UDC 004.93

M.O. CHORNOBUK, V.I. DUBROVIN
National University Zaporizhzhia Polytechnic

AN OVERVIEW OF USING OF FRACTAL ANALYSIS FOR DETECTING DDOS NETWORK ATTACKS

Distributed Denial-of-Service (DDoS) attacks are among the most severe cybersecurity threats, continuously evolving and causing extensive financial losses worldwide. Unlike traditional Denial-of-Service (DoS) attacks, DDoS attacks leverage multiple compromised systems, creating a coordinated effort to overwhelm network resources and disrupt service availability. The growing complexity of these attacks, often indistinguishable from legitimate traffic, presents significant challenges for detection and mitigation. This article examines various machine learning techniques for DDoS detection, including Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Decision Trees, and Naïve Bayes, all of which demonstrate high accuracy in classifying attack patterns on synthetic datasets. While effective in controlled environments, these methods often struggle with the nuances of real-world network traffic, where hybrid and novel attack types obscure detection efforts. To address these challenges, we explore the application of fractal analysis, a promising approach for identifying self-similarity in network traffic.

Fractal analysis, which captures the self-similarity in network traffic, has shown potential for identifying abnormal patterns indicative of DDoS activity. Although it has limitations, fractal analysis can improve the detection process when combined with statistical features and machine learning algorithms.

Fractal characteristics, such as those quantified by the Hurst Exponent, reveal long-term dependencies and autocorrelation structures in traffic, making them suitable for detecting irregularities commonly associated with DDoS attacks. Our analysis demonstrates that fractal-based methods, when combined with statistical and machine learning approaches, can enhance detection accuracy and improve adaptability to real-world scenarios. Although no single method offers a universal solution, this study underscores the importance of using diverse techniques to effectively monitor and protect against DDoS threats. Further research should focus on integrating multifaceted detection models to better address the evolving landscape of cybersecurity threats posed by DDoS attacks.

Key words: *machine learning, DDoS, fractal analysis, classification.*

М.О. ЧОРНОБУК, В.І. ДУБРОВІН
Національний університет «Запорізька політехніка»

ОГЛЯД ВИКОРИСТАННЯ ФРАКТАЛЬНОГО АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ МЕРЕЖЕВИХ DDOS-АТАК

Розподілені атаки на відмову в обслуговуванні (DDoS-атаки) є однією з найсерйозніших загроз кібербезпеці, яка постійно розвивається і завдає значних фінансових збитків у всьому світі. На відміну від традиційних атак типу «відмова в обслуговуванні» (DoS), DDoS-атаки використовують декілька скомпрометованих систем, створюючи скоординовані зусилля для перевантаження мережевих ресурсів і порушення доступності сервісів. Зростаюча складність цих атак, які часто неможливо відрізнити від легітимного трафіку, створює значні труднощі для виявлення та пом'якшення їх наслідків. У цій статті розглядаються різні методи машинного навчання для виявлення DDoS-атак, зокрема машина опорних векторів (SVM), K-найближчих сусідів (KNN), дерева рішень та наївний Байєс, які демонструють високу точність у класифікації шаблонів атак на синтетичних наборах даних. Хоча ці методи ефективні в контрольованих середовищах, вони часто борються з нюансами реального мережевого трафіку, де гібридні та нові типи атак затуманюють зусилля з виявлення. Щоб вирішити ці проблеми, ми досліджуємо застосування фрактального аналізу – перспективного підходу для виявлення самоподібності у мережевому трафіку.

Фрактальний аналіз, який фіксує самоподібність мережевого трафіку, продемонстрував потенціал для виявлення аномальних закономірностей, що свідчать про DDoS-активність. Хоча він має свої обмеження, фрактальний аналіз може покращити процес виявлення у поєднанні зі статистичними ознаками та алгоритмами машинного навчання.

