International Journal of Research Publication and Reviews, Vol 4, no 12, pp 4771-4776 December 2023

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Review on DDoS Attacks on IOT Devices

Gudla Satya Abhishek

B. Tech Student, Department of IT, GMR Institute of Technology, Rajam-532127, Andhra Pradesh, India.
Email: 21341A1247@gmrit.edu.in[1]

ABSTRACT

Distributed Denial-of-Service (DDoS) attacks have drawn extensive attention in the cyberspace during the last few years. The DDoS attacks can threaten the availability of the SDN due to the difference in the architecture between the SDN network and the traditional network. Especially, the SDN controller is the most vulnerable part to be affected by the DDoS attacks. In general, the DoS attack is an attempt to make the resources of a network unavailable for legitimizing users. Real-time applications of DDoS (Distributed Denial of Service) attacks on IoT devices highlight the potentially disastrous consequences of such cyberattacks. These attacks can have a profound impact on various sectors, including Smart Homes: Attackers can target IoT devices within smart homes, disrupting essential services like security cameras, smart locks, thermostats, and even appliances. This can lead to breaches of privacy, property damage, or theft. DoS attacks exploit various weaknesses in computer network technologies. They may target servers, network routers. weak security mechanisms, and lack of standardization. To effectively combat DDoS attacks on IoT devices, proactive measures are necessary. This section will discuss various strategies and countermeasures to mitigate the vulnerabilities associated with IoT devices, including enhanced security protocols, intrusion detection systems, and the development of more robust and resilient IoT infrastructure. It will explore ongoing research and industry efforts to address these limitations and protect IoT ecosystems. we propose to experimentally evaluate an entropy-based solution to detect and mitigate DoS and DDoS attacks in IoT scenarios using a stateful SDN data plane.

Keywords: *DDoS Attacks, Strateful SDN, IOT, Cyber Security*

1. INTRODUCTION

Everyday objects like smart thermostats and refrigerators and to industrial sensors and autonomous vehicles, are now interconnected, allowing for different techniques like remote control automation etc. However, amid this technological revolution lies a pressing cybersecurity concern: Distributed Denial of Service attacks targeting IoT devices. DDoS attacks on IoT devices represent a significant and growing threat. These attacks involve flooding a device or network with a deluge of malicious traffic, originating from a multitude of sources. The objective is to overwhelm the target, rendering it inaccessible to legitimate users. The consequences of such attacks can be severe, ranging from disruptions and data breaches to financial losses and even safety risks in critical infrastructure scenarios. These attacks are diverse. Some attackers may have financial or political motives. IoT devices are attractive targets due to their often inadequate security measures, making them susceptible to compromise and inclusion in botnets, armies of compromised devices controlled by malicious actors.

2. LITERATURE SURVEY

2.1 Zeeshan, M., Riaz, Q., Bilal, M. A., Shahzad, M. K., Jabeen, H., Haider, S. A., & Rahim, A. (2021). Protocol-based deep intrusion detection for dos and ddos attacks using unsw-nb15 and bot-iot data-sets.

The literature survey focused on the detection and mitigation of DoS attacks in a network environment. The experimental setup involved a network topology with a Ryu controller managing the network and an application for detection and mitigation running on top of it. Different types of DoS attacks, including flooding and TCP SYN flood attacks, were considered in the experiments. Entropy-based algorithms were used for attack detection, and flow tables were modified to drop malicious traffic while preserving legitimate traffic. These algorithms measure the randomness or uncertainty of network traffic patterns to identify abnormal or malicious behavior. The use of entropy-based algorithms allows for effective and accurate detection of DoS attacks, enabling timely mitigation measures to be implemented.

2.2 Rahman, O., Quraishi, M. A. G., & Lung, C. H. (2019, July). DDoS attacks detection and mitigation in SDN using machine learning. In 2019 IEEE world congress on services (SERVICES) (Vol. 2642, pp. 184-189). IEEE.

Focused on the topic of network security in software-defined networking (SDN) environments. The survey examined the common threat of Distributed Denial of Service (DDoS) attacks on the network controller in SDN. These algorithms analyse the randomness or uncertainty of network traffic patterns to identify abnormal behaviour indicative of DoS attacks.

J48 is a decision tree algorithm that is commonly used for classification tasks. It is a type of supervised learning algorithm, which means that it needs to be trained on a dataset of labeled examples in order to make predictions on new data.

Random Forest is an ensemble learning algorithm that combines multiple decision trees to make predictions. This makes it more robust to noise in the data than J48, and it can also capture more complex relationships between features. However, it can be more computationally expensive to train and use than J48.

2.3 Li, J., Liu, M., Xue, Z., Fan, X., & He, X. (2020). RTVD: A real-time volumetric detection scheme for DDoS in the Internet of Things. IEEE Access, 8, 36191-36201.

