International Journal of Wireless and Ad Hoc Communication

♦ ISSN: 2692-4048 Vol: 08, No .02, 2024 ♦ PP. 25–28

Article DOI: https://doi.org/10.54216/IJWAC.080205

FULL LENGTH ARTICLE

Enhancing Wireless Ad-Hoc Network Security by Mitigating Distributed Denial-of-Service (DDoS) Attacks

Mahmoud M. Ismail[1,*] **Ahmed A. Metwaly**[2]

[1,2] Information Systems Department, Faculty of Computers and Informatics, Zagazig University, Zagazig, Sharqiyah, 44519, Egypt

Emails: mmsabe@zu.edu.eg · a.metwaly23@fci.zu.edu.eg

Received: September 07, 2023 Revised: December 26, 2023 Accepted: April 05, 2024 ⋆ Corresponding author

ABSTRACT

The increasing threat landscape of Distributed Denial-of-Service (DDoS) attacks makes network security a major concern. These attacks are a serious challenge to the stability and integrity of digital infrastructures. This research paper is an in-depth study on how to enhance network security through the detection and mitigation of DDoS attacks. The study reviews existing literature on DDoS attack mitigation strategies, emphasizing the evolving nature of these threats and the imperative for robust defense mechanisms. The research uses statistical analysis and logistic regression to provide a detailed methodology for distinguishing DDoS attacks from normal network activities. The results show that logistic regression is an effective classification model, providing insights into improved detection measures. Finally, the study concludes by recommending a multi-faceted approach that combines theoretical insights with empirical validation, highlighting the need for stronger network security measures against DDoS attacks and enhancing digital resilience.

Keywords: Ransomware ▪ Threats ▪ Industrial Internet of Things ▪ Detection ▪ Cybersecurity ▪ Security Measures ▪ Intrusion Detection ▪ IoT Networks ▪ Cyber Threats

1. INTRODUCTION

Network security is a crucial aspect of digital infrastructure as it protects against various cyber threats that compromise the integrity, confidentiality, and availability of data and services. One of the most persistent and disruptive threats to network stability is Distributed Denial-of-Service (DDoS) attacks [1]. These attacks are orchestrated by malicious actors who aim to disrupt the normal functioning of networks by flooding targeted systems with an overwhelming amount of traffic, making them inaccessible to legitimate users [2]. The increasing frequency, sophistication, and devastating consequences of DDoS attacks highlight the urgent need for strong defense mechanisms that can protect network infrastructures from such malicious intrusions [3, 4, 5].

The proliferation of interconnected devices coupled with the evolution of cyber threats has increased the vulnerability of networks to DDoS attacks. As the digital landscape expands to include cloud-based services, Internet of Things (IoT) devices, and critical infrastructures, these attacks have a much greater potential impact [6, 7]. Understanding how DDoS attacks work, from their modus operandi to the possible vulnerabilities they exploit, is fundamental in developing effective defense strategies. Hence, this paper aims to delve into the multifaceted nature of DDoS attacks, exploring both their technical underpinnings and the diverse methodologies available to detect, mitigate, and prevent these assaults [8].

The research is significant because it seeks to explain how network security can be strengthened by comprehensively countering DDoS attacks. This study examines the landscape of existing defense mechanisms and evaluates their effectiveness in stopping various forms of DDoS attacks to

provide insights that are crucial for enhancing the resilience of network infrastructures [9]. The paper aims to provide a comprehensive framework for detection and mitigation strategies that will enable network administrators and cybersecurity professionals to proactively protect against the disruptive effects of DDoS attacks, thus strengthening the stability and reliability of network operations [10].

In summary, this paper explores DDoS attacks by recognizing their threat landscape, dissecting their methodologies, and evaluating the efficacy of existing defense strategies. By merging theoretical insights with practical applications, it hopes to pave the way for improved network security paradigms that will provide a strong shield against the destructive impact of DDoS assaults.

2. RELATED WORKS

The evolving landscape of Distributed Denial-of-Service (DDoS) attacks has been extensively explored in recent literature, each study offering distinct insights and methodologies. Guleria et al. [11] investigated the nuanced challenges of DDoS attacks within Vehicular Ad Hoc Networks (VANETs). Their study focused on refining detection and mitigation techniques specific to the unique characteristics of VANETs, contributing valuable insights into securing vehicular communication systems against DDoS threats.

