Original article
UDK 004.492.3
https://doi.org/10.24143/2072-9502-2024-3-65-74
EDN ODPOMX

An approach to configuring CatBoost for advanced detection of DoS and DDoS attacks in network traffic

Abdulkader Hajjouz*✉, *Elena Yu. Avksentieva

ITMO University,
Saint Petersburg, Russia, hajjouz@itmo.ru✉

Abstract. In the ever-evolving landscape of network security, the sophistication of cyber-attacks, especially Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, poses a formidable challenge to intrusion detection systems. Recognizing the longstanding application of CatBoost in various domains, this study explores its novel optimization for network intrusion detection, a critical area in need of advanced solutions. Leveraging the strengths of CatBoost in handling categorical data and imbalanced datasets, we meticulously adapt the classifier to meet the complex demands of distinguishing between DoS, DDoS, and benign traffic within the comprehensive CICIDS2017 and CSE-CIC-IDS2018 datasets. This research is an attempt to refine the learning efficiency and detection capabilities of CatBoost through the implementation of advanced feature selection and data preparation, contributing to the field by improving detection accuracy within real-time intrusion detection systems. The results show a notable improvement in performance, underscoring the classifier's role in advancing cybersecurity measures. Furthermore, the study paves the way for future exploration into adversarial machine learning and automated feature engineering, fortifying the resilience and adaptability of intrusion detection systems against the backdrop of a rapidly changing cyber threat landscape. These efforts provide solid approaches to address the current challenges in network security, signaling a move towards more refined and dependable intrusion detection methods.

Keywords: DoS, DDoS, network intrusion detection, information security, machine learning, feature selection

For citation: Hajjouz A., Avksentieva E. Yu. An approach to configuring CatBoost for advanced detection of DoS and DDoS attacks in network traffic. *Vestnik of Astrakhan State Technical University. Series: Management, computer science and informatics*. 2024;3:65-74. (In Russ.). https://doi.org/10.24143/2072-9502-2024-3-65-74. EDN ODPOMX.

Научная статья

Подход к настройке CatBoost для продвинутого обнаружения атак DoS и DDoS в сетевом трафике

Абдулкадер Хажжуз*✉, *Елена Юрьевна Авксентьева

Национальный исследовательский университет ИТМО,
Санкт-Петербург, Россия, hajjouz@itmo.ru✉

Аннотация. В постоянно развивающемся ландшафте угроз сетевой безопасности сложность кибератак, особенно атак типа «отказ в обслуживании» (DoS) и распределенных атак «распределенная атака отказа в обслуживании» (DDoS), представляет собой значительный вызов для систем обнаружения вторжений. Учитывая долгое применение библиотеки градиентного бустинга CatBoost в различных областях, в данном исследовании рассматривается оптимизация ее алгоритма для обнаружения сетевых вторжений – критически важной области, нуждающейся в передовых решениях. Используя преимущества CatBoost в обработке категориальных данных и несбалансированных наборов данных, мы тщательно адаптируем этот классификатор для удовлетворения сложных требований различения между DoS, DDoS и благонадежным трафиком в рамках обширных наборов данных CICIDS2017 и CSE-CIC-IDS2018. Это исследование – попытка улучшить эффективность обучения и возможности обнаружения вторжений алгоритмом CatBoost в реальном времени. Результаты показывают заметное улучшение производительности, подчеркивая роль алгоритма классификатора в продвижении мер кибербезопасности. Кроме того, исследование прокладывает путь для дальнейшего изучения состязательного машинного обучения и автоматизированного инжиниринга признаков, укрепляя устойчивость и адаптивность систем обнаружения вторжений на фоне быстро меняющегося ландшафта киберугроз. Эти усилия предоставляют надежные подходы к решению текущих вызовов в сетевой безопасности, сигнализируя о движении к более усовершенствованным и надежным методам обнаружения вторжений.

Ключевые слова: DoS, DDoS, обнаружение сетевых вторжений, информационная безопасность, машинное обучение, выбор функций

Для цитирования: *Хажжуз А., Авксентьева Е. Ю.* Подход к настройке CatBoost для продвинутого обнаружения атак DoS и DDoS в сетевом трафике // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2024. № 3. С. 65–74. https://doi.org/10.24143/2072-9502-2024-3-65-74. EDN ODPOMX.

Introduction

In the evolving digital landscape, the escalation of sophisticated cyber threats, notably Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, presents a significant challenge to cybersecurity defenses [1, 2]. The primary obstacle is the increasing complexity in distinguishing malicious network traffic from the vastly more prevalent benign activities, a task complicated by the rapid evolution of cyberattack methodologies [3]. This challenge is further intensified by the inherent imbalance in network traffic datasets, where benign traffic significantly outnumbers instances of attacks, thus complicating the training and accuracy of detection models [4].

In response to this critical challenge, our research proposes an innovative approach through the application of the CatBoost classifier, a machine learning algorithm known for its proficiency in managing categorical data and datasets with imbalanced classes [5]. Utilizing the comprehensive and diverse scenarios presented in the CICIDS2017 and CSE-CIC-IDS2018 datasets [6, 7], this study aims to significantly enhance the accuracy and efficiency of intrusion detection systems. Our methodology focuses on meticulously optimizing the CatBoost classifier to accurately identify and classify DoS, DDoS, and benign traffic, thereby overcoming the challenges posed by dataset imbalance and the subtleties of network behavior.