Фрактальні характеристики, наприклад, кількісно вимірювані за допомогою експоненти Херста, виявляють довгострокові залежності та автокореляційні структури у трафіку, що робить їх придатними для виявлення нерегулярностей, які зазвичай асоціюються з DDoS-атаками. Наш аналіз демонструє, що методи на основі фракталів у поєднанні зі статистичними підходами та підходами машинного навчання можуть підвищити точність виявлення та покращити адаптивність до реальних сценаріїв. Хоча жоден метод не пропонує універсального рішення, це дослідження підкреслює важливість використання різноманітних методів для ефективного моніторингу та захисту від DDoS-загроз. Подальші дослідження мають бути зосереджені на інтеграції багатогранних моделей виявлення для кращого реагування на мінливий ландшафт загроз кібербезпеці, які створюють DDoS-атаки.

Ключові слова: *машинне навчання, DDoS, фрактальний аналіз, класифікація.*

https://doi.org/10.32782/mathematical-modelling/2025-8-1-25

Problem Statement

Distributed Denial-of-Service (DDoS) attacks are one of the most dangerous among cybersecurity threats. In a basic Denial-of-Service (DoS) attack, a single source generates a high volume of traffic or repeated requests to overwhelm a network or service, aiming to exhaust its resources and disrupt normal functionality causing denial of service for legitimate customers. While DoS attacks can be damaging to some extent, they are generally limited by the attacker's own resources and are easier to detect and counteract due to their single point of origin. Currently, they are seldom used and pose minimal cybersecurity threats. DDoS attacks, however, are a more advanced and destructive form of DoS. They harness multiple compromised systems, typically organized into a botnet, to conduct a coordinated attack. This distributed approach not only amplifies the scale and impact but also makes these attacks much more challenging to trace and mitigate [1].

Analysis of recent studies and publications

DDoS attacks remain one of the most widespread problems in network security. Despite the fact that such attacks have existed for more than 20 years, and the means to combat them are improving every year, attackers are constantly attracting more and more resources to carry out attacks, and the annual damage from them is estimated in billions of dollars [2]. According to [3] the total number of DDoS attacks in 2023 decreased by more than 50% compared to data from 2022. However, the maximum attack size has increased by an enormous 93.42% up to 700 Gbps. And an average attack size increased by 233% up to 0.8 Gbps. The difficult geopolitical situation and global tensions make cybersecurity even more important. Combined with the constant growth of computing resources and network bandwidth available to the average user, this underscores the importance of protection against DDoS attacks.

There are a huge number of types of DDoS attacks. This diversity makes it much more difficult to counter them, because they are so hard to detect. Numerous DDoS attacks masquerade as legitimate traffic, and unusual types of attacks usually have no distinguishing features. These factors preclude the development of a universal and clear algorithm for detecting such attacks [4]. In such a situation, the task of detecting DDoS attacks is usually reduced to the formal task of classifying traffic based on its features. This task is often addressed using statistical methods or machine learning algorithms.

Presentation of the main research material

The machine learning approach remains one of the most popular approaches for detecting DDoS attacks. Popular classification methods are used for this task: KNN, SVM, Decision Trees, Artificial Neural Networks, Naïve Bayes, etc [5]. Selected papers examining the application of some of these methods will be discussed below.

Paper [6] describes DDoS attack detection using Support Vector Machine, K-Nearest Neighbor, Decision Tree and other common classification methods. Authors used a well-known dataset KDD99 which contains 494021 samples. Using the features extraction method 8 features with the most information gain were selected. Those features include data such as connection protocol, number of data bytes transferred from source to destination, percentage of different services on the current host, etc. According to the study, all methods demonstrated classification accuracy levels above 90% and the Fuzzy C Mean method showed the highest result with 98.7% of accuracy.

Paper [7] contains a similar study which analyzes DDoS detection using Naïve Bayes, Decision Trees, SVM. It also compares two feature selection methods: Principal Component Analysis (PCA) and Learning Vector Quantization (LVQ). The study shows that feature selection methods play an important role in reducing the dimensionality of the data, thus increasing the efficiency of the classification algorithms used. According to the results of the study, the Decision Tree method used in conjunction with LVQ showed the best results. A classification accuracy of 98.74% was achieved.