Alosaimi et al. [12] conducted a simulation-based study, meticulously exploring prevention strategies against DDoS attacks in cloud environments. Their research not only identified vulnerabilities but also proposed and evaluated effective preventive measures crucial in fortifying cloud-based services against potential disruptions caused by DDoS assaults.

Kumar [13] contributed a comprehensive update on the evolving nature of Denial-of-Service attacks, delving into the changing tactics and impacts of such attacks in contemporary network environments. This analysis offered an enriched understanding of the evolving DDoS landscape, identifying key factors influencing the efficacy of mitigation strategies. Robinson et al. [14] critically evaluated a spectrum of mitigation methods designed to combat DDoS attacks.

Mölsä [15] made a significant contribution by providing a comprehensive tutorial that explained how to mitigate Denial of Service attacks. Fung et al. [16] introduced VGuard, an innovative mitigation technique that uses Network Function Virtualization to combat DDoS attacks. Mallikarjunan et al. [17] conducted an extensive survey that comprehensively mapped out the landscape of DDoS attacks. Chahal et al. [18] wrote an exhaustive review on the intricacies of DDoS attacks and their implications for modern network security.

3. METHODOLOGY

This section explains how the research was done and how the data was analyzed to determine the effectiveness of different defense mechanisms against DDoS attacks. Logistic regression is a basic classification algorithm used in machine learning. The theory behind logistic regression is about modeling the probability of binary outcomes by using a logistic function that transforms the output into a range between 0 and 1. This algorithm is especially good at solving classification problems by fitting a linear decision boundary to separate different classes within a dataset, thereby classifying new instances based on learned patterns. In this study, logistic regression is used as the main classification model for distinguishing and classifying Distributed Denial-of-Service attacks from normal network traffic [19].

Several sequential steps are involved in the application of logistic regression. First, data preprocessing includes cleaning, transforming, and preparing the dataset for analysis. Feature selection and engineering identify relevant attributes that capture network behavior during attack and non-attack scenarios. The dataset is then split into training and testing subsets to evaluate generalization. The logistic regression model learns coefficients that map traffic features to attack labels, and its predictions are evaluated using accuracy, precision, recall, and confusion-matrix analysis.

The logistic regression model is expressed as:

$$P(Y = 1 \mid X) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n)}}. \quad (1)$$

Here, $P(Y = 1 \mid X)$ is the probability that a network instance belongs to the DDoS class, $X_1, \ldots, X_n$ are input traffic features, and $\beta_0, \ldots, \beta_n$ are model parameters learned from the training data.

4. RESULTS ANALYSIS AND DISCUSSION

Table 1 presents a statistical summary of representative dataset attributes used to assess the performance and effectiveness of the deployed defense mechanisms against DDoS attacks. The overview covers important traffic parameters such as packet length, active time, idle time, and labels. These statistics provide a quantitative understanding of the nature and impact of DDoS assaults within the experimental framework.

Figure 1 provides a visual representation of the class distribution within the dataset, delineating the prevalence and distribution of categories pertinent to the nature and characteristics of DDoS attacks. This graphical depiction offers an insightful portrayal of the relative frequency of different classes and highlights potential imbalance across attack and benign traffic categories.

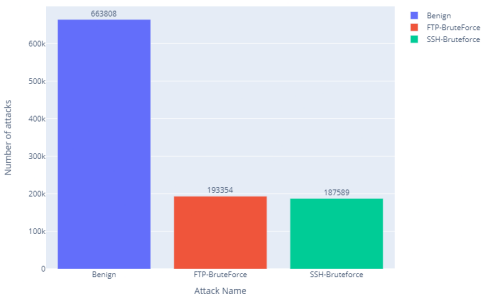

Figure 1. Class distribution of Distributed Denial-of-Service (DDoS) attack types within the dataset.