Despite significant advances in technology aimed at thwarting and mitigating DDoS (Distributed Denial of Service) attacks, data from NETSCOUT's DDoS Threat Intelligence Report indicates a concerning trend: around 7.9 million DDoS attacks were recorded in the initial six months of 2023. This figure marks a 31% increase compared to the previous year, underscoring the critical and growing necessity for enhancing intrusion detection methodologies. Our work contributes to this pressing need by significantly improving the model's performance in detecting network intrusions through refined CatBoost classifier configurations and data preparation and feature selection techniques.

The contributions of our research are twofold: Firstly, it offers a scalable, precise, and efficient solution to bolster cybersecurity measures against evolving digital threats. Secondly, initial results suggest a notable improvement in detection accuracy, contributing to advancements in the standards for real-time intrusion detection systems. This paper outlines our comprehensive methodology, from data analysis and model tuning to the validation of our approach, demonstrating a significant stride towards mitigating the challenge of accurately identifying cyber threats within highly imbalanced and complex datasets.

Related work

The domain of network intrusion detection is witnessing rapid evolution, propelled by advanced machine learning and deep learning techniques. This section critically reviews seminal contributions to the field, situating our research within this dynamic landscape and underscoring the distinctive advantages of our approach with the CatBoost classifier.

Manimurugan et al. [8] leveraged a Deep Belief Network (DBN) algorithm to develop a deep learning-based intrusion detection system, applied to the CICIDS2017 dataset. Their work demonstrates the potential of deep learning in identifying a broad spectrum of cyber threats, achieving notable success across various attack vectors. This underscores the increasing relevance of deep learning in cybersecurity, yet it also highlights a critical gap-efficient handling of imbalanced datasets and categorical data.

Exploring the effectiveness of Machine Learning (ML) techniques, Farhat and colleagues [9] investigated the detection of DoS/DDoS attacks within cloud environments using the CICIDS2017 dataset. Their findings spotlight the eXtreme Gradient Boosting (XGBoost) algorithm's high performance, validating the potential of ML in this context. However, they also signal the need for ML techniques that expand the detectable attack spectrum and enhance real-time detection capabilities.

Abu Bakar et al. [10] presented an agent-based detection system focusing on automatic feature extraction and selection for DDoS attack detection. Their methodology achieved significant accuracy improvements, showcasing the power of combining ML techniques with feature selection.

Dora et al. [11] explored the synergy between Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) models for DDoS attack detection, emphasizing the importance of optimal feature selection. While their approach demonstrates the potential of deep learning models in cybersecurity, it also reveals the complexity of deploying such models in real-time environments.

Building on existing research, our application of the CatBoost classifier not only enhances network intrusion detection by addressing the challenges of imbalanced datasets and categorical data but also demonstrates superior results with a high processing speed. This combination of improved accuracy and efficiency positions our study as a valuable advancement in the pursuit of more adaptable, precise, and swift cybersecurity solutions.

Datasets

Our investigation leveraged the CICIDS2017 and CSE-CIC-IDS2018 datasets, reputable sources of simulated network traffic data that incorporate a wide range of cyberattack scenarios. These datasets were developed collaboratively by the Canadian Institute for Cybersecurity and the Communications Security Establishment (CSE), embodying a diverse array of both benign and malevolent network behaviors which are essential for training robust intrusion detection systems.

CICIDS2017 offers a rich mix of network traffic, including a week-long simulation of regular activities peppered with orchestrated attacks. In contrast, the CSE-CIC-IDS2018 dataset is known for its inclusion of evolved cyber threats, reflecting the progressive complexity of cyberattacks [6, 7].

Each dataset contains 79 features that describe the complex nature of network traffic in detail, allowing for a sophisticated analysis of network behavior. These features are instrumental in characterizing the various aspects of network behavior, facilitating a nuanced approach to the classification of network activities. In our analysis, network activities were aggregated into three overarching classes for simplicity and focus:

– “Benign”: Normal network traffic, devoid of any malicious intent;

– “DoS” (Denial of Service): Aggregates various forms of DoS attacks such as Hulk, GoldenEye, and Slowloris;

– “DDoS” (Distributed Denial of Service): Encompasses various DDoS strategies including those using High Orbit Ion Cannon (HOIC), Low Orbit Ion Cannon (LOIC) over HTTP and UDP, and LOIT.

The classification reflects a targeted approach to discern the intricate patterns of network attacks and provides a streamlined framework for the development of detection algorithms. By consolidating similar attack methodologies into broader categories, our model can efficiently learn to differentiate between benign traffic and malicious attacks, which is paramount for deploying effective real-time intrusion detection systems. Table 1 presents a comparison of instance counts across the CICIDS2017 and CSE-CIC-IDS2018 datasets, revealing the distribution between benign and malicious traffic.

Table 1

Comparison of Instance Counts by Class in Network Intrusion Datasets

Class	Number of Instances		
	CICIDS2017	CSE-CIC-IDS2018	CICIDS2017 + CSE-CIC-IDS2018
Benign	537,749	9,176,239	9,713,988
DDOS	128,027	1,263,933	1,391,960
DOS	252,661	654,300	906,961

The numbers in Table 1 represent the counts of instances for each class in the respective datasets.

The deliberate selection of these datasets, coupled with the comprehensive set of features they offer, lays a solid foundation for the development and validation of a sophisticated intrusion detection model. Our methodology is designed to leverage the depth and breadth of the available data, ensuring robustness and efficacy in the detection of network anomalies.

