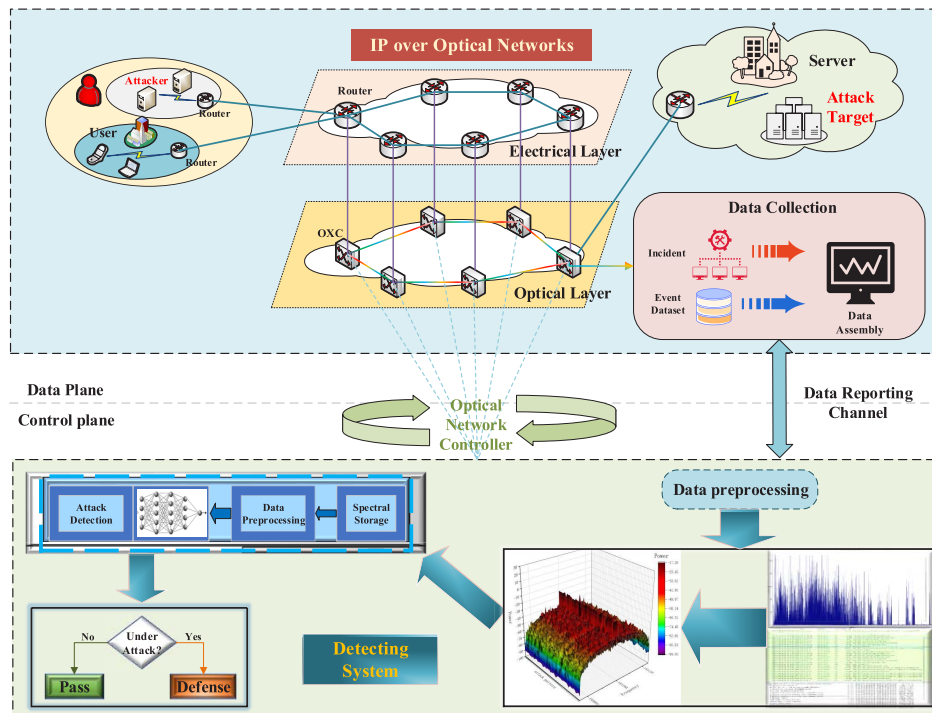


Fig. 1. The proposed framework for DoS attack detection

The overall detection process in the framework can be summarized as follows. It begins with the periodic collection of optical spectrum information at the receiving end, followed by data storage and pre-processing. Next, a trained machine-learning algorithm for DoS attack detection is employed to ascertain whether the data is under attack or legitimate. If deemed legitimate, normal data transmission proceeds. However, if an attack is detected, appropriate defense measures are activated. This method, focusing on spectrum features at the optical network layer rather than packet characteristics at the IP layer, allows for quicker detection of DoS attacks. This rapid identification provides the network management system with sufficient time to respond effectively to any attacks.

Figure 2 illustrates our machine-learning-based DoS attack detection scheme, framed as a classification problem. The algorithm inputs include both normal and attacked optical spectrum data, with the outputs being their respective classifications. It is important to note that the optical spectrum data collected within the same frequency range may vary due to differing data volumes within identical time windows during numerical simulations. To address this, cluster analysis is employed to unify the number of data. Following this, the data are labeled and Min-max normalization of the data. We then split the dataset into training and test sets. The training set is used to train the models, while the test set is utilized to evaluate the algorithm's performance by feeding its samples into the trained models.

2.2. Methodology and evaluation metrics

In our research, we employ three machine learning algorithms, i.e., XGBoost, LightGBM and the BP neural network, for analyzing optical spectrum features in DoS attack detection. Although both XGBoost and LightGBM are integrated learning algorithms based on decision trees, and they can provide a more comprehensive comparison in practical applications due to their differences

