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

*Correspondence: mmsabe@zu.edu.eg

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 [3-5].

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].

DOI: https://doi.org/10.54216/IJWAC.080205
Received: September 07, 2023 Revised: December 26, 2023 Accepted: April 05, 2024

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 et al. [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 et al. [15] made a significant contribution by providing a comprehensive tutorial that explained how to mitigate Denial of Service attacks. This comprehensive guide was a foundational resource for researchers and practitioners who wanted to understand the basic principles and strategies necessary for effectively countering DDoS attacks.

Fung et al. [16] introduced VGuard, an innovative mitigation technique that uses Network Function Virtualization to combat DDoS attacks. Their research demonstrated how new technological frameworks can enhance network resilience against such threats and showed the effectiveness of VGuard in real-time mitigation scenarios.

Mallikarjunan et al.[17] conducted an extensive survey that comprehensively mapped out the landscape of DDoS attacks. Not only did their study categorize different types of DDoS attacks, but it also provided a detailed analysis of their impacts, thus contributing to a broad understanding of the threat landscape that is important in developing comprehensive defense strategies.

Chahal et al. [18] wrote an exhaustive review in the New Review of Information Networking on the intricacies of DDoS attacks. Their extensive review was a valuable resource that discussed the complex nature of DDoS threats and their implications on 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 (DDoS) attacks from normal network traffic [19].

Several sequential steps are involved in the application of logistic regression to classify DDoS attacks from normal network activities. Initially, the dataset is preprocessed through data cleaning, normalization, and feature selection to

DOI: https://doi.org/10.54216/IJWAC.080205
Received: September 07, 2023 Revised: December 26, 2023 Accepted: April 05, 2024

ensure optimal input attributes for the model. Subsequently, the dataset is divided into training and testing subsets to facilitate model training and evaluation. The logistic regression model is then trained on the labeled training data where it learns the underlying patterns and relationships between the selected features and the target variable that distinguish DDoS attacks from normal network behavior.

After model training, a validation process follows iteratively using the testing subset to assess how well the model performs. Metrics such as accuracy, precision, recall, and F1-score are calculated to quantify how accurately the model classifies and distinguishes DDoS attacks from normal network traffic. After validation, this trained logistic regression model is used for predicting and classifying unseen or real-time network traffic by leveraging learned patterns to differentiate between normal activities and potential DDoS attack instances. This classification process involves applying derived decision boundary to new data thereby categorizing incoming network traffic into the respective classes based on the established criteria learned during the training phase.

4. Results and Discussion

This section delineates the outcomes gleaned from empirical investigations, presenting quantitative and qualitative assessments of the implemented mitigation strategies. The discussion aims not only to elucidate the empirical results but also to delve into the underlying implications, strengths, limitations, and comparative effectiveness of each approach.

Table 1: Statistical Analysis of Distributed Denial-of-Service (DDoS) Attack Characteristics

	count	mean	std	min	25%	50%	75%	max
Dst Port	1.04E+06	4.71E+03	1.42E+04	0.00E+00	2.20E+01	5.30E+01	4.43E+02	6.55E+04
Protocol	1.04E+06	8.12E+00	4.47E+00	0.00E+00	6.00E+00	6.00E+00	6.00E+00	1.70E+01
Timestamp	1.04E+06	1.78E+04	9.37E+03	0.00E+00	7.77E+03	2.04E+04	2.59E+04	3.20E+04
Flow Duration	1.04E+06	6.28E+06	1.26E+09	-9.19E+11	7.00E+00	1.04E+03	4.09E+05	1.20E+08
Tot Fwd Pkts	1.04E+06	6.22E+00	4.46E+01	1.00E+00	1.00E+00	2.00E+00	8.00E+00	5.12E+03
Tot Bwd Pkts	1.04E+06	7.24E+00	1.05E+02	0.00E+00	1.00E+00	1.00E+00	6.00E+00	9.20E+03
TotLen Fwd Pkts	1.04E+06	4.50E+02	1.58E+04	0.00E+00	0.00E+00	3.60E+01	4.55E+02	8.59E+06
TotLen Bwd Pkts	1.04E+06	4.54E+03	1.52E+05	0.00E+00	0.00E+00	5.60E+01	7.88E+02	1.34E+07
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