Data preparation

To elevate the reliability of our intrusion detection outcomes, it's crucial to enhance our dataset's integrity through a comprehensive data preparation strategy. This essential stage includes three key actions: normalizing outliers, correcting negative values, and refining the dataset's framework. Adjusting for outliers helps maintain the balance and genuine nature of the dataset, ensuring its core characteristics are preserved. Correcting negative values by averaging out column data aids in creating a consistent dataset, which in turn, supports more accurate distinctions between benign and malicious network behavior. Refining the structure of the dataset is critical for improving our ability to classify network activities accurately. These preparatory measures not only serve to optimize the dataset but also significantly bolster the reliability and sharpness of our detection mechanisms. Emphasizing the dataset's integrity through this detailed process is fundamental in advancing our system's efficacy and trustworthiness, an imperative in the continuously advancing field of cybersecurity.

Feature selection strategies

In the intricate domain of cyber intrusion detection, the strategic selection of features is paramount. These features, crucial for identifying data patterns, must be relevant, distinct, and enhance the model's predictive accuracy [12]. This selection process bolsters machine learning model efficiency, reduces computational load, and simplifies model comprehension. Initial steps include the elimination of constant features through variability assessment, using standard deviation measures to discard those with no variation. Non-contributory attributes, like 'timestamp', are also excluded to avoid introducing unnecessary variability. Further, the examination of feature relationships through Spearman rank-order correlation and the use of heatmaps and hierarchical clustering, especially employing the Ward linkage method, facilitate the understanding of feature interconnections and groupings. Finally, cluster-based feature consolidation employs a correlation-based clustering approach to group features, selecting the most representative feature from each cluster to maintain essential information while reducing dimensionality, thereby ensuring the selected features aptly represent each cluster's characteristics.

The Fig. 1 visualizes the rigorous process of feature selection, from the initial removal of constant features to the final stage of cluster-based feature consolidation, culminating in a refined set of significant features.

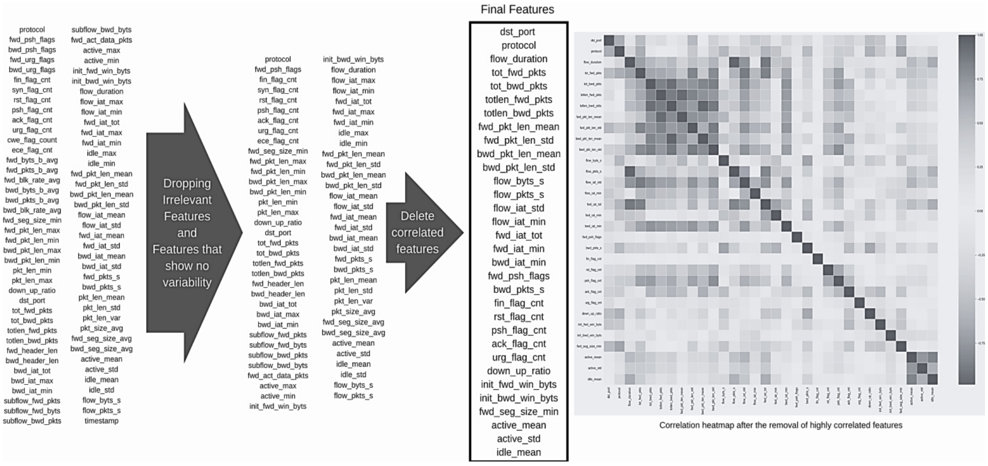


Fig. 1. Feature selection process and correlation analysis in network traffic data

Following this comprehensive selection process, the dataset is refined to its most significant 32 features.

This refinement not only simplifies the dataset but also prepares it for a more streamlined and effective model training process. The resultant set of features is both manageable and rich in information, striking an optimal balance between computational efficiency and the accuracy of the predictive model.

Stratified sampling

In our detailed exploration, we employed a stratified sampling method to segment the dataset into training (80%), validation (10%), and testing (10%) portions, as outlined in Table 2.

Table 2

Distribution of Network Traffic Classes in Training, Evaluation, and Testing Sets

Set	Benign	DOS	DDOS
Train	7,771,190	725,569	1,113,568
Eval	971,399	90,696	139,196
Test	971,399	90,696	139,196

The values in Table 2 represent counts of instances for each class.

This method was carefully chosen to ensure proportional representation of each class across these segments, adhering to the formula for balanced allocation:

$$n_k = (N \cdot N_k) / N_{tot} \quad (1)$$

with in the equation (1), n_k – represents the sample size allocated to each class k within a given subset; N is the total number of samples in that subset; N_k – indicates the total number of samples for class k across the dataset, and N_{tot} is the total number of samples in the dataset [13].

The approach described ensures that each class – Benign, DoS, and DDoS – is represented proportionally within each subset (training, validation, and testing) of the dataset. This means that the stratified sampling method is designed to maintain the same distribution of classes across all subsets as is present in the full dataset.

Model configuration and training

In our exploration of machine learning applications within cybersecurity, particularly for network intrusion detection, the configuration and subsequent training of the model are critical to its success. For this purpose, we chose the CatBoostClassifier, a decision tree-based ensemble model noted for its exceptional performance with categorical data and its adept handling of imbalanced datasets [5].