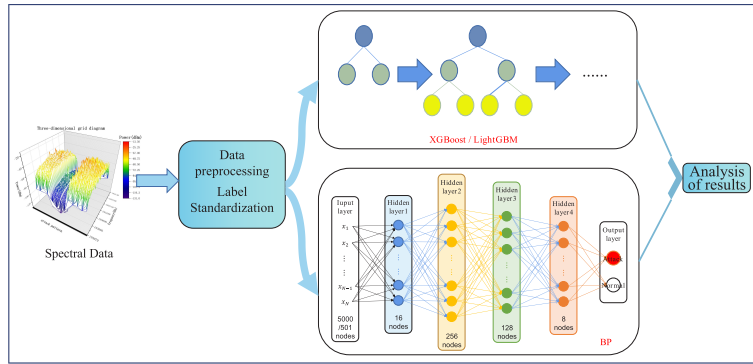


Fig. 2. Machine-learning-based DoS attack detection scheme

in implementation and optimization. The BP neural network is a deep learning algorithm utilizing back-propagation. These algorithms are renowned for their efficiency and effectiveness, particularly in solving classification problems and handling large-scale datasets. The BP neural network algorithm is structured with an input layer, several hidden layers, and an output layer. During the simulation, the input layer comprises 5000 nodes, and there are 3 hidden layers with 8, 64, and 8 nodes, respectively. The hidden layers employ a sigmoid function as the activation function, and gradient descent is used for loss minimization. In the experimental setup, the BP neural network’s input layer has 501 nodes, with all other parameters remaining consistent with the default setup.

To evaluate the performance of the machine learning algorithms in DoS attack detection, we use Accuracy (ACC), False Positive Rate (FPR), and False Negative Rate (FNR) as metrics. The confusion matrix, detailed in Table 1, helps classify the cases. In this matrix, 'TP' (True Positives) represents correctly predicted positive samples, 'FP' (False Positives) denotes negative samples incorrectly labeled as positive, 'FN' (False Negatives) refers to positive samples wrongly classified as negative, and 'TN' (True Negatives) indicates correctly predicted negative samples. 'N' is the total number of samples in the dataset. In our simulation, normal spectral data is categorized as the positive class, and DoS attack spectral data as the negative class. The expressions for calculating ACC, FPR, and FNR are:

$$ACC = \frac{TP + TN}{N} \tag{1}$$

$$FAR = \frac{FN}{N} \tag{2}$$

$$FRR = \frac{FP}{N} \tag{3}$$

Table 1. Confusion Matrix

Sample Category	Discrimination Category	
	Negative Class	Positive Class
Positive Class	FN	TP
Negative Class	TN	FP

To thoroughly validate the proposed scheme’s effectiveness and feasibility, we conducted extensive numerical simulations and experimental investigations. Numerical simulations provide

synthetic datasets that mimic real-world scenarios, offering a controlled environment for initial testing and analysis. Experimental explorations, on the other hand, reveal the behavior of optical spectrum data under actual conditions, thus validating the simulation outcomes. By integrating these methods, we achieve a comprehensive understanding of the spectral features' effectiveness and their practical application in real IP over optical network environments.

3. Synthetic data simulation and result analysis

The simulation to collect the dataset for machine learning algorithms follows the process shown in Fig. 3. This involves segmented data collection, division, pre-processing, conversion, and spectral data acquisition. The data representing both DoS attacks and normal network activity, as shown in Fig. 3, are sourced from the DARPA 1998 dataset, courtesy of MIT labs. This dataset is particularly valuable as it includes comprehensive TCP dump files, allowing for an in-depth analysis of packet contents.