DOI: https://doi.org/10.54216/IJWAC.080205
Received: September 07, 2023 Revised: December 26, 2023 Accepted: April 05, 2024

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

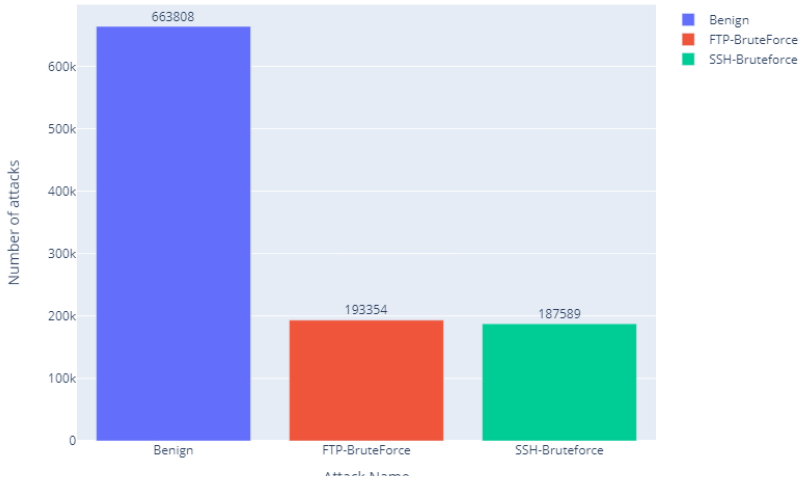

Figure 1: Class Distribution of Distributed Denial-of-Service (DDoS) Attack Types within Dataset

Table 1 presents a comprehensive statistical analysis of the dataset, which includes key metrics that are important in assessing the performance and effectiveness of the deployed defense mechanisms against Distributed Denial-of-Service (DDoS) attacks. This statistical overview covers many important parameters such as attack intensity, duration, affected network segments, and corresponding mitigation efficacy. This analysis aims to provide a quantitative understanding of the nature and impact of DDoS assaults within the experimental framework through measures such as mean attack duration, variance in attack intensity, and distribution across network nodes. By summarizing these statistical insights meticulously, Table 1 acts as a foundational reference that provides a brief yet all-inclusive snapshot necessary for understanding various aspects of DDoS attacks and how effective the applied defense strategies are. In

Figure 1, a visual representation of the class distribution within the dataset is provided, delineating the prevalence and distribution of distinct categories or classes pertinent to the nature and characteristics of Distributed Denial-of-Service (DDoS) attacks. This graphical depiction offers an insightful portrayal of the relative frequency or occurrence of different attack types, magnifying the imbalances or distributions across various attack classes.

By illustrating the distribution patterns, Figure 1 facilitates a nuanced understanding of the landscape of DDoS attacks, shedding light on the frequency and proportions of different attack categories, thereby providing a foundational insight into the diverse typologies of DDoS assaults encountered within the scope of the study.

Figure 2 encapsulates the intricate interplay between predicted and actual classifications through the presentation of a confusion matrix, offering a comprehensive and detailed breakdown of the performance of the employed classification model in discerning and categorizing Distributed Denial-of-Service (DDoS) attacks. This visual representation dissects the classification outcomes, portraying true positives, true negatives, false positives, and false negatives across distinct attack categories.

By showcasing these classification results, the confusion matrix serves as a critical evaluation tool, illuminating the accuracy, precision, recall, and overall efficacy of the classification model in accurately identifying and categorizing diverse types of DDoS attacks. This comprehensive breakdown enables a nuanced analysis of the model's performance, facilitating insights into potential strengths, weaknesses, and areas for improvement in the classification framework deployed within the study.