Central to our model's configuration was the implementation of class weights, specifically set to {“Benign”: 1.2366609232305477, “DDOS”: 8.630211177045318, “DOS”: 13.245228227777096}. These weights were carefully calculated to counterbalance the disproportionate representation of classes within our dataset, ensuring that the model adequately learns from each category despite the inherent imbalance. Such a measure is crucial in cybersecurity contexts, where failing to detect rare but dangerous threats could have significant repercussions.

Our model configuration was meticulously designed to optimize performance while preventing overfitting – a critical consideration given the complexity of our task. After thorough experimentation, we configured the model with 1,300 iterations. This specific number of iterations was chosen to strike an optimal balance between adequate learning and computational efficiency. Extensive testing indicated that fewer iterations led to underfitting, while significantly more iterations did not yield proportional performance improvements and risked overfitting. We set the learning rate to 0.1 to ensure robust model training without overfitting, complemented by a depth of 6 to capture complex patterns within the data effectively. The model employed a MultiClass loss function, suitable for our multi-class classification task, and was trained on a GPU to leverage accelerated computational capabilities, thereby reducing training time.

Recognizing the importance of reproducibility and consistency in scientific research, we fixed the random seed at 42. Additionally, we adjusted the L2 leaf regularization to 4 and maintained a border count of 1,024, balancing the model's accuracy with training speed. Extensive experimentation showed that 1,024 provided the optimal balance, as lower counts reduced precision and higher counts unnecessarily increased training time. To further mitigate overfitting, we implemented early stopping after 100 rounds without improvement, allowing the model to halt training once no significant gain in performance was observed, thereby conserving computational resources.

The choice of evaluation metric was Total F1, selected for its relevance in assessing models trained on imbalanced datasets like ours, where precision and recall are equally important. The model's configuration also included specific class weights for “Benign”, “DDOS”, and “DOS” classes, derived from their distribution in the dataset, to address the inherent class imbalance and ensure fair representation of each class during the learning process.

During training, the model underwent evaluation on a separate validation set, with an early stopping mechanism based on the Total F1 metric to prevent overfitting and ensure optimal performance. This method led to notable achievements: a best test Total F1 score of 0.9999911775 at iteration 735. This strategy not only validated our hyperparameter selection but also showcased the CatBoost algorithm's capability to manage complex, imbalanced datasets effectively.

Result analysis and discussion

In contexts where it's essential to categorize into various groups, confusion matrices are key to assessing the performance of machine learning algorithms on a testing dataset. This is especially true for evaluating network intrusion detection systems, where such matrices are vital for gauging the system's capability to differentiate between diverse forms of network activity, including normal traffic, Distributed Denial of Service (DDoS), and Denial of Service (DoS) attacks, as illustrated in Table 3.

Table 3

Confusion Matrix of Intrusion Detection System Predictions on the test set

Actual Class	Pred Benign	Pred DDOS	Pred DOS
True Benign	971,369	8	22
True DDOS	1	139,195	0
True DOS	2	0	90,694

Table 3 shows the count of true and predicted instances for each class, providing insight into the performance of the intrusion detection system.

Derived from the confusion matrix, we obtain essential metrics for evaluating the performance of each class within our network intrusion detection analysis:

$$Accuracy = (TP + TN) / (TP + FN + TN + FP); \quad (2)$$

$$Precision = TP / (TP + FP); \quad (3)$$

$$Recall = TP / (TP + FN); \quad (4)$$

$$F1 = 2 \cdot (Precision \cdot Recall) / (Precision + Recall). \quad (5)$$

Accuracy (2): this measures the proportion of true results, both true positives and true negatives, among the entire set of samples.

Precision (3): this metric assesses the fraction of true positive predictions in relation to all positive predictions made, serving as an indicator of the model's precision in avoiding false positive errors.

Recall (4): this quantifies the fraction of true positives detected out of all actual positives, evaluating the model's capacity to correctly identify positive instances.

F1 Score (5): representing the weighted average of Precision and Recall, this metric provides a balanced view of both, offering a singular measure of the model's overall performance.

These metrics are computed for each traffic type-benign, DDoS, and DoS-and then averaged to furnish a holistic view of model performance. These formulas relate to the performance metrics of the model, specifically Accuracy (2), Precision (3), Recall (4), and F1 Score (5).

The performance evaluation of the CatBoost classifier on the test set highlights its exceptional accuracy of 99.9973% and demonstrates its effectiveness in network intrusion detection. The analysis reveals the classifier's proficiency in distinguishing between benign traffic, DDoS, and DoS attacks, evidenced by the high precision, recall, and F1 scores for each category as seen in Table 4.

Table 4

Classification Metrics for Network Traffic Intrusion Detection on the test set

Class	Precision	Recall	F1-score	Support
Benign	1.00000	0.999969	0.999983	971,399
DDOS	0.999943	0.999993	0.999968	139,196
DOS	0.999757	0.999978	0.999868	90,696
accuracy	–	–	0.999973	1,201,291

This evaluation, especially focusing on the F1 scores, is critical in scenarios with imbalanced classes or significant implications for false predictions. The results affirm the model's robustness and reliability in accurately classifying different types of network traffic, underscoring its value as a tool in enhancing cybersecurity measures.

Fig. 2 showcases the Receiver Operating Characteristic (ROC) Curve and Precision-Recall curves for our CatBoost model, tailored for multi-class classification in network intrusion detection, encompassing benign, DDoS, and DoS traffic types.