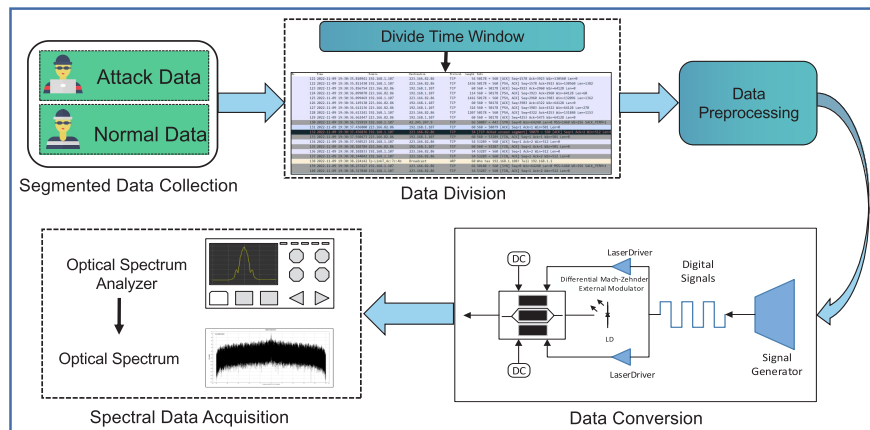


Fig. 3. Simulation setup for collecting the spectrum data

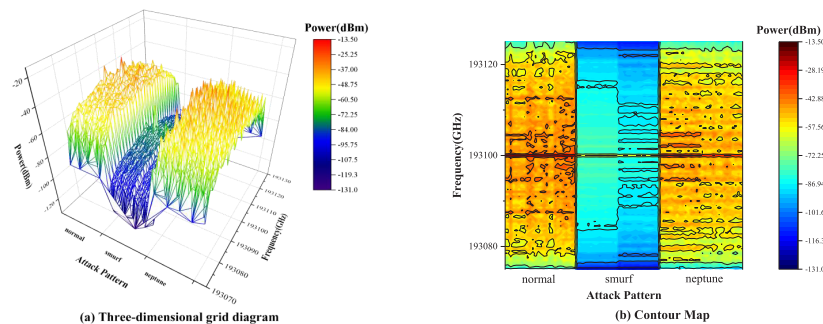
Based on the attack log table in [16], we selected segments of DoS attack data (specifically Smurf and Neptune attacks) and normal data from a five-week dataset, as detailed in Table 2. We chose eight periods of attack data and one of normal data. Noting the regular patterns in network data during DoS attacks, we selected a representative period from each attack dataset to simplify computations. These data were then segmented into 500 ms time windows, resulting in 1015 sets of DoS attack data and 500 sets of normal data for our sample dataset. Using Wireshark software, we then extracted detailed packet information such as IP addresses, content, and byte size from each data set. This data underwent preprocessing into byte format, followed by conversion into optical signals through an electro-optical modulation module. Spectral data extraction was then performed using an optical spectrum analyzer. Upon completion of data extraction and processing, each data set was labeled for identification, with attack data marked as '1' and normal data as '0'.

Figure 4 illustrates the comparison of optical spectrum data under Smurf attack, Neptune attack and normal data. Figure 4(a) represents the three-dimensional grid diagram of optical spectrum data in the measured frequency range (193.07 THz-193.13 THz), and Fig. 4(b) represents the contour map of optical spectrum data in this frequency range. It can be seen from Fig. 4(a) that the optical spectrum energy of the Smurf attack is consistently at lower energy compared with that of the normal data and the Neptune attack in the whole measured frequency ranges. Whereas the optical spectrum of the normal data and the Neptune attack have similar energy distributions. Nevertheless, it can still be seen from Fig. 4(b) that the optical spectrum of Neptune attack has

Table 2. Confusion Matrix

Serial number	Week	Day	Attack Name	Time Of Duration(s)
1	1	Wed	Smurf	36
2	3	Wed	Smurf	70
3	3	Thurs	Neptune	3670
4	5	Mon	Smurf	1866
5	5	Thurs	Neptune	3308
6	5	Thurs	Smurf	1914
7	5	Fri	Neptune	2238
8	5	Fri	Smurf	758
9	3	Tues	Normal	all

more concentrated energy in the frequency range, while the optical spectrum of normal data has more uniform energy distribution. Therefore, it can be concluded that the optical spectrum characteristics of the data will be changed to a certain extent when a DoS attack occurs, which confirms the feasibility of using the optical spectrum characteristics as a feature for detecting DoS attacks.

**Fig. 4.** Comparison of spectral data in simulation

Next, we evaluate the performance of DoS attack detection on the three classification algorithms, i.e., XGBoost, LightGBM and the BP neural network. A total of 1515 sets of optical spectrum samples are collected for the simulation, each of which has a feature dimension of 5000. The dataset division ratio of the training set and test set is 7:3. The three classification algorithms mentioned above were trained separately, and the optimal training results are taken as the performance comparison evaluation of attack detection. The confusion matrix comparison graph for validating the trained models with the test set is shown in Fig. 5. It can be seen that the test set has low FP, and low FN on all three algorithms. It means that using the optical spectrum data as features for prediction, all three algorithms have low false positive rates and can achieve accurate prediction of the results. Among them, the BP neural network algorithm has an optimal test result with an FN value of 0 and an FP value of 2 after validation on 454 test sets.