In [8] it is proposed to use a more complicated machine learning algorithm – Long Short-Term Memory (LSTM), which is a deep learning technique that includes a feature selection and extraction

https://doi.org/10.32782/mathematical-modelling/2025-8-1-25

algorithm. A popular CICDDoS2019 dataset was used, which includes different types of attacks: UDP-Lag, LDAP, NetBIOS, SSDP, SNMP and many others. Each sample contains 88 features which are used as an input for the proposed model. The authors achieved an accuracy rate of 98%. It is shown that LSTM can be a better solution to the problem as it encompasses both feature selection and extraction in its model, which makes it superior to shallow machine learning methods.

Paper [9] proposes a usage of a Random Forest ensemble machine learning algorithm for solving the problem. CICIDS 2017 and CICDDoS 2019 datasets which contain a range of popular DDoS attack types were used. Mutual Information (MI) and Random Forest Feature Importance (RFFI) methods were used for the feature selection process. The proposed model achieved a remarkable classification accuracy of 99.997%.

Despite success on synthetic datasets, detecting malicious traffic during DDoS attacks in real-world environments remains challenging. New types of attacks, combining different types of attacks, varying attack strength over time, all these factors significantly complicate DDoS detection in real time. One solution to such a problem may be to analyze traffic using fractal analysis.

As demonstrated in [10–12], network traffic exhibits a fractal (self-similar) nature. This self-similarity is characterized by strong traffic autocorrelation and long-term dependence, meaning that the correlation structures remain consistent even when observed over extended time scales. Fractal analysis methods help identify structural features that may indicate abnormal changes typical of illegitimate traffic. These abnormalities often include various types of network attacks. The paper demonstrates that a fractal approach can be used to identify different types of DDoS attacks.

The use of statistical features of traffic for detecting DDoS attacks, including fractal analysis using Hurst Exponent, is also discussed in [13]. The Hurst exponent expresses the degree of self-similarity of the time series. It is used in various areas of applied mathematics, including fractals, chaos theory, long-term memory processes, spectral analysis, and network parameter sizing in queueing theory. Authors show that Hurst Exponent had a tendency to change significantly during particular types of attacks. It is concluded, however, that it can't be used for classifying network traffic without other features, because the exponent sometimes took unusually high values during the processing of legitimate traffic.

Paper [14] focuses on fractal analysis to model and understand the self-similarity in network traffic patterns. Through wavelet analysis, the authors examine the Hurst exponent to quantify these patterns across multiple scales. This fractal modeling, particularly through multifractal wavelet models, reveals that network traffic exhibits both large-scale self-similarity and small-scale multifractal characteristics. Authors use publicly available datasets with network data to prove that proposed approach may be used for detecting DDoS attacks. Proposed fractal-based model demonstrates high accuracy in monitoring and predicting network performance anomalies. The authors concede, however, that their model will require additional customization for other types of network attacks and is not universally efficient.

DDoS detection remains a complex problem, requiring a combination of different methods for detection of exotic types of attacks. Popular machine learning classification methods, such as SVM, Decision Trees, and Naïve Bayes, have proven effective in identifying attack patterns with high accuracy on synthetic datasets. However, the problem of accurate detection of all types of DDoS attacks in a real environment is yet to be solved. Techniques such as fractal analysis offer promising results by identifying the self-similar patterns in network traffic that often signify DDoS attacks. Although statistical methods can extract network traffic features, [13] indicates that no single statistical characteristic can accurately identify all types of attacks. Further development of these methods and improved accuracy in DDoS attack detection may depend on using diverse traffic characteristics as inputs to machine learning models.

https://doi.org/10.32782/mathematical-modelling/2025-8-1-25

An example of traffic analysis using Hurst Exponent

In order to illustrate the usage of fractal analysis for the traffic feature extraction a part of a well-known dataset IDS 2018 Intrusion was used [15]. The Hurst Exponent of the forward packets per second rate was calculated for an interval of 12 hours of data which included a popular type of an HTTP flood DDoS attack. Table 1 shows resulting values for malicious samples, legitimate samples and resulting mixed traffic.