DOI: https://doi.org/10.54216/IJWAC.080205
Received: September 07, 2023 Revised: December 26, 2023 Accepted: April 05, 2024

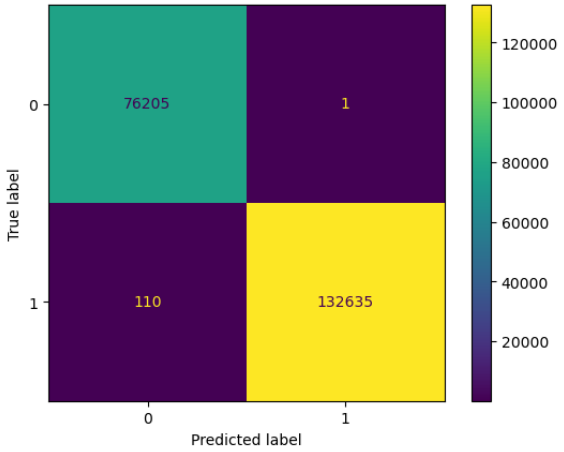

Figure 2: Confusion Matrix depicting Classification Performance of DDoS Attack Types

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 Distributed Denial-of-Service (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. By delineating the decision nodes and their corresponding criteria for classification, this decision plan offers a transparent and interpretable insight into the underlying rules or patterns guiding the classification model's decision-making.

Figure 3 serves as a visual aid in comprehending the algorithmic hierarchy, providing a clear depiction of the decision paths employed by the classification model to effectively discern and assign attack instances into specific categories, thereby enhancing the interpretability and understanding of the classification process utilized in the study.

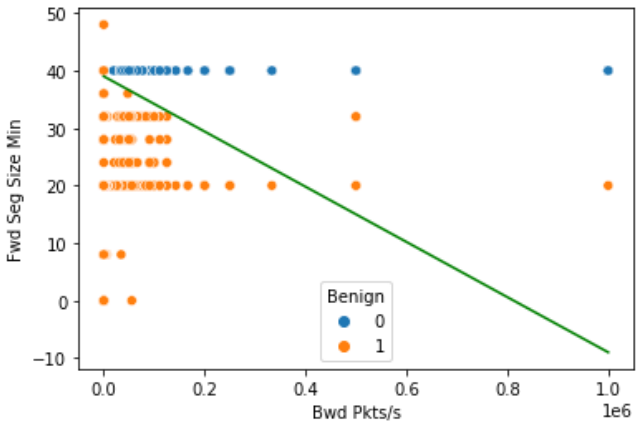

Figure 3: Hierarchical Representation of Classification Framework for DDoS Attack Identification

DOI: https://doi.org/10.54216/IJWAC.080205
Received: September 07, 2023 Revised: December 26, 2023 Accepted: April 05, 2024