Figure 2 encapsulates the interplay between predicted and actual classifications through the presentation of a confusion matrix. The matrix offers a detailed breakdown of the performance of the employed classification model in discerning and categorizing DDoS attacks. By portraying true positives, true

Table 1. Statistical analysis of representative DDoS dataset features

Feature	Count	Mean	Std	Min	25%	50%	75%	Max
Fwd Pkt Len Max	1.04E+06	1.75E+02	2.88E+02	0.00E+00	0.00E+00	3.50E+01	2.01E+02	6.44E+04
Fwd Pkt Len Min	1.04E+06	8.42E+00	1.95E+01	0.00E+00	0.00E+00	0.00E+00	0.00E+00	1.46E+03
Fwd Seg Size Min	1.04E+06	2.33E+01	1.11E+01	0.00E+00	2.00E+01	2.00E+01	3.20E+01	4.80E+01
Active Mean	1.04E+06	5.17E+04	5.83E+05	0.00E+00	0.00E+00	0.00E+00	0.00E+00	1.10E+08
Active Std	1.04E+06	2.14E+04	2.19E+05	0.00E+00	0.00E+00	0.00E+00	0.00E+00	5.72E+07
Active Max	1.04E+06	8.82E+04	7.41E+05	0.00E+00	0.00E+00	0.00E+00	0.00E+00	1.10E+08
Active Min	1.04E+06	4.01E+04	5.61E+05	0.00E+00	0.00E+00	0.00E+00	0.00E+00	1.10E+08
Idle Mean	1.04E+06	3.11E+06	5.42E+08	0.00E+00	0.00E+00	0.00E+00	0.00E+00	3.39E+11
Idle Std	1.04E+06	7.32E+05	3.83E+08	0.00E+00	0.00E+00	0.00E+00	0.00E+00	2.43E+11
Idle Max	1.04E+06	4.83E+06	1.52E+09	0.00E+00	0.00E+00	0.00E+00	0.00E+00	9.80E+11
Idle Min	1.04E+06	2.13E+06	1.82E+07	0.00E+00	0.00E+00	0.00E+00	0.00E+00	1.26E+10
Label	1.04E+06	6.35E-01	4.81E-01	0.00E+00	0.00E+00	1.00E+00	1.00E+00	1.00E+00

negatives, false positives, and false negatives, the confusion matrix serves as a critical evaluation tool for assessing model accuracy, precision, recall, and overall efficacy.

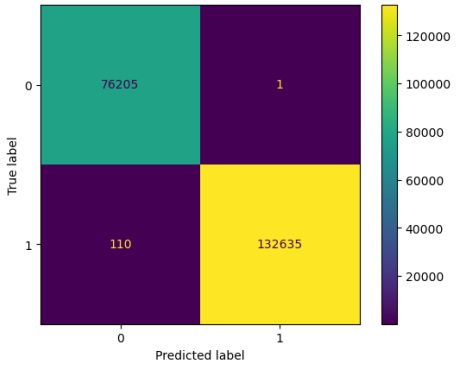

Figure 2. Confusion matrix depicting classification performance of DDoS attack types.

Figure 3 portrays a decision plan or tree structure that encapsulates the hierarchical and sequential decision-making process employed within the classification framework for identifying and categorizing DDoS attacks. This visual representation elucidates the logical flow of the decision process, showcasing the series of conditions or features used to partition the dataset into distinct attack categories.

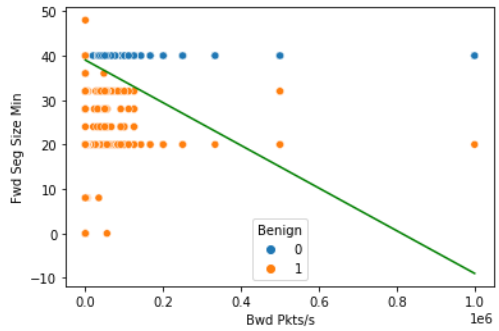

Figure 3. Hierarchical representation of the classification framework for DDoS attack identification.

5. CONCLUSION

This study underscores the critical importance of robust defense mechanisms in combating the persistent threat of Distributed Denial-of-Service (DDoS) attacks within network infrastructures. Through a comprehensive exploration of detection and mitigation strategies, including an in-depth analysis of various literature studies, statistical analysis of attack characteristics, and the application of logistic regression for classification, this research contributes to the arsenal of cybersecurity measures aimed at fortifying network resilience. The findings underscore the efficacy of logistic regression as a classification model in discerning DDoS attacks from normal network traffic, offering insights into enhancing detection and response mechanisms.