Table 1

Hurst Exponent values for different parts of traffic

Traffic type	Hurst Exponent
Legitimate	0.9570044
Malicious	0.5808738
Mixed	0.9570041

The data shows that the Hurst Exponent for malicious samples differs significantly from that of normal traffic. Nevertheless, given the sluggish nature of the attack, which lasted for 12 hours, the value of the Hurst Exponent for the resulting traffic does not change much. This suggests that the Hurst Exponent can help detect network attacks, though raw statistical data may require additional processing to be useful. Fig.1 shows an illustrative graph of the value of forward packets per second rate for the used dataset.

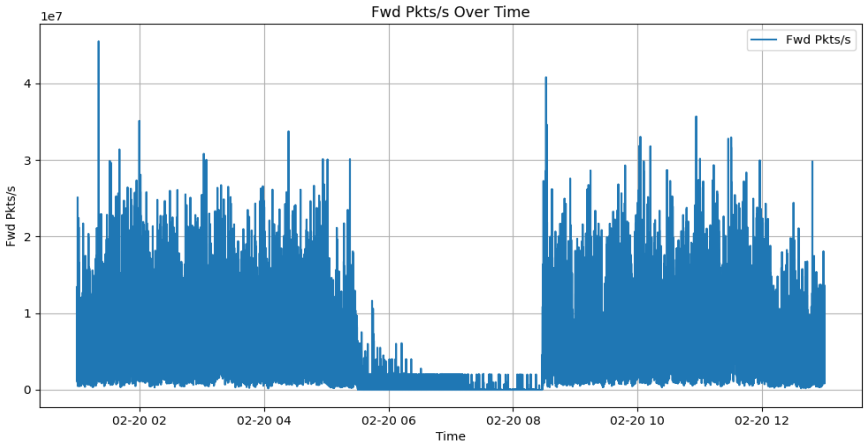

Fig. 1. Forward packets per second rate

Conclusions

In conclusion, while Distributed Denial-of-Service (DDoS) attacks continue to pose a significant threat to network security, they often can be detected by using machine learning algorithms. Techniques such as SVM, Decision Trees, and Naïve Bayes have demonstrated high accuracy in detecting attack patterns on synthetic datasets. However, real-world application remains challenging due to the evolving and often unpredictable nature of DDoS attacks. Fractal analysis, which captures the self-similarity in network traffic, has shown potential for identifying abnormal patterns indicative of DDoS activity. Although it has limitations, fractal analysis can improve the detection process when combined with statistical features and machine learning algorithms.

Bibliography

1. Merkebaiuly M. Overview of Distributed Denial of Service (DDoS) attack types and mitigation methods. *InterConf*. 2024. № 43(193). С. 494–508. https://doi.org/10.51582/interconf.19-20.03.2024.048 (дата звернення: 17.01.2025).

