International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at :www.ijsrcseit.com
doi : https://doi.org/10.32628/CSEIT2361053

A Comprehensive Review on Multi-Class DDoS Attack Classification in IoT

Shivani Sinha[*1], **Sheshang Degadwala**[2]

[*1]Research Scholar, Dept. of Computer Engineering, Sigma Institute of Engineering, Gujarat, India
shivanisinha1000@gmail.com[1]

[2]Associate Professor & Head of Department, Dept. of Computer Engineering, Sigma University, Gujarat, India
sheshang13@gmail.com [2]

ARTICLEINFO

Article History:

Accepted: 10 Oct 2023
Published: 20 Nov 2023

Publication Issue
Volume 9, Issue 10
September-October-2023
Page Number
313-318

ABSTRACT

This review paper provides a comprehensive analysis of multi-class Distributed Denial of Service (DDoS) attack classification in the context of Internet of Things (IoT) environments. The exponential growth of IoT devices has introduced new challenges in securing networks against sophisticated DDoS attacks. In this study, we explore and evaluate various classification techniques and methodologies designed to identify and mitigate multi-class DDoS attacks in IoT ecosystems. The paper synthesizes existing research, highlights key advancements, and identifies gaps in the current literature, offering insights into the state-of-the-art approaches for enhancing the security posture of IoT systems.

Keywords: IoT, DDoS attacks, Multi-class classification, Security, Internet of Things, Attack mitigation, Classification techniques.

I. INTRODUCTION

The advent of the Internet of Things (IoT) has revolutionized the way devices communicate and operate, fostering unprecedented levels of connectivity in various domains. However, this surge in interconnectivity has also exposed IoT environments to a growing array of security threats, with Distributed Denial of Service (DDoS) attacks standing out as a particularly potent menace. Multi-class DDoS attacks, characterized by diverse strategies and vectors, pose a significant challenge to the robustness of IoT systems. As the number of connected devices continues to escalate, understanding and effectively mitigating these sophisticated attacks become paramount. This comprehensive review delves into the intricate landscape of multi-class DDoS attack classification in the context of IoT, aiming to provide a detailed synthesis of existing research, methodologies, and emerging trends.

The escalating threat landscape necessitates a deeper exploration of the existing strategies and methodologies employed for classifying multi-class DDoS attacks in IoT environments. This review aims to bridge the gap in the current literature by systematically examining the various classification techniques and their effectiveness in distinguishing and mitigating diverse forms of DDoS threats targeting IoT devices. By scrutinizing the strengths and limitations of these approaches, this paper aims to equip researchers, practitioners, and policymakers with a nuanced understanding of the state-of-the-art in multi-class DDoS attack classification, paving the way for more resilient and adaptive security frameworks.

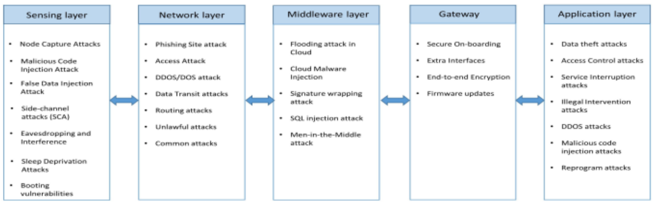

Figure 1. Security Thread in IoT

As we embark on this comprehensive review, it becomes evident that a holistic understanding of the intricacies surrounding multi-class DDoS attacks in IoT is essential for fortifying the security posture of these interconnected systems. By synthesizing existing knowledge and identifying research gaps, this paper seeks to contribute to the ongoing discourse on IoT security, providing valuable insights that can inform the development of robust countermeasures against the evolving landscape of multi-class DDoS threats in IoT ecosystems.

II. LITERATURE STUDY

The literature study encompasses a diverse range of research efforts aimed at advancing the field of soybean leaf disease detection and classification. Li et al. [1] proposed a method based on RGB images and machine learning for soybean leaf estimation. Shrivastava [2] employed intelligent deep learning techniques for cotton leaf and plant disease identification. Barro et al. [3] provided a comprehensive review of frogeye leaf spot caused by Cercospora sojina, emphasizing its impact on soybean crops. Gautam et al. [4] introduced a transfer learning-based artificial intelligence model for leaf disease assessment, contributing to the ongoing exploration of transfer learning applications in agriculture.

Miao et al. [5] focused on soybean disease identification using deep learning, adding to the growing body of research leveraging deep neural networks in plant pathology. Fagodiya et al. [6] investigated the impact of weather parameters on Alternaria leaf spot of soybean, shedding light on the environmental factors influencing disease development. Tugrul et al. [7] presented a comprehensive review on the application of convolutional neural networks in the detection of plant leaf diseases, providing insights into the advancements in deep learning techniques.

Lin et al. [8] offered a global perspective on breeding for disease resistance in soybean, addressing the importance of disease-resistant cultivars. Vallabhajosyula et al. [9] introduced a transfer learning-based deep ensemble neural network for plant leaf disease detection, contributing to the development of robust detection models. McDonald et al. [10] proposed an automated, image-based disease measurement approach for phenotyping resistance to soybean frogeye leaf spot, showcasing advancements in automated phenotyping methods.