REFERENCES

[1] A. Aljuhani, "Machine learning approaches for combating distributed denial of service attacks in modern networking environments," *IEEE Access*, vol. 9, pp. 42 236–42 264, 2021.

[2] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," *International Journal of Distributed Sensor Networks*, vol. 13, no. 12, p. 1550147717741463, 2017.

[3] A. Mishra, B. B. Gupta, and R. C. Joshi, "A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques," in *2011 European Intelligence and Security Informatics Conference*, 2011, pp. 286–289.

[4] V. Borgiani, P. Moratori, J. F. Kazienko, E. R. R. Tubino, and S. E. Quincozes, "Toward a distributed approach for detection and mitigation of denial-of-service attacks within industrial internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4569–4578, 2020.

[5] S. Wani, M. Imthiyas, H. Almohamedh, K. M. Alhamed, S. Almotairi, and Y. Gulzar, "Distributed denial of service (ddos) mitigation using blockchain—a comprehensive insight," *Symmetry*, vol. 13, no. 2, p. 227, 2021.

[6] K. Bhushan and B. B. Gupta, "Distributed denial of service (ddos) attack mitigation in software defined network (sdn)-based cloud computing environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 1985–1997, 2019.

[7] X. Geng and A. B. Whinston, "Defeating distributed denial of service attacks," *IT Professional*, vol. 2, no. 4, pp. 36–42, 2000.

[8] B. B. Gupta, R. C. Joshi, and M. Misra, "Defending against distributed denial of service attacks: Issues and challenges," *Information Security Journal: A Global Perspective*, vol. 18, no. 5, pp. 224–247, 2009.

[9] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic, "Distributed denial of service attacks," in *SMC 2000 Conference Proceedings. 2000 IEEE International Conference on Systems, Man and Cybernetics*, vol. 3, 2000, pp. 2275–2280.

[10] R. R. Zebari, S. R. M. Zeebaree, A. B. Sallow, H. M. Shukur, O. M. Ahmad, and K. Jacksi, "Distributed denial of service attack mitigation using high availability proxy and network load balancing," in *2020 International Conference on Advanced Science and Engineering (ICOASE)*, 2020, pp. 174–179.

[11] C. Guleria and H. K. Verma, "Improved detection and mitigation of ddos attack in vehicular ad hoc network," in *2018 4th International Conference on Computing Communication and Automation (ICCCA)*, 2018, pp. 1–4.

[12] W. Alosaimi, M. Alshamrani, and K. Al-Begain, "Simulation-based study of distributed denial of service attacks prevention in the cloud," in *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, 2015, pp. 60–65.

[13] G. Kumar, "Denial of service attacks—an updated perspective," *Systems Science & Control Engineering*, vol. 4, no. 1, pp. 285–294, 2016.

[14] R. R. R. Robinson and C. Thomas, "Evaluation of mitigation methods for distributed denial of service attacks," in *2012 7th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, 2012, pp. 713–718.

[15] J. Mölsä, "Mitigating denial of service attacks: A tutorial," *Journal of Computer Security*, vol. 13, no. 6, pp. 807–837, 2005.

[16] C. J. Fung and B. McCormick, "Vguard: A distributed denial of service attack mitigation method using network function virtualization," in *2015 11th International Conference on Network and Service Management (CNSM)*, 2015, pp. 64–70.

[17] K. N. Mallikarjunan, K. Muthupriya, and S. M. Shalinie, "A survey of distributed denial of service attack," in *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, 2016, pp. 1–6.

[18] J. Kaur Chahal, A. Bhandari, and S. Behal, "Distributed denial of service attacks: A threat or challenge," *New Review of Information Networking*, vol. 24, no. 1, pp. 31–103, 2019.

[19] A. A. Metwaly and I. Elhenawy, "Sustainable intrusion detection in vehicular controller area networks using machine intelligence paradigm," *Sustainable Machine Intelligence Journal*, vol. 4, 2023.