https://doi.org/10.32782/mathematical-modelling/2025-8-1-25

2. Singh A., Gupta B. B. Distributed denial-of-service (ddos) attacks and defense mechanisms in various web-enabled computing platforms. *International journal on semantic web and information systems*. 2022. Т. 18, № 1. С. 1–43. https://doi.org/10.4018/ijswis.297143 (дата звернення: 17.01.2025).
3. DDoS trend report 2024. Official sate. Nexusguard - Simplifying DDoS for Communications Service Providers. URL: https://www.nexusguard.com/threat-report/ddos-trend-report-2024 (дата звернення: 17.01.2025).
4. Majeed alhammadi N. A., Zaboon K. H., Abdullah A. A. A review of the common ddos attack: types and protection approaches based on artificial intelligence. *Fusion: practice and applications*. 2021. Т. 7(1). С. 08–14. https://doi.org/10.54216/fpa.070101 (дата звернення: 17.01.2025).
5. Alqahtani Haya Malooh, Abdullah Monir. A review on ddos attacks classifying and detection by ML/DL models. *International journal of advanced computer science and applications*. 2024. Т. 15, № 2. С. 824–833. https://doi.org/10.14569/ijacsa.2024.0150283 (дата звернення: 17.01.2025).
6. Yusof A., Udzir N., Selamat A. An evaluation on KNN-SVM algorithm for detection and prediction of ddos attack. *Trends in applied knowledge-based systems and data science*. 2016. (Springer Nature Link, 14 липня 2016 р.), С. 95–102. https://doi.org/10.1007/978-3-319-42007-3_9 (дата звернення: 17.01.2025).
7. Bagyalakshmi C., Samundeeswari E.S. DDoS attack classification on cloud environment using machine learning techniques with different feature selection methods. *International journal of advanced trends in computer science and engineering*. 2020. Т. 9, № 5. С. 7301–7308. https://doi.org/10.30534/ijatcse/2020/60952020 (дата звернення: 17.01.2025).
8. Kumar D., Pateriya R. K., Gupta R. K., Dehalwar V., Sharma A. DDoS detection using deep learning. *Procedia computer science*. 2023. Т. 218. С. 2420–2429. https://doi.org/10.1016/j.procs.2023.01.217.
9. Alduailij M., Khan Q. W., Tahir M., Sardaraz M., Alduailij M., Malik F. Machine-Learning-Based ddos attack detection using mutual information and random forest feature importance method. *Symmetry*. 2022. Т. 14, № 6. С. 1095. https://doi.org/10.3390/sym14061095.
10. Kirichenko L., Radivilova T., Yeremenko O. Fractal features of DDoS attacks series. *WomENcourage:* conference Rome. 17–19 September,2019. Rome. 2019. URL: https://www.researchgate.net/publication/337335195_Fractal_features_of_DDoS_attacks_series (дата звернення: 17.01.2025).
11. Yan R., Xu G., Qin X. Detect and identify DDoS attacks from flash crowd based on self-similarity and Renyi entropy. *Chinese automation congress* (CAC-2017), Jinan, 20–22 жовт. 2017 p. Jinan, 2017. P. 7188–7194. https://doi.org/10.1109/cac.2017.8244075 (дата звернення: 17.01.2025).
12. Xia H., Xu W. *Research on method of network abnormal detection based on hurst parameter estimation*. In International conference on computer science and software engineering, Wuhan, China, 12–14 груд. 2008 p. Wuhan, China, 2008. P. 559–562. https://doi.org/10.1109/csse.2008.1069 (дата звернення: 17.01.2025).
13. Smiesko J., Segec P., Kontsek M. Machine recognition of ddos attacks using statistical parameters. *Mathematics*. 2023. Т. 12, № 1. С. 142. https://doi.org/10.3390/math12010142 (дата звернення: 17.01.2025).
14. Ding C., Chen Y., Liu Z., Alshehri A.M., Liu T. Fractal characteristics of network traffic and its correlation with network security *Fractals*. 2022. Т. 30, № 02. https://doi.org/10.1142/s0218348x22400679 (дата звернення: 17.01.2025).
15. IDS 2018 Intrusion CSVs (CSE-CIC-IDS2018). Official sate. *www.kaggle.com*. URL: https://www.kaggle.com/datasets/solarmainframe/ids-intrusion-csv (дата звернення: 17.01.2025).