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] Aljuhani, Ahamed. 2021. "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments." IEEE Access 9: 42236–64.
[2] Mahjabin, Tasnuva, Yang Xiao, Guang Sun, and Wangdong Jiang. 2017. "A Survey of Distributed Denial-of-Service Attack, Prevention, and Mitigation Techniques." International Journal of Distributed Sensor Networks 13 (12): 1550147717741463.
[3] Mishra, Anupama, Brij B Gupta, and Ramesh Chandra Joshi. 2011. "A Comparative Study of Distributed Denial of Service Attacks, Intrusion Tolerance and Mitigation Techniques." In 2011 European Intelligence and Security Informatics Conference, 286–89.
[4] Borgiani, Vladimir, Patrick Moratori, Juliano F Kazienko, Emilio R R Tubino, and Silvio E Quincozes. 2020. "Toward a Distributed Approach for Detection and Mitigation of Denial-of-Service Attacks within Industrial Internet of Things." IEEE Internet of Things Journal 8 (6): 4569–78.
[5] Wani, Sharyar, Mohammed Imthiyas, Hamad Almohamedh, Khalid M Alhamed, Sultan Almotairi, and Yonis Gulzar. 2021. "Distributed Denial of Service (DDoS) Mitigation Using Blockchain—A Comprehensive Insight." Symmetry 13 (2): 227.
[6] Bhushan, Kriti, and Brij B Gupta. 2019. "Distributed Denial of Service (DDoS) Attack Mitigation in Software Defined Network (SDN)-Based Cloud Computing Environment." Journal of Ambient Intelligence and Humanized Computing 10: 1985–97.
[7] Geng, Xianjun, and Andrew B Whinston. 2000. "Defeating Distributed Denial of Service Attacks." It Professional 2 (4): 36–42.
[8] Gupta, Brij B, Ramesh Chandra Joshi, and Manoj Misra. 2009. "Defending against Distributed Denial of Service Attacks: Issues and Challenges." Information Security Journal: A Global Perspective 18 (5): 224–47.
[9] Lau, Felix, Stuart H Rubin, Michael H Smith, and Ljiljana Trajkovic. 2000. "Distributed Denial of Service Attacks." In Smc 2000 Conference Proceedings. 2000 Ieee International Conference on Systems, Man and Cybernetics.'cybernetics Evolving to Systems, Humans, Organizations, and Their Complex Interactions'(Cat. No. 0, 3:2275–80.
[10] Zebari, Rizgar R, Subhi R M Zeebaree, Amira Bibo Sallow, Hanan M Shukur, Omar M Ahmad, and Karwan Jacksi. 2020. "Distributed Denial of Service Attack Mitigation Using High Availability Proxy and Network Load Balancing." In 2020 International Conference on Advanced Science and Engineering (ICOASE), 174–79.
[11] Guleria, Charu, and Harsh Kumar Verma. 2018. "Improved Detection and Mitigation of DDoS Attack in Vehicular Ad Hoc Network." In 2018 4th International Conference on Computing Communication and Automation (ICCCA), 1–4.
[12] Alosaimi, Wael, Mazin Alshamrani, and Khalid Al-Begain. 2015. "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, 60–65.
[13] Kumar, Gulshan. 2016. "Denial of Service Attacks--an Updated Perspective." Systems Science \& Control Engineering 4 (1): 285–94.
[14] Robinson, R R Rejimol, and Ciza Thomas. 2012. "Evaluation of Mitigation Methods for Distributed Denial of Service Attacks." In 2012 7th IEEE Conference on Industrial Electronics and Applications (ICIEA), 713–18.
[15] Mölsä, Jarmo. 2005. "Mitigating Denial of Service Attacks: A Tutorial." Journal of Computer Security 13 (6): 807–37.
[16] Fung, Carol J, and Bill McCormick. 2015. "VGuard: A Distributed Denial of Service Attack Mitigation Method Using Network Function Virtualization." In 2015 11th International Conference on Network and Service Management (CNSM), 64–70.

DOI: https://doi.org/10.54216/IJWAC.080205
Received: September 07, 2023 Revised: December 26, 2023 Accepted: April 05, 2024

[17] Mallikarjunan, K Narasimha, K Muthupriya, and S Mercy Shalinie. 2016. "A Survey of Distributed Denial of Service Attack." In 2016 10th International Conference on Intelligent Systems and Control (ISCO), 1–6.
[18] Kaur Chahal, Jasmeen, Abhinav Bhandari, and Sunny Behal. 2019. "Distributed Denial of Service Attacks: A Threat or Challenge." New Review of Information Networking 24 (1): 31–103.
[19] A. Metwaly, A. and Elhenawy, I. (2023) "Sustainable Intrusion Detection in Vehicular Controller Area Networks using Machine Intelligence Paradigm", *Sustainable Machine Intelligence Journal*, 4. doi: 10.61185/SMIJ.2023.44104.

DOI: https://doi.org/10.54216/IJWAC.080205
Received: September 07, 2023 Revised: December 26, 2023 Accepted: April 05, 2024