Figure 6 presents a comparative analysis of the ACC, FPR and FNR for the XGBoost, LightGBM, and BP neural network algorithms on the test set. It can be seen that XGBoost, LightGBM, and the BP neural network achieve detection accuracies of 97.39%, 98.02%, and 99.55%, respectively. The FPR and FNR for XGBoost are observed at 0.72% and 1.89%, and for LightGBM at 0.99% and 0.99%, respectively. Remarkably, the BP neural network demonstrates significantly lower rates, with FPR and FNR at 0% and 0.45%, respectively. Overall, the BP neural network outperforms in all three evaluation metrics. In Fig. 7, we show the variation in

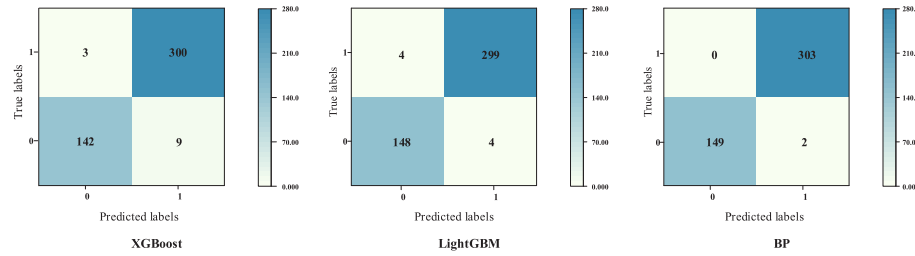


Fig. 5. Comparison of spectral data in the simulation

detection accuracy and loss during the BP neural network’s training process across 100 iterations. Notably, both accuracy and loss stabilize after about 40 iterations. This pattern indicates that the BP neural network algorithm exhibits strong convergence properties and is easy to implement.

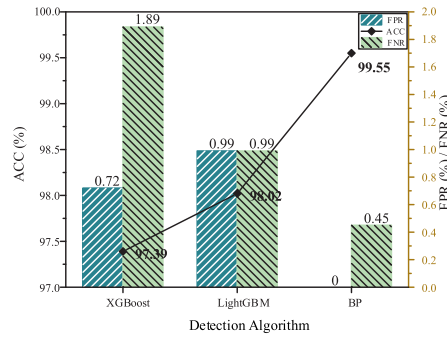


Fig. 6. Performance comparison in the simulation

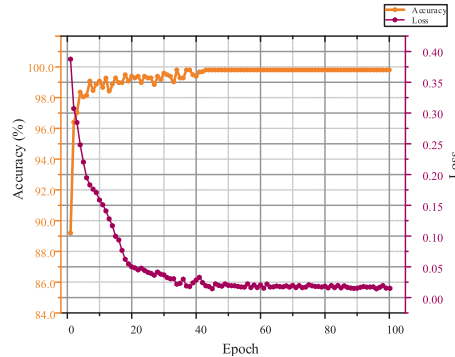


Fig. 7. Accuracy and loss of the BP neural network vary with iterations in the simulation

4. Practical experiments and results analysis

In this section, we present the experimental setup of DoS attacks depicted in Fig. 8. In particular, Fig. 8(a) gives the network topology link of the experimental platform, which mainly consists of a legitimate user (P1) and a server (S0), two switches (SW) together with two optical modules (OMs) connected by a standard single-mode fiber (SSMF) with the length of 20 km for normal data transmission. Additionally, an attacker (P2) is configured to initiate DoS attacks, while an

optical spectrum analyzer (OSA) is accessed via an optical splitter to capture spectral data for attack detection.

