International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 12 | Dec 2024 www.irjet.net p-ISSN: 2395-0072

DoS and DDoS Attack Detection: A Comprehensive Literature Review

Jinsu Anna John[1], K V Neha[2], Vanimol Sajan[3]

Dept. of Computer Science and Engineering
College of Engineering, Kallooppara, Thiruvalla

Abstract - *As the IoT (Internet of Things) keeps expanding across diverse domains, ensuring the security of IoT devices becomes paramount. One critical aspect of this security landscape is the identification of Denial of Service- DoS and Distributed Denial of Service- DDoS attacks targeting IoT systems. This paper presents a comprehensive literature survey that navigates the evolving IoT security landscape, focusing on the application of CNN- CNN-convolutional neural Network and GRU Gated Recurrent Unit models for attack detection. The survey examines key research contributions, methodologies, and findings from existing studies, shedding light on modern IoT security techniques. Special attention is given to the unique characteristics and challenges posed by attacks via DoS and DDoS in the context of IoT. Furthermore, the paper explores the capabilities of CNN-GRU models in capturing spatial and temporal patterns, critically analyzing their effectiveness in enhancing IoT security. With this survey, we hope to offer insightful information about the current trends, gaps, and future directions in securing IoT ecosystems against DoS and DDoS threats.*

Key Words: DoS, DDoS, CNN, GRU, SMOTE

1. INTRODUCTION

While the Internet of Things (IoT) paradigm has offered unparalleled ease, it has also highlighted a multitude of security vulnerabilities due to the rapid proliferation of interconnected devices. Among the formidable threats faced by IoT ecosystems, DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks stick out as persistent and evolving adversaries. These attacks, orchestrated to disrupt normal functioning by overwhelming targeted systems with a flood of malicious requests, pose a severe risk to the integrity and availability of IoT devices.

Traditional methods of combating DoS and DDoS attacks often fall short in the dynamic and heterogeneous landscape of IoT. As adversaries continually refine their strategies, there arises a pressing need for adaptive and intelligent security mechanisms. This has encouraged the application of deep learning methods to IoT security, such as Gated Recurrent Units (GRU) and Convolutional Neural Networks (CNN).

CNN, with its proficiency in capturing spatial patterns, and GRU, renowned for handling temporal dependencies, offer promising avenues for robust intrusion detection. By leveraging the inherent characteristics of IoT data, these deep learning models have demonstrated notable success in identifying anomalous patterns associated with DoS and DDoS attacks. The integration of deep learning and IoT security is explored in this paper's extensive literature review, specifically focusing on the efficacy of CNN and GRU models in detecting and mitigating such attacks.

Furthermore, we explore the integration of SMOTE-Synthetic Minority Over Sampling Technique algorithms to address class imbalance issues inherent in intrusion detection datasets. The application of SMOTE aims to enhance the models' ability to discern subtle patterns associated with attacks, thereby contributing to a more resilient and accurate defense mechanism for IoT environments.

Through an examination of existing literature, methodologies, and emerging trends, this paper aims to unravel the intricate interplay between DoS, DDoS, Deep Learning, CNN, GRU, and the strategic application of the SMOTE algorithm in fortifying the security posture of IoT ecosystems. Through our contributions to the current conversation on safeguarding the quickly changing Internet of Things, we provide light on current research and suggest directions for future study.

2. LITERATURE SURVEY

1.1 Attack Detection Using Machine Learning and Neural Network [11]

The contemporary digital landscape heavily relies on ubiquitous internet usage, with its prevalence continually increasing. However, this surge in internet use is accompanied by a corresponding rise in threats. Among these threats is the DoS attack, a tactic that exploits seemingly legitimate demands for services to acquire overuse of network and computing resources, leading to the denial of access for authorized users. Denial of Service attacks can appear at the network, transport, and application layers of the OSI model. This paper addresses the effective detection of DoS attacks by leveraging Machine Learning (ML) and Neural Network (NN) algorithms [11]. Notably, the focus of identification is directed notably towards application layer DoS attacks, distinct from transport and network DoS attacks. The study employs the CIC IDS 2017 dataset, the latest in DoS attack datasets, segmented into different splits for analysis. The comparative analysis of Random Forest-RF and Multi-Layer Perceptron- MLP algorithms reveals the superior performance of RF over MLP.

The suggested procedure comprises multiple stages categorizing DoS attacks: The preprocessing step involves training the system with a predetermined percentage of data. Finally, machine learning and neural network classifiers, such as RF and MLP, are simulated to categorize the dataset into Benign and DoS attack classes. The system gathers input data from the CIC IDS 2017 Wednesday dataset with all attributes. Simulation is conducted using the well-known machine learning tool Weka.