Yu et al. [11] developed a recognition method for soybean leaf diseases based on an improved deep learning model, contributing to the refinement of deep learning techniques in disease classification. Andrew et al. [12] explored deep learning-based leaf disease detection in crops for agricultural applications, highlighting the potential of deep learning in precision agriculture. Karlekar and Seal [13] introduced SoyNet, a soybean leaf diseases classification model, showcasing specialized architectures for disease recognition. Rajput et al. [14] focused on soybean leaf diseases detection and classification using recent image processing techniques, contributing to the broader exploration of image processing methods in disease identification. Wallelign et al. [15] utilized convolutional neural networks for soybean plant disease identification, demonstrating the application of advanced neural network architectures in the context of agriculture.

This comprehensive literature study underscores the diverse and evolving approaches in the field of soybean leaf disease detection, ranging from traditional machine learning methods to state-of-the-art deep learning techniques. The collective insights from these studies provide a foundation for ongoing research endeavors aimed at enhancing the accuracy and efficiency of disease detection systems for sustainable soybean cultivation.

III.METHODOLOGY

A. Dataset [1]

The Comprehensive, International Cybersecurity for Distributed Denial of Service (CICDDoS2019) dataset represents a critical resource for studying network security, specifically focusing on two network attack scenarios and the corresponding victim network. This dataset is designed to simulate the execution of two Distributed Denial of Service (DDoS) attacks, targeting both TCP and UDP protocols, offering a diverse set of challenges for cybersecurity researchers. Researchers can access the data in two convenient formats: packet capture (PCAP) and comma-separated values (CSV). This flexibility enables a wide range of analyses, from in-depth packet-level examinations to comprehensive statistical evaluations, making the CICDDoS2019 dataset an asset for advancing research in DDoS attack detection and mitigation within the realm of network security.

B. Pre-Process

Null Removal: This crucial pre-processing step involves the identification and removal of null or missing values within the dataset. Null removal ensures the integrity of the dataset, preventing potential disruptions in subsequent analyses.

Unwanted Column Drop: To streamline the dataset and focus on relevant features, unwanted columns are identified and subsequently dropped. This step aims to enhance computational efficiency and improve the overall performance of the classification models.

Categorical Encoding: Categorical encoding transforms categorical variables into numerical representations, enabling machine learning algorithms to process and analyze these features effectively. This step is essential for models that require numerical inputs, ensuring a seamless integration of categorical information.

Normalization: Normalization is applied to standardize numerical features, preventing biases in the model due to varying scales. This process ensures that all numerical values are within a consistent range, promoting fair and accurate comparisons during model training.

C. Machine Learning

Machine Learning Within the expansive realm of machine learning, a sophisticated array of powerful algorithms has been intricately applied to grapple with the multifaceted challenge of classifying multi-class Distributed Denial of Service (DDoS) attacks in the intricate landscape of Internet of Things (IoT) environments:

Support Vector Machine (SVM) [1,3]: Leveraging its prowess in navigating high-dimensional spaces, SVM diligently seeks to establish an optimal hyperplane that effectively segregates various classes of DDoS attacks. In the context of IoT security, SVM plays a crucial role in ensuring precise and discerning classification of different types of DDoS attacks targeting interconnected devices.

K-Nearest Neighbors (KNN) [1,3]: Operating as a neighbor-based classifier, KNN meticulously examines the proximity of instances in the feature space. In the context of multi-class DDoS attack classification in IoT, KNN provides a nuanced understanding by considering the collective characteristics of neighboring samples, thereby enhancing the granularity of the classification process.

Random Forest (RF) [10,14]: Functioning as a sophisticated ensemble learning approach, RF taps into the collective wisdom of multiple decision trees to discern intricate patterns within IoT network traffic. This approach fosters robust classification outcomes, particularly in the context of the diverse and evolving landscape of DDoS attacks on IoT systems.

Decision Tree (DT) [10,14]: With its intuitive tree-like structure, DT navigates through feature attributes to make decisions, offering transparency in understanding the decision-making process. In the realm of IoT security, DT enhances our ability to classify diverse forms of DDoS attacks on connected devices, providing valuable insights into the underlying factors influencing classification outcomes.

XGBoost [3]: Renowned for its efficiency, XGBoost employs optimized gradient boosting, constituting an ensemble method that incrementally refines models to achieve superior accuracy. In the context of multi-class DDoS attack classification in IoT, XGBoost stands out for its ability to adapt and evolve, contributing to the identification and classification of diverse DDoS threats with precision in the dynamic IoT security landscape.