https://doi.org/10.32782/mathematical-modelling/2025-8-1-25

References

1. Merkebaiuly, M. (2024). Overview of Distributed Denial of Service (DDoS) attack types and mitigation methods. *InterConf*, 43(193), 494–508. https://doi.org/10.51582/interconf.19-20.03.2024.048 [in English].
2. Singh, A., & Gupta, B. B. (2022). Distributed denial-of-service (ddos) attacks and defense mechanisms in various web-enabled computing platforms. *International Journal on Semantic Web and Information Systems*, 18(1), 1–43. https://doi.org/10.4018/ijswis.297143 [in English].
3. *DDoS trend report 2024*. (2024). Official sate. Nexusguard - Simplifying DDoS for Communications Service Providers. Retrieved from: https://www.nexusguard.com/threat-report/ddos-trend-report-2024 [in English].
4. Majeed alhammadi, N. A., Zaboon, K. H., & Abdullah, A. A. (2021). A review of the common ddos attack: Types and protection approaches based on artificial intelligence. *Fusion: Practice and Applications*, 7(1), 08–14. https://doi.org/10.54216/fpa.070101 [in English].
5. Alqahtani, H. M., & Abdullah, M. (2024). A review on ddos attacks classifying and detection by ML/DL models. *International Journal of Advanced Computer Science and Applications*, 15(2), 824–833. https://doi.org/10.14569/ijacsa.2024.0150283 [in English].
6. Yusof, A., Udzir, N., & Selamat, A. (2016). An evaluation on KNN-SVM algorithm for detection and prediction of ddos attack. *In Trends in applied knowledge-based systems and data science* (Springer Nature Link, 14 липня 2016 р.), 95–102. https://doi.org/10.1007/978-3-319-42007-3_9 [in English].
7. Bagyalakshmi, C., & Samundeeswari, E.S.. DDoS attack classification on cloud environment using machine learning techniques with different feature selection methods. (2020). *International Journal of Advanced Trends in Computer Science and Engineering*, 9(5), 7301–7308. https://doi.org/10.30534/ijatcse/2020/60952020 [in English].
8. Kumar, D., Pateriya, R. K., Gupta, R. K., Dehalwar, V., & Sharma, A. (2023). DDoS detection using deep learning. *Procedia Computer Science*, 218, 2420–2429. https://doi.org/10.1016/j.procs.2023.01.217 [in English].
9. Alduailij, M., Khan, Q. W., Tahir, M., Sardaraz, M., Alduailij, M., & Malik, F. (2022). Machine-Learning-Based ddos attack detection using mutual information and random forest feature importance method. *Symmetry*, 14(6), 1095. https://doi.org/10.3390/sym14061095 [in English].
10. Kirichenko, L., Radivilova, T., & Yeremenkj, O. (2019). Fractal features of DDoS attacks series. Proceedings conference *WomENcourage*, Rome. Retrieved from: https://www.researchgate.net/publication/337335195_Fractal_features_of_DDoS_attacks_series (дата звернення: 17.01.2025) [in English].
11. Yan, R., Xu, G., & Qin, X. (2017). Detect and identify DDoS attacks from flash crowd based on self-similarity and Renyi entropy. In *Chinese automation congress* (CAC-2017). Jinan. https://doi.org/10.1109/cac.2017.8244075 [in English].
12. Xia, H., & Xu, W. (2008). Research on method of network abnormal detection based on hurst parameter estimation. In *2008 international conference on computer science and software engineering*. Wuhan, China. https://doi.org/10.1109/csse.2008.1069 [in English].
13. Smiesko, J., Segec, P., & Kontsek, M. (2023). Machine recognition of ddos attacks using statistical parameters. *Mathematics*, 12(1), 142. https://doi.org/10.3390/math12010142 [in English].
14. Ding, C., Chen, Y., Liu, Z., Alshehri, A. M., & Liu, T. (2022). Fractal characteristics of network traffic and its correlation with network security. *Fractals*, 30(02). https://doi.org/10.1142/s0218348x22400679 [in English].
15. *IDS 2018 Intrusion CSVs (CSE-CIC-IDS2018)*. (2018). [Official sate]. www.kaggle.com. Retrived from: https://www.kaggle.com/datasets/solarmainframe/ids-intrusion-csv [in English].

https://doi.org/10.32782/mathematical-modelling/2025-8-1-25

Chornobuk Maksym Olehovych – student at the Software Engineering Department of the National University Zaporizhzhia Polytechnic. E-mail: chornobuk.maksym@zp.edu.ua, ORCID: 0000-0003-3200-7306.

Dubrovin Valery Ivanovych – Candidate of Technical Sciences, Professor at the Department of Software of the National University Zaporizhzhia Polytechnic. E-mail: vdubrovin@gmail.com, ORCID: 0000-0002-0848-8202.

Чорнобук Максим Олегович – студент кафедри програмних засобів Національного університету «Запорізька політехніка». E-mail: chornobuk.maksym@zp.edu.ua, ORCID: 0000-0003-3200-7306.

Дубровін Валерій Іванович – к.т.н., професор кафедри програмних засобів Національного університету «Запорізька політехніка». E-mail: vdubrovin@gmail.com, ORCID: 0000-0002-0848-8202.

https://doi.org/10.32782/mathematical-modelling/2025-8-1-25