Notably, the suggested system does not do multi-classification for particular attacks such as HTTP flood, slowhttptest, Heartbleed, and slow loris. The next step is to evaluate the system for the multi-classification of DoS attacks while minimizing the features.

1.2 An Anomaly Behavior-based Detection and Prevention of DoS Attack in IoT Environment [4]

IoT stands out as a predominant technology facilitating information gathering and sharing across various applications. In the realm of IoT, communication among devices is established through protocols such as IEEE 802.11 and IEEE 802.15.4. For IoT nodes, using Low Power IEEE 802.11 as the communication protocol guarantees more bandwidth and a wide coverage range. However, In this case, Denial of Service (DoS) attacks, including as de-authentication, disassociation, injection tests, authentication floods, and association floods, might affect the MAC Layer protocols.

This paper introduces the Topology Management Method (TMM) as a preventive measure against DoS attacks, employing behavior analysis. The approach involves scrutinizing the order in which the protocol changes at the MAC layer during a given period of time. It is possible to assess how well IoT nodes communicate by keeping an eye on these transitions. Frame Capture and Feature Extractor, Behavior Analysis, Normal Model for Sequential Patterns Generation, Anomaly Characterization Function, and Prevention of Denial of Service Attack are the five modules that make up the Anomaly Behavior Detection for Denial of Service Attacks.

1.3 A Denial of Service Attack Method for an IoT System [5]

In recent years, the widespread adoption of the Internet of Things (IoT) across various domains has become increasingly prevalent. However, this proliferation of IoT systems has introduced new challenges, particularly in terms of security. The vulnerability of IoT systems to potential attacks poses a significant risk, as such breaches could result in substantial property losses. This paper delves into the realm of IoT security, specifically exploring the threat of a DoS attack. Using the versatile penetration testing tool Kali Linux, the study demonstrates a DoS attack on an IoT system, employing three distinct methods. This paper also provides a comparative analysis of the three DoS attack methods, shedding light on their respective effectiveness.

Furthermore, the research introduces a novel DoS attack method specifically designed and implemented for IoT systems. The experiment involves launching DoS attacks on the target IoT system using different methods, and the resulting empirical data serves to examine the impact of these cyberattack techniques. The study anticipates further exploration, with upcoming research aiming to delve into additional attack methods and conduct a comprehensive analysis of their effectiveness. This ongoing investigation seeks to provide an incisive analysis of the evolving landscape of Internet of Things security and cyber-attack mitigation.

1.4 DDoS Attack Detection Based on Simple ANN with SMOTE for IoT Environment [7]

With the rapid development of the Internet of Things (IoT) era in recent years, cyber attackers increasingly target IoT environments. They exploit IoT devices, essentially turning them into bots to launch attacks on target organizations. These devices are particularly susceptible to IoT malware due to their resource constraints, making it challenging to implement robust security mechanisms. Notably, infamous IoT malware like Mirai has executed DDoS attacks on targeted organizations via hacked Internet of Things devices. Despite the implementation of various security measures for IoT devices, there remains a crucial need for an effective detection system tailored to IoT environments.

To address this need, our detection system leverages a publicly available dataset and employs a ML technique, specifically an Artificial Neural Network with a straightforward architecture. While detecting DDoS attack with the use of the contemporary botnet attack dataset Bot-IoT, a significant challenge arises due to an imbalance in the dataset. This imbalance is characterized by a significant quantity of attack data and a little amount of benign data. To mitigate this issue, we incorporate the Synthetic Minority Over-sampling Technique-SMOTE, an effective approach that balances the data between normal behavior and deviant behavior.

SMOTE proves to be a crucial tool in achieving balanced data, addressing the misclassification problem that can arise when there is a significant disparity in the number of data points for each class. Importantly, employing an imbalanced dataset in the development of a classification model potentially affects the detection system's stability and performance. Looking ahead, our prospects intend to extend the effectiveness of the suggested approach by detecting other types of attacks tailored for IoT environments. This ongoing research strives to enhance the overall security posture of IoT ecosystems

1.6 Detection of DDoS Attack and Classification Using a Hybrid Approach [6]

In the realm of cloud security, detecting Distributed Denial of Service (DDoS) attacks poses a significant challenge, especially to ensure legitimate users can properly utilize cloud resources. This paper addresses this challenge by employing various machine-learning classifiers to detect and classify attacking packets and normal packets. The dataset NSL KDD is utilized, and pertinent characteristics are selected using five commonly employed feature selection methods: Information gain, gain ratio, chi-squared, reliefF, and symmetrical uncertainty [10].

The KDD DDoS dataset is produced by separating only the DDoS packets from the entire dataset using the selected features, hence producing a specialized dataset for DDoS detection. This dataset is discretized using the Weka tool to enhance performance. Subsequently, the discretized dataset is evaluated using frequently employed classifiers, including Bayes Net, Naive Bayes, J48, Decision Table and Random Forest. The system's robustness is measured through 10-fold cross-validation.