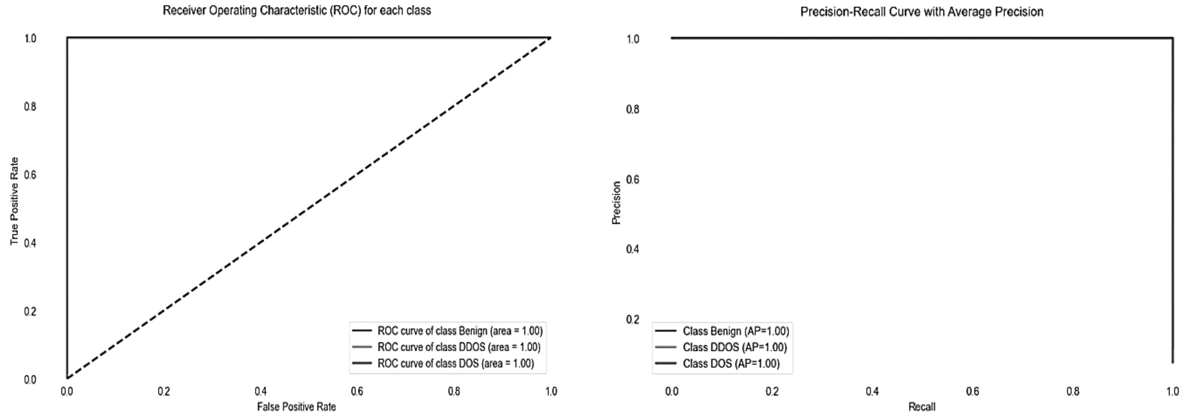


Fig. 2. ROC and Precision-Recall curve

The ROC Curve, included in this combined figure, exhibits a macro-average Area Under the Curve (AUC) of 1.00. This perfect AUC value highlights the model's exceptional performance, illustrating an optimal balance between the True Positive Rate and False Positive Rate across all traffic categories. Such an achievement signals the model's superior discriminative ability to distinctively separate positive from negative class instances without confusion.

Moreover, the Precision-Recall curves, depicted alongside the ROC Curve, display near-perfect Average Precision (AP) scores for each class. In the context of our imbalanced test set, these curves are particularly informative, offering a nuanced view of the model's performance. The AP scores, nearing the ideal mark of 1, emphasize the model's consistent precision across varying levels of recall. This indicates the CatBoost classifier's robustness in correctly identifying instances of each class type-benign, DDoS, and DoS-with a high true positive rate, further validating its efficacy as a dependable tool for network intrusion detection.

The MCC scores, which will be detailed in an upcoming table, underscore the remarkable efficacy of our classifier within the multi-class framework of Benign, DDOS, and DOS traffic types. Given the MCC's value in evaluating performance, especially in imbalanced datasets, these scores as seen in Table 5 reflect the classifier's precision and its strong correlation between predicted and actual classifications.

Table 5

Matthews Correlation Coefficient Scores for Network Intrusion Classification

Metric	Benign	DDOS	DOS	Average
MCC	0.9999	1.0000	0.9999	0.9999

This performance underlines the model's reliability and accuracy, highlighting its suitability for deployment in real-world network intrusion detection scenarios.

The analysis of feature importances from our trained CatBoost classifier as seen in Fig. 3 reveals significant insights into the factors most critical in distinguishing between benign, DDOS, and DOS traffic types.

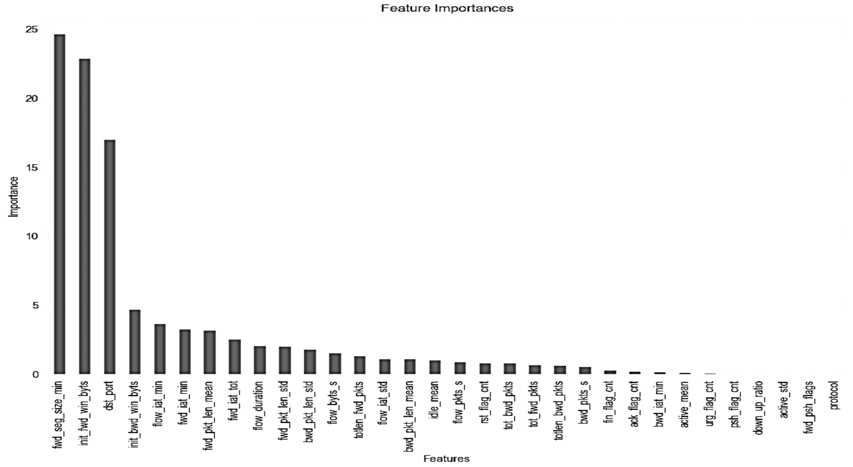


Fig. 3. Bar chart of feature importances in CatBoost classifier

The top features, such as "fwd_seg_size_min", "init_fwd_win_byts", and "dst_port", emerged as highly influential, underscoring their pivotal role in the model's decision-making process. This prioritization reflects the model's reliance on specific aspects of network traffic for accurate intrusion detection. Notably, features related to packet size, initiation windows, and destination ports were deemed most informative, highlighting the nuanced approach required to effectively identify and classify network threats. The derived feature importance rankings offer a clear view into the model's operational dynamics, guiding further refinements and emphasizing areas of focus for enhancing network security measures.