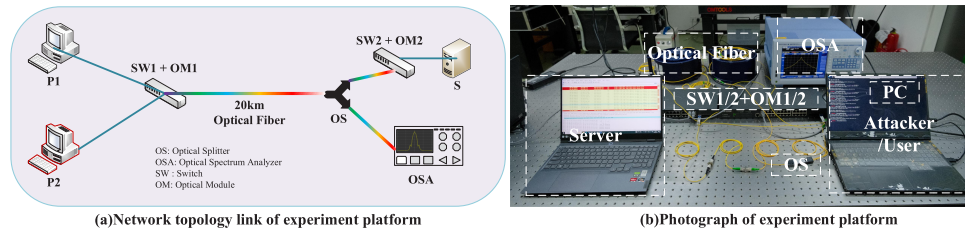


Fig. 8. Experimental setup

The experimental platform, as illustrated in Fig. 8(b), incorporates a PC dual-booting Windows 11 and Kali Linux via a virtual machine. Here, Windows 11 functions as a legitimate user, sending standard data through SW1 and OM1, then via the SSMF to the server after passing through OM2 and SW2. Conversely, Kali Linux serves as the attacker's tool, executing a remote DoS attack (TCP Flood) by sending numerous TCP requests to the server using the hping3 tool. Real-time optical spectrum data are monitored and gathered by the OSA through an optical splitter. Table 3 provides detailed parameter settings and descriptions of the experimental devices.

Table 3. Parameter settings and descriptions of the experimental devices

Grade	Device	Operating system/Device model	Device function
P1	User	Windows11	Send normal data
P2	Attacker	Kali Linux	Send attack data
SW	Switch	TL-SH5428	Forward data
OM	Optical Module	SFP-10G-ER	Perform photoelectric/electro-optical conversion
OS	Optical Splitter	PLC Splitter	Realize the splitting of the optical signal
S	Server	Windows11	Receive data
OSA	Optical Spectrum Analyzer	YOKOGAWA AQ6370D	Monitoring and collecting the optical spectrum data

In our experiment, the OSA collects optical spectrum data every 100ms, resulting in 1300 sets of samples. This includes 800 sets of attack spectral data and 500 sets of normal spectral data, of which 200 sets are collected without server side data transmission. With the OSA's 0.01 nm resolution, 0.001 nm sampling rate, and 0.5 nm range, each data set comprises 501 sampling points, translating to 501 feature dimensions per optical spectrum data set.

Figure 9 examines the characteristics of the collected optical spectrum data. While some differences are observed in normal data with and without transmission, distinguishing the attack spectrum from the normal spectrum in Fig. 9(a) and Fig. 9(b) is less apparent. Nevertheless, a discernible difference exists between the attacked and normal signal spectra. Utilizing these spectral characteristics, correlations in the optical spectrum data can be analyzed to quickly determine the presence of an attack, once the data is fed into machine learning models.

Mirroring the approach used in our synthetic data simulations, we divided the experimental dataset into training and test sets with a 7:3 ratio. We then assessed the performance of the XGBoost, LightGBM, and BP neural network algorithms. Figure 10 displays a comparative analysis of their confusion matrices. Compared with Fig. 5 in the simulations, the FNR and

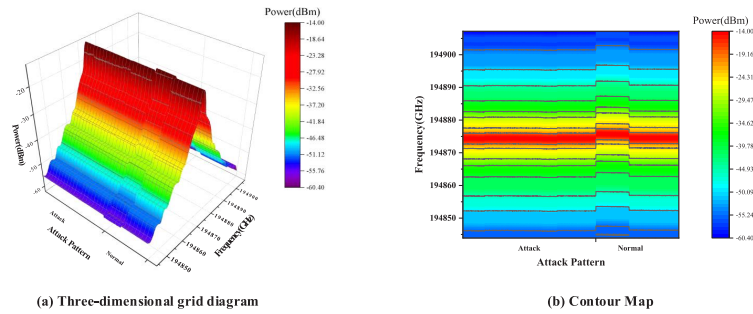


Fig. 9. Comparison of spectral data in the experiment

FP of the three algorithms in the experiment have been reduced, and the BP neural network algorithm is still optimal results with the FN value of 0 and the FP value of 1. The performance comparison of the ACC, FNR and FPR is shown in Fig. 11. It can be seen that the ACC of XGBoost, LightGBM and the BP neural network on the test set reaches 99.23%, 99.48% and 99.74%, respectively, which also has a certain improvement compared with the accuracy in the simulation. The FNR and FPR of XGBoost, LightGBM, and the BP neural network are reduced to 0.26%, 0.51%, 0.26%, 0.26%, and 0.26%, 0, respectively. Across these metrics, the BP neural network consistently exhibits optimal performance among the evaluated models.