The effectiveness of hybrid technique for selecting features is assessed by comparing its performance with existing feature selection methods on the above mentioned dataset. The procedure that is suggested obtains an average detection rate of 98.47% and a spectacular anomaly detection rate of 99.72% Analogous evaluations are conducted on the NSL DDoS dataset, yielding a DDoS detection rate average of 99.01% and an optimal DDoS detection rate of 99.86%. Comparative analyses with existing methods reveal that the proposed hybrid approach outperforms others in DDoS attack detection rates.

Looking ahead, the authors express intentions to create a DDoS detector in an actual cloud setting, leveraging actual traffic data. Additionally, efforts will be made to create a preventative plan to effectively minimize actual DDoS attacks in future work.

1.7 A Novel Algorithm for DoS and DDoS attack detection in Internet Of Things [2]

The intricate network of diverse objects connected to the Internet poses significant challenges in ensuring the security and privacy of users. As the Internet is the foundation of the IoT, it inherits and propagates security threats and attacks. The resource-constrained nature of IoT networks makes them susceptible to Distributed Denial of Service attacks, posing a grave risk to the functionality and longevity of these devices. Early detection of Denial of Service and DDoS attacks is crucial to preventing victims of devices with limited resources. The constrained Application Protocol (CoAP) is frequently used at the application layer in the context of constrained networks, its security protocol being Datagram Transport Layer Security (DTLS). Nevertheless, DoS attacks can be launched against DTLS itself.

This paper introduces an innovative algorithm designed for the early identification and defense against DDoS and DoS attacks, specifically tailored for constrained environments. The proposed algorithm is implemented and evaluated using the Contiki Cooja simulator. Results demonstrate its superior performance compared to the E-Lithe algorithm. Evaluation metrics include malicious packet delivery ratio and legitimate packet delivery ratio [3]. As part of upcoming projects, the suggested algorithm will be in contrast with additional existing methods, and a more in-depth analysis will be conducted to enhance its robustness and effectiveness in securing constrained IoT environments.

1.8 IoT DoS and DDoS Attack Detection using ResNet [1]

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks have emerged as particularly prevalent threats in IoT networks. In many cases, sophisticated DoS and DDoS attacks are difficult for conventional security measures, such as firewalls and intrusion detection systems, to detect due to their reliance on static predefined rules for filtering normal and malicious traffic. However, integrating these solutions with artificial intelligence (AI) techniques enhances their reliability and effectiveness. Leveraging CNN models potential, this study proposes an approach that transforms network traffic data into image format. The advanced CNN model used in this research, namely ResNet, is trained on the converted data. The results underscore the efficacy of the proposed approach in leveraging deep learning for the efficient detection of complex DoS and DDoS attacks in IoT networks. Nevertheless, because of their effective performance in the fields of computer vision and image processing, deep learning models—particularly CNN models—have attained great prominence. Nevertheless, network threat detection is another function for these CNN models.

2. COMPARISON

The following session shows a comparison between several methods discussed in the above papers for detection of DoS and DDoS

Sr.no	Title	Algorithm/Method	Description
1	DoS Attack Detection Using Machine Learning and Neural Network[11]	Random Forest, Multi-Layer Perceptron	DoS attack detection using ML and NN algorithms, focusing on app layer attacks, employing CICIDS2017 dataset, showing Random Forest's superiority over MLP in classification.
2	An Anomaly Behavior based Detection and Prevention of DoS Attack in IoT Environment [4]	The behavior analysis-based Topology Management Method(TMM)	Paper introduces a detection and Prevention of Anomalies based on Behaviour system for IoT DoS attacks, utilizing TMM and Fine-Grained Detection Algorithm to analyze MAC layer protocol transitions and detect anomalies
3	Denial of Service Attack Method for an IoT System[5]	Comparative analysis of Kali Linux-based three denial of service (DoS) attack techniques for Internet of Things systems	Paper showcases various DoS attack methods on IoT systems via Kali Linux
4	DDoS Attack Detection Based on Simple ANN with SMOTE for IoT Environment [7]	Artificial Neural Network(ANN), SMOTE	DDoS attack detection system for IoT, using a simple ANN architecture and addressing data imbalance with SMOTE from the Bot-IoT dataset.
6	Detection of DDoS Attack and Classification Using a Hybrid Approach[6]	Decision Tree, Random Forest	The paper introduces a hybrid approach for identifying and categorizing DDoS assaults in cloud computing se tings, employing machine learning classifiers and feature selection methods on the NSL KDD dataset. It achieves high detection rates, surpassing existing approaches
7	A Novel Algorithm for DoS and DDoS attack detection in Internet Of Things[2]	Novel algorithm which consist of primary check and secondary check algorithm	An innovative technique for early DoS and DDoS attack detection and mitigation in Internet of Things scenarios, tailored for constrained networks using CoAP and DTLS is discussed in paper
8	IoT DoS and DDoS Attack Detection using ResNet [1]	ResNet	A ResNet- based approach for identifying IoT DoS and DDoS attacks .By transforming network traffic data into images and training ResNet, the approach efficiently detects complex attacks in IoT networks using deep learning techniques