The performance analysis of CatBoost classifier, as illustrated in Fig. 4, reveals its high accuracy in categorizing network traffic into "Benign", "DDOS", and "DOS" segments, using a vast dataset containing 12,012,909 entries.

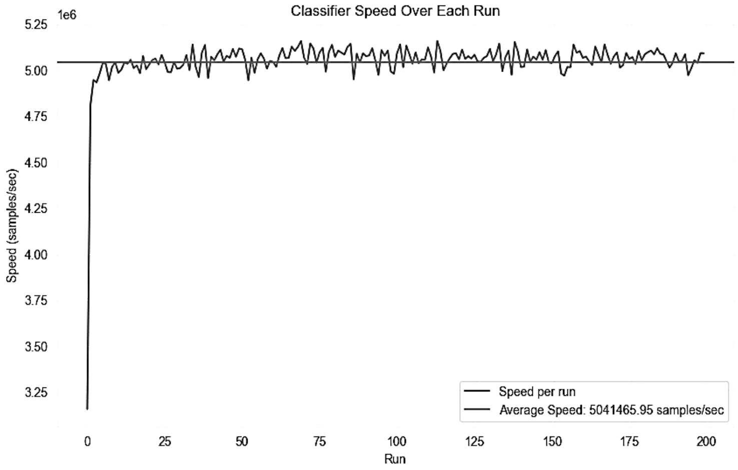
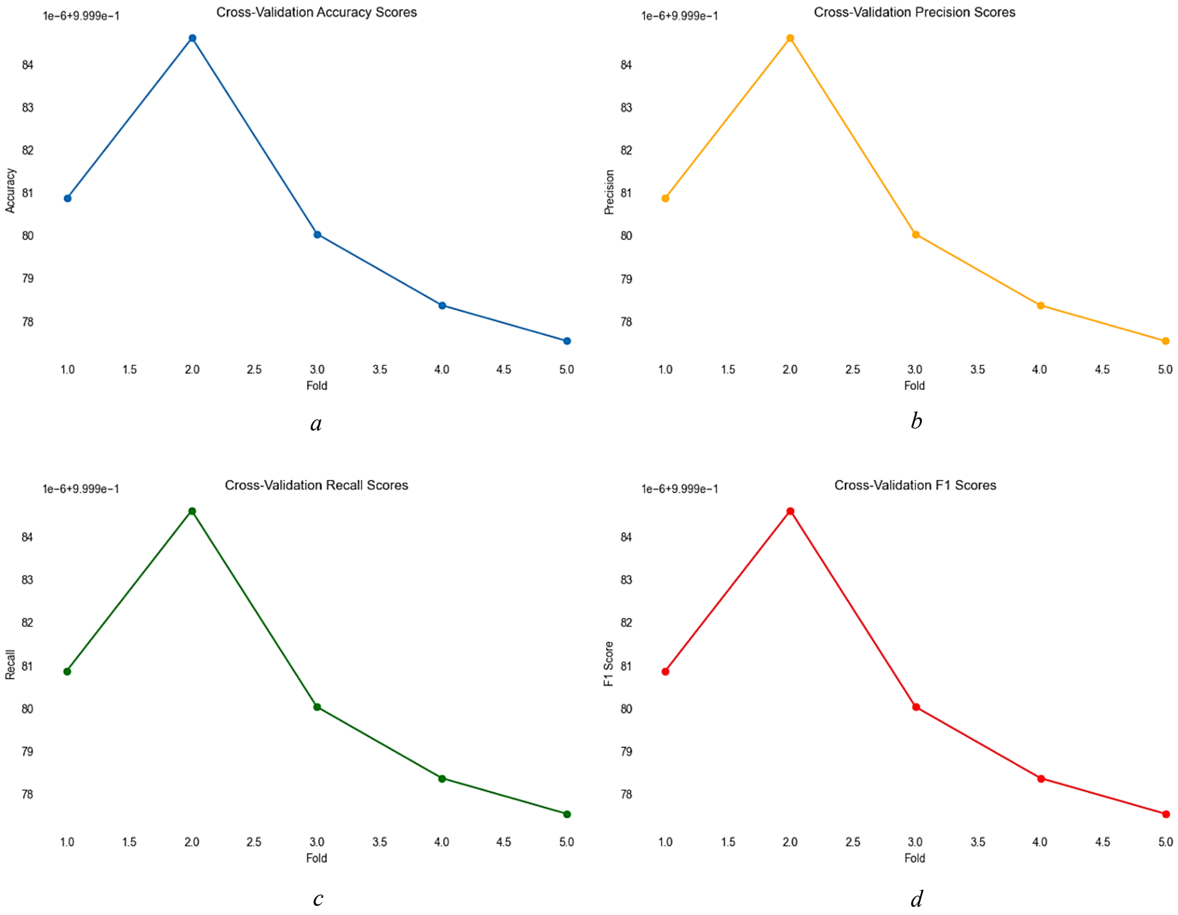


Fig. 4. CatBoost classifier's speed and stability

This evaluation, conducted over 200 iterations, utilized a state-of-the-art computing setup that includes an RTX 3080 GPU, an Intel Core i7 13700k CPU, and 32 GB of DDR5 RAM. The classifier achieved an outstanding average processing speed 5,041,465 samples per second. This level of consistency in processing speed, with very little variation, highlights the classifier's reliability. Such stable and rapid throughput is critical for real-time intrusion detection systems, proving the classifier's efficiency in handling large datasets.