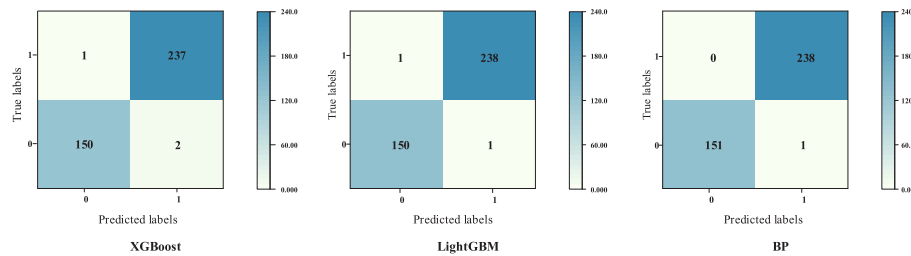


Fig. 10. The comparison of the confusion matrix in the experiment

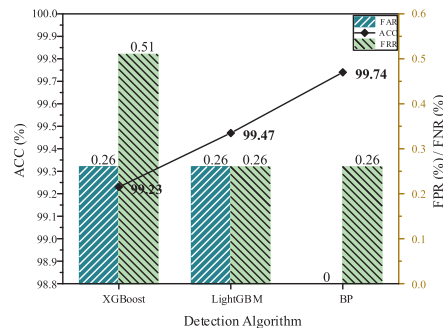


Fig. 11. Performance comparison in the experiment

Additionally, Fig. 12 illustrates the variation in detection accuracy and loss for the BP neural network algorithm over the course of its iterations. The algorithm undergoes 50 training iterations, with both accuracy and loss stabilizing after just 10 iterations. These results underscore the high detection accuracy, low false positive rate, and low false negative rate achieved when using

optical spectrum data as a detection metric. This consistency in performance further reinforces the viability and reliability of optical spectrum data as an effective tool for DoS attack detection.

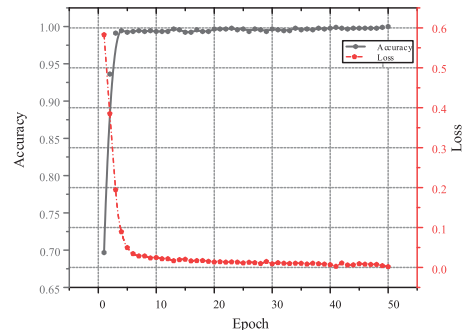


Fig. 12. Accuracy and loss vary with iterations in the experiment

5. Conclusion

In this paper, the potential of using machine learning for optical spectrum feature analysis to detect DoS attacks in IP over optical networks has been investigated through synthetic data simulations and practical experiments. A DoS attack detection system was developed based on machine learning and optical spectrum analysis. Simulation and experimental environments were set up to acquire optical spectrum data under normal conditions and DoS attacks. Using this dataset, three machine learning algorithms XGBoost, LightGBM, and a BP neural network were evaluated for attack detection accuracy, false positive rate, and false negative rate. The results showed all three machine learning models achieved over 97% detection accuracy. Further comparison found the BP neural network to be best suited for detecting DoS attacks. This work demonstrates a simple and effective way to achieve DoS attack detection. By leveraging optical spectrum analysis in the underlying optical network, DoS attacks can be identified earlier, before photoelectric conversion, reducing pressure on electronic processing.

Funding. National Key Research and Development Program of China (2023YFB2906200); National Natural Science Foundation of China (62075024, 62201105, 62205043, 62025105, 62221005, 62222103, 62331017); Chongqing Municipal Education Commission (CXQT21019, KJQN202100643).