Table -1: Comparative Analysis

3. CONCLUSIONS

A Denial-of-Service attack is an attack which can be used to influence the connection of network, making it inaccessible to its intended users [5]. In DDoS attack server gets too many service requests from multiple systems [9]. After getting so many requests the server becomes very busy and cannot respond to any of the service requests [6]. In conclusion, this literature survey navigates the intricate landscape of IoT security, with a focused exploration of DoS and DDoS attack detection using deep learning models, specifically CNN and GRU, supplemented by the strategic application of the SMOTE algorithm. The synthesis of diverse studies reveals a growing recognition of the severity of security threats in IoT environments and the imperative for advanced intrusion detection mechanisms. The effectiveness of CNN and GRU models in capturing spatial and temporal patterns, coupled with the mitigation of class imbalance through SMOTE, underscores the potential for robust defense mechanisms. As we reflect on the existing body of knowledge, it becomes evident that while substantial progress has been made, challenges persist, and opportunities for further refinement and innovation abound. This survey not only consolidates current insights but it acts as a basis for upcoming research paths, promoting the ongoing development of security strategies to safeguard the expanding realm of IoT.

4. FUTURE SCOPE

DoS and DDoS attacks emerge as prominent threats within the Internet of Things (IoT) landscape. Existing solutions encounter difficulties in accurately identifying the intricate nature of these attacks. This challenge stems primarily from their reliance on outdated or incomplete datasets that fail to encompass modern reflective DDoS attacks. Convolutional Neural Networks (CNNs) demonstrate limited effectiveness when low-dimensional or non-image datasets were used for

training, as their architecture is primarily optimized for addressing computer vision tasks. Notably, network traffic datasets are typically available in formats such as .pcap, .csv, or .txt. To harness the CNNs capacity to effectively identify DoS and DDoS attacks and convert network traffic data into visual representations is advisable. A CNN-GRU model emerges as a promising approach for detecting both DoS and DDoS attacks.

REFERENCES

[1] Faisal Hussain, Syed Ghazanfar Abbas, Muhammad Husnain, Ubaid U Fayyaz, Farrukh Shahzad, and Ghalib A Shah. Iot dos and ddos attack detection using resnet. In 2020 IEEE 23rd International Multitopic Conference (INMIC), pages 1–6. IEEE, 2020.

[2] Shruti Kajwadkar and Vinod Kumar Jain. A novel algorithm for dos and ddos attack detection in internet of things. In 2018 Conference on Information and Communication Technology (CICT), pages 1–4. IEEE, 2018.

[3] Zainab Dalaf Katheeth and KK Raman. Performance evaluation with throughput and packet delivery ratio for mobile ad-hoc networks. International Journal of Advanced Resaerch in Computer and Com munication Engineering, 3(5), 2014.

[4] S Santhosh Kumar and K Kulothungan. An anomaly behavior based detection and prevention of dos attack in iot environment. In 2017 Ninth International Conference on Advanced Computing (ICoAC), pages 287 292. IEEE, 2017.

[5] Lulu Liang, Kai Zheng, Qiankun Sheng, and Xin Huang. A denial of service attack method for an iot system. In 2016 8th international conference on Information Technology in Medicine and Education (ITME), pages 360–364. IEEE, 2016.

[6] Suman Nandi, Santanu Phadikar, and Koushik Majumder. Detection of ddos attack and classification using a hybrid approach. In 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP), pages 41–47. IEEE, 2020.

[7] Yan Naung Soe, Paulus Insap Santosa, and Rudy Hartanto. Ddos attack detection based on simple ann with smote for iot environment. In 2019 fourth international conference on informatics and computing (ICIC), pages 1–5. IEEE, 2019.

[8] I Varalakshmi, M Thenmozhi, and R Sasi. Detection of distributed denial of service attack in an internet of things environment-a review. In 2021 international conference on system, computation, automation and networking (ICSCAN), pages 1–6. IEEE, 2021.

[9] Keerthi Vasan K and Surendiran B. Feature subset selection for intrusion detection using various rank based algorithms. International Journal of Computer Applications in Technology, 55:298, 01 2017.

[10] Shreekh Wankhede and Deepak Kshirsagar. Dos attack detection using machine learning and neural network. In 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), pages 1–5. IEEE, 2018