These metrics collectively affirm the CatBoost classifier's robustness and accuracy in a critical application domain like network intrusion detection. The precision in these results, especially considering the dynamic and complex nature of cybersecurity threats, demonstrates the model's advanced capability and readiness for real-world applications. The high degree of performance consistency across different metrics highlights the effectiveness of our model configuration and training approach, cementing the CatBoost classifier's position as an advanced solution in the field of cybersecurity.

The cross-validation results from CatBoost model as seen in Fig. 5 are exceptionally promising, indicating a highly robust and reliable system for network intrusion detection.



a

b

c

d

Fig. 5. Consistently high performance indicators on five folds when detecting network intrusions using the proposed model: *a* – Cross-Validation Accuracy Scores; *b* – Cross-Validation Precision Scores; *c* – Cross-Validation Recall Scores; *d* – Cross-Validation F1 Scores

Across five folds, the model consistently achieved near-perfect metrics, with accuracy, precision, recall, and F1 scores all closely approximating 1.0. Such high values across these metrics demonstrate the model's exceptional capability in correctly identifying and classifying network traffic, including benign, DDOS, and DOS activities. This consistency in performance highlights the effectiveness of the model's training and its potential in deploying a real-world intrusion detection system with high confidence in its predictive accuracy.

In our study, leveraging the combined datasets of CICIDS 2017 and CSE-CIC-IDS2018, the CatBoost classifier has demonstrated high performance in network intrusion detection, achieving overall accuracy, precision, recall, and F1-scores of approximately 99.9973, 99.9975, 99.9972and 99.9973%, respectively. This achievement significantly surpasses the outcomes reported in related work utilizing various techniques on the CICIDS 2017 dataset alone. Notable comparisons as seen in Table 6 include methods like DBN, SVM, RNN, SNN, and FNN, which showed respectable results but did not approach the near-perfect scores of our CatBoost model.

Table 6

Comparison between the proposed model and current research

Ref	Dataset	Technique	Accuracy	Precision	Recall	F1-Score
[8]	CICIDS 2017	DBN	96.67	95.21	97.34	0.9700
		SVM	95.55	94.32	96.15	0.9500
		RNN	94.40	93.91	95.59	0.9400
		SNN	93.30	92.01	94.25	0.9300
		FNN	92.25	91.08	91.13	0.9200
[9]	CICIDS 2017	NB	80.84	81.12	80.84	0.8043
		LR	84.13	86.04	84.13	0.8345
		RF	98.96	98.97	98.96	0.9896
		XGBoost	99.11	99.12	99.11	0.9912
[10]	CICIDS 2017	KNN	99.87	99.84	N/A*	0.9987
[11]	CICIDS 2017	CNN	96.70	97.59	N/A	0.9818
Ours	CICIDS 2017 + CSE-CIC-IDS2018	Catboost	99.9973	99.9975	99.9972	0.999973

* "N/A" indicates that the value is not available for the specific case.

Even algorithms like RF and XGBoost, while reaching high accuracy levels up to 99.12%, still fell short of the benchmarks set by our approach. The KNN technique, while yielding an impressive F1-score of 99.87%, lacks the comprehensive performance validation across all metrics provided by our study. Similarly, the CNN technique, despite its high F1-score of 98.18%, does not match the across-the-board excellence of our CatBoost model.

Conclusion and future directions

Our research has successfully showcased the CatBoost classifier's exceptional capability in detecting network intrusions, effectively distinguishing between DoS, DDoS, and benign traffic with remarkable accuracy. This achievement was made possible through meticulous feature selection, hyperparameter optimization, and class weight adjustment, alongside the utilization of the comprehensive CICIDS2017 and CSE-CIC-IDS2018 datasets. Our rigorous cross-validation process further affirmed the model's reliability and robustness. The classifier's real-time detection prowess marks a significant leap forward in cybersecurity, offering a scalable solution adept at navigating the complexities of modern digital threats. This sets a solid foundation for subsequent research endeavors and practical applications aimed at bolstering network security.

Looking forward, our focus will pivot to integrating adversarial machine learning to enhance the resilience of our classifier against complex threats and to automating feature engineering to dynamically refine predictive features. These initiatives are aimed at ensuring the model's continuous adaptation to the evolving landscape of cyber threats, keeping our cybersecurity measures at the forefront of technological innovation. In essence, our study not only validates the effectiveness of the CatBoost classifier in network intrusion detection but also charts a course for future advancements. By embracing adversarial learning and automated feature engineering, we aim to enhance our proactive defenses against an ever-changing threat landscape, ensuring that our cybersecurity strategies remain robust and forward-thinking.

References

1. Huseinović A., Mrdović S., Bicakci K., Uludag S. A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid. *IEEE Access*, 2020, vol. 8, pp. 177447-177470.

2. Tandon R. A Survey of Distributed Denial of Service Attacks and Defenses. *arXiv preprint*, 2020, arXiv:2008.01345.

3. Li Y., Liu Q. A comprehensive review study of cyberattacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 2021, vol. 7, pp. 8176-8186.

4. Karatas G., Demir O., Sahingoz O. K. Increasing the Performance of Machine Learning-Based IDSs on an Imbalanced and Up-to-Date Dataset. *IEEE Access*, 2020, vol. 8, pp. 32150-32162.

5. Bhati N. S., Khari M. A New Intrusion Detection Scheme Using CatBoost Classifier. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, 2021, pp. 169-176.