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

References

1. R. S. Tucker, R. Parthiban, J. Baliga, *et al.*, "Evolution of WDM Optical IP Networks: A Cost and Energy Perspective," *J. Lightwave Technol.* **27**(3), 243–252 (2009).
2. V. Viscardi, D. Schroetter, and M. Kattan, "Routed Optical Networking: an alternative architecture for IP+Optical aggregation networks," in *2022 International Conference on Optical Network Design and Modeling (ONDM)*, (2022), pp. 1–4.
3. M. Garrich, J. L. Romero-Gázquez, F. J. Moreno-Muro, *et al.*, "Joint Optimization of IT, IP and WDM Layers: From Theory to Practice," in *2020 International Conference on Optical Network Design and Modeling (ONDM)*, (2020), pp. 1–4.
4. Y. H. Lu, S. H. Y. Hsiao, C. Y. Li, *et al.*, "Insecurity of Operational IMS Call Systems: Vulnerabilities, Attacks, and Countermeasures," *IEEE/ACM Trans. Networking* **31**(2), 800–815 (2023).
5. M. Wakaiki, A. Cetinkaya, and H. Ishii, "Stabilization of Networked Control Systems Under DoS Attacks and Output Quantization," *IEEE Trans. Autom. Control* **65**(8), 3560–3575 (2020).
6. N. Ashodia and K. Makadiya, "Detection and Mitigation of DDoS attack in Software Defined Networking: A Survey," in *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, (2022), pp. 1175–1180.

7. N. G. B. Amma, S. Selvakumar, and R. L. Velusamy, "A Statistical Approach for Detection of Denial of Service Attacks in Computer Networks," *IEEE Trans. Netw. Serv. Manage.* **17**(4), 2511–2522 (2020).
8. J. Chen, L. Yang, and Z. Qiu, "Survey of DDoS Attack Detection Technology for Traceability," in *2022 IEEE 4th Eurasia Conference on IOT, Communication and Engineering (ECICE)*, (2022), pp. 112–115.
9. Y. Lui, G. Shen, and W. Shao, "Energy-minimized design for IP over WDM networks under modular router line cards," in *2012 1st IEEE International Conference on Communications in China (ICCC)*, (2012), pp. 266–269.
10. J. Gossels, G. Choudhury, and J. Rexford, "Robust network design for IP/optical backbones," *J. Opt. Commun. Netw.* **11**(8), 478–490 (2019).
11. S. Liu, W. Lu, and Z. Zhu, "On the cross-layer orchestration to address IP router outages with cost-efficient multilayer restoration in IP-over-EONs," *J. Opt. Commun. Netw.* **10**(1), A122–A132 (2018).
12. Y. Li, N. Hua, J. Li, *et al.*, "Optical spectrum feature analysis and recognition for optical network security with machine learning," *Opt. Express* **27**(17), 24808–24827 (2019).
13. X. Chen, C. Y. Liu, R. Proietti, *et al.*, "Automating Optical Network Fault Management with Machine Learning," *IEEE Commun. Mag.* **60**(12), 88–94 (2022).
14. X. Pan, H. Yang, Z. Xu, *et al.*, "Adversarial Analysis of ML-Based Anomaly Detection in Multi-Layer Network Automation," *J. Lightwave Technol.* **40**(15), 4934–4944 (2022).
15. X. Chen, B. Li, R. Proietti, *et al.*, "Self-Taught Anomaly Detection With Hybrid Unsupervised/Supervised Machine Learning in Optical Networks," *J. Lightwave Technol.* **37**(7), 1742–1749 (2019).
16. R. P. Lippmann, D. J. Fried, I. Graf, *et al.*, "Evaluating intrusion detection systems: the 1998 DARPA off-line intrusion detection evaluation," in *Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00*, (2000), pp. 12–26 vol.2.
17. M. Du, "Economic Forecast Model and Development Path Analysis Based on BP and RBF Neural Network," in *2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT)*, (2023), pp. 619–624.
18. Y. Sun, C. Song, S. Yu, *et al.*, "A Novel Genetic Algorithm-XGBoost Based Intrusion Detection Method," in *2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, (2021), pp. 1–5.
19. W. Tong, B. Liu, Z. Li, *et al.*, "Intrusion Detection Method of Industrial Control Network Based on Lightgbm," in *2021 International Conference on Communications, Information System and Computer Engineering (CISCE)*, (2021), pp. 631–635.