TABLE I

COMPARATIVE ANALYSIS

Method	Pros	Cons
Support Vector Machine (SVM) [1,3]	- Effective in high-dimensional spaces. - Works well with clear margin of separation. - Memory efficient.	- Can be sensitive to noise. - Prone to overfitting if the data is not well-scaled and normalized.
K-Nearest Neighbors (KNN) [1,3]	- Simple and intuitive. - No training phase; directly uses labeled data. - Robust to noisy training data.	- Computationally expensive, especially with large datasets. - Highly sensitive to irrelevant features.
Random Forest (RF) [10,14]	- High accuracy and robustness. - Effective in handling large datasets with many features. - Reduces overfitting.	- Can be computationally intensive. - Lacks interpretability due to ensemble structure.
Decision Tree (DT) [10,14]	- Easy to understand and interpret. - Requires minimal data preparation. - Handles both numerical and categorical data.	- Prone to overfitting. - Sensitive to small variations in data, leading to different tree structures.
XGBoost [3]	- High performance and efficiency. - Regularization to prevent overfitting. - Handles missing values and outliers well.	- Requires careful tuning of hyperparameters. - Can be computationally demanding.

IV.CONCLUSION

In conclusion, this comprehensive review on multi-class DDoS attack classification in IoT has provided valuable insights into the current state of research in this critical domain. The exploration of various classification techniques, including machine learning algorithms, has underscored the complexity and dynamic nature of the DDoS threat landscape in the context of Internet of Things (IoT) environments. The synthesis of existing literature has revealed that while significant progress has been made in developing effective classification models, there is still room for improvement. Particularly, the integration of feature selection methods with ensemble learning techniques emerges as a promising avenue for enhancing the accuracy and efficiency of multi-class DDoS attack classification in IoT scenarios.

Future research endeavors should focus on the practical implementation and evaluation of feature selection in conjunction with ensemble learning methodologies. Rigorous empirical studies should be conducted to assess the performance of these combined approaches across diverse IoT environments and under various attack scenarios. Additionally, exploring adaptive and real-time feature selection mechanisms can further refine the models' capabilities in responding to the evolving nature of DDoS attacks. As the IoT landscape continues to expand, incorporating innovative technologies and refining existing methodologies will be essential to fortify the security posture of IoT systems against the growing threat of DDoS attacks.

V. REFERENCES

[1] J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, “Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks,” Engineering Applications of Artificial Intelligence, vol. 123, no. July 2022, p. 106432, 2023, doi: 10.1016/j.engappai.2023.106432.

[2] F. S. de Lima Filho, F. A. F. Silveira, A. de Medeiros Brito Junior, G. Vargas-Solar, and L. F. Silveira, “Smart detection: An online approach for DoS/DDoS attack detection using machine learning,” Secur. Commun. Netw., vol. 2019, pp. 1–15, 2019.

[3] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, “Toward a lightweight intrusion detection system for the internet of things,” IEEE Access, vol. 7, pp. 42450–42471, undefined 2019.

[4] Y. Otoum and A. Nayak, “AS-IDS: Anomaly and signature-based IDS for the internet of things,” J. Netw. Syst. Manag., vol. 29, no. 3, 2021.

[5] R. Zagrouba and R. AlHajri, “Machine Learning based attacks detection and countermeasures in IoT,” International j. commun. netw. inf. secur., vol. 13, no. 2, 2021.

[6] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, “Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology,” Internet of things, vol. 11, no. 100227, p. 100227, 2020.

[7] S. Pokhrel, R. Abbas, and B. Aryal, “IoT Security: Botnet detection in IoT using Machine learning,” arXiv [cs.LG], 2021.

[8] E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap, “A supervised intrusion detection system for smart home IoT devices,” IEEE Internet Things J., vol. 6, no. 5, pp. 9042–9053, 2019.

[9] M. Essaid, D. Kim, S. H. Maeng, S. Park, and H. T. Ju, “A collaborative DDoS mitigation solution based on ethereum smart contract and RNN-LSTM,” in 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2019, pp. 1–6.

[10] U. Javaid, A. K. Siang, M. N. Aman, and B. Sikdar, “Mitigating loT Device based DDoS Attacks using Blockchain,” in Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, 2018.

[11] R. Singh, S. Tanwar, and T. P. Sharma, “Utilization of blockchain for mitigating the distributed denial of service attacks,” Secur. Priv., vol. 3, no. 3, 2020.

[12] K. Bhardwaj, J. C. Miranda, and A. Gavrilovska, “Towards IoT-DDoS prevention using edge computing,” Usenix.org. [Online]. Available: https://www.usenix.org/system/files/conference/hotedge18/hotedge18-papers-bhardwaj.pdf.

[13] P. Kumar, R. Kumar, G. P. Gupta, and R. Tripathi, "A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT Systems by leveraging Fog computing," Trans. emerg. telecommun. technol., vol. 32, no. 6, 2021.

[14] N.-N. Dao et al., "Securing heterogeneous IoT with intelligent DDoS attack behavior learning," IEEE Syst. J., pp. 1–10, undefined 2021.

[15] V. Adat and B. B. Gupta, "A DDoS attack mitigation framework for internet of things," in 2017 International Conference on Communication and Signal Processing (ICCSP), 2017, pp. 2036–2041.

Cite this article as :

Shivani Sinha, Sheshang Degadwala, "A Comprehensive Review on Multi-Class DDoS Attack Classification in IoT ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 10, pp.313-318, September-October-2023. Available at doi : https://doi.org/10.32628/CSEIT2361053
Journal URL : https://ijsrcseit.com/CSEIT2361053