6. *Canadian Institute for Cybersecurity. A Realistic Cyber Defense Dataset (CSE-CIC-IDS2018).* Available at: https://registry.opendata.aws/cse-cic-ids2018/ (accessed: 09.10.2023).

7. Sharafaldin I., Habibi Lashkari A., Ghorbani A. A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 2018, pp. 108-116.

8. Manimurugan S., Al-Mutairi S., Aborokbah M. M., Chilamkurti N., Ganesan S., Patan R. Effective Attack Detection in Internet of Medical Things Smart Environment

Using a Deep Belief Neural Network. *IEEE Access*, 2020, vol. 8, pp. 77396-77404.

9. Farhat S., Abdelkader M., Meddeb-Makhlouf A., Zarai F. Evaluation of DoS/DDoS Attack Detection with ML Techniques on CIC-IDS2017 Dataset. *Proceedings of the 9th International Conference on Information Systems Security and Privacy*, 2023, pp. 287-295.

10. Abu Bakar R., Huang X., Javed M. S., Hussain S., Majeed M. F. An Intelligent Agent-Based Detection System for DDoS Attacks Using Automatic Feature Extraction and Selection. *Sensors*, 2023, vol. 23, no. 6, p. 3333.

11. Dora V. R. S., Lakshmi V. N. Optimal feature selection with CNN-feature learning for DDoS attack detection using meta-heuristic-based LSTM. *Int. J. Intell. Robot Appl.*, 2022, vol. 6, no. 2, pp. 323-349.

12. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecur*, 2019, vol. 2, no. 1, pp. 1-22.

13. Kathiravan P., Shanmugavadivu P., Saranya R. Mitigating Imbalanced Data in Online Social Networks using Stratified K-Means Sampling. *2023 8th International Conference on Business and Industrial Research (ICBIR)*, 2023, pp. 883-888.

Список источников

1. Huseinović A., Mrdović S., Bicakci K., Uludag S. A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid // IEEE Access. 2020. V. 8. P. 177447–177470.

2. Tandon R. A Survey of Distributed Denial of Service Attacks and Defenses // arXiv preprint. 2020. arXiv:2008.01345.

3. Li Y., Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments // Energy Reports. 2021. V. 7. P. 8176–8186.

4. Karatas G., Demir O., Sahingoz O. K. Increasing the Performance of Machine Learning-Based IDSs on an Imbalanced and Up-to-Date Dataset // IEEE Access. 2020. V. 8. P. 32150–32162.

5. Bhati N. S., Khari M. A New Intrusion Detection Scheme Using CatBoost Classifier // Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. 2021. P. 169–176.

6. Canadian Institute for Cybersecurity. A Realistic Cyber Defense Dataset (CSE-CIC-IDS2018). URL: https://registry.opendata.aws/cse-cic-ids2018/ (дата обращения: 09.10.2023).

7. Sharafaldin I., Habibi Lashkari A., Ghorbani A. A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization // Proceedings of the 4th International Conference on Information Systems Security and Privacy. 2018. P. 108–116.

8. Manimurugan S., Al-Mutairi S., Aborokbah M. M., Chilamkurti N., Ganesan S., Patan R. Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network // IEEE Access. 2020. V. 8. P. 77396–77404.

9. Farhat S., Abdelkader M., Meddeb-Makhlouf A., Zarai F. Evaluation of DoS/DDoS Attack Detection with ML Techniques on CIC-IDS2017 Dataset // Proceedings of the 9th International Conference on Information Systems Security and Privacy. 2023. P. 287–295.

10. Abu Bakar R., Huang X., Javed M. S., Hussain S., Majeed M. F. An Intelligent Agent-Based Detection System for DDoS Attacks Using Automatic Feature Extraction and Selection // Sensors. 2023. V. 23. N. 6. P. 3333.

11. Dora V. R. S., Lakshmi V. N. Optimal feature selection with CNN-feature learning for DDoS attack detection using meta-heuristic-based LSTM // Int. J. Intell. Robot Appl. 2022. V. 6. N. 2. P. 323–349.

12. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges // Cybersecur. 2019. V. 2. N. 1. P. 1–22.

13. Kathiravan P., Shanmugavadivu P., Saranya R. Mitigating Imbalanced Data in Online Social Networks using Stratified K-Means Sampling // 2023 8th International Conference on Business and Industrial Research (ICBIR). 2023. P. 883–888.

The article was submitted 21.03.2024; approved after reviewing 15.05.2024; accepted for publication 08.07.2024
Статья поступила в редакцию 21.03.2024; одобрена после рецензирования 15.05.2024; принята к публикации 08.07.2024

Information about the authors / Информация об авторах

Abdulkader Hajjouz – Postgraduate Student of the Faculty of Software Engineering and Computer Systems; ITMO University; hajjouz@itmo.ru

Elena Yu. Avksentieva – Candidate of Pedagogic Sciences, Assistant Professor; Assistant Professor of the Faculty of Software Engineering and Computer Systems; ITMO University; eavksenteva@itmo.ru

Абдулкадер Хажжуз – аспирант факультета программной инженерии и компьютерной техники; Национальный исследовательский университет ИТМО; hajjouz@itmo.ru

Елена Юрьевна Авксентьева – кандидат педагогических наук, доцент; доцент факультета программной инженерии и компьютерной техники; Национальный исследовательский университет ИТМО; eavksenteva@itmo.ru