This includes multiple papers on DDoS attack detection and prevention techniques. One proposes a single directional packet filter to prevent DDoS attacks by appending the timestamp of each packet to the 5-tuple, allowing for consideration of time-domain characteristics. Another paper suggests using an LSTM-based prediction model to filter out background noise and reduce false alarms in DDoS detection. A modified Quartile Deviation algorithm, called QuinDC, is proposed for immediate check and alarm of suspicious packets based on real-time entropy values.The TFOR scheme is used to measure the effectiveness of DDoS attack recognition, with an average delay of 0.015172 seconds for volumetric DDoS attacks.This includes DDoS attack detection and prevention techniques, such as a single directional packet filter, LSTM-based prediction model, modified Quartile Deviation algorithm (QuinDC), and methods to reduce entropy calculation time complexity. The effectiveness of DDoS attack recognition is measured using the TFOR scheme.

2.4 Galeano-Brajones, J., Carmona-Murillo, J., Valenzuela-Valdés, J. F., & LunaValero, F. (2020). Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: An experimental approach. Sensors, 20(3), 816.

DDoS attack detection and prevention techniques have been extensively studied in the literature. Various approaches have been proposed, including single directional packet filters, LSTM-based prediction models, modified Quartile Deviation algorithms, and methods to reduce entropy calculation time complexity. The effectiveness of DDoS attack recognition can be measured using the TFOR scheme, which has shown an average delay of 0.015172 seconds for volumetric DDoS attacks. Overall, the literature survey highlights the importance of developing efficient and reliable DDoS detection and mitigation techniques to protect cyberspace. DDoS detection and mitigation techniques have been extensively studied in the literature.

2.5 Vishwakarma, R., & Jain, A. K. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommunication systems, 73(1), 3-25.

Malware and botnets play a significant role in DDoS attacks in IoT networks. Once a botnet is formed, the attacker instructs each bot to send bogus packets to the targeted web server simultaneously, making it inaccessible to legitimate traffic. Neglecting in securing IoT devices contributes to their vulnerability to botnet infections. Detecting IoT malware botnets can be done using image processing techniques and lightweight convolutional neural networks. IOT botnets are more advanced than traditional botnets as they can compromise a larger number of IoT devices that are constantly connected to the internet. Once a botnet is formed, the attacker instructs each bot to send bogus packets to the targeted web server simultaneously, making it inaccessible to legitimate traffic.

3.METHODOLOGY

3.1 DL Algorithm And LSTM Model:

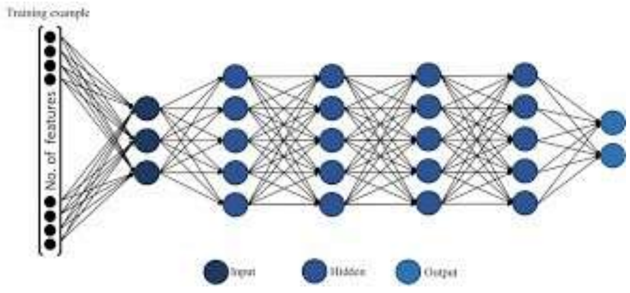

Figure 1: Basic structure of DL algorithm

Figure 1 The diagram has three layers: input, hidden, and output. The input layer has six nodes, the hidden layer has nine nodes, and the output layer has three nodes.

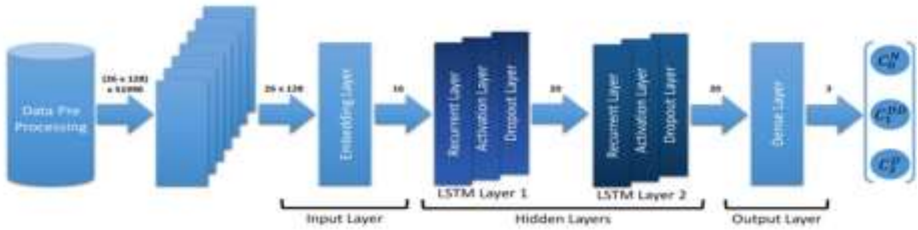

Figure 2: Structure of LSTM Model

Figure 2: Structure of LSTM model showing input, hidden and output layers. The diagram has three layers. The first layer is the input layer, which is represented by a blue cylinder labeled “Data Pre-Processing”. The second layer is the hidden layer, which is represented by a series of blue rectangles labeled “Embedding Layer”, “Recurrent Layer 1”, “Dropout Layer”, “Recurrent Layer 2”, and “Dense Layer”. The third layer is the output layer, which is represented by a blue rectangle labeled “Output Layer”. The layers are connected by blue arrows, indicating the flow of data through the network.

3.2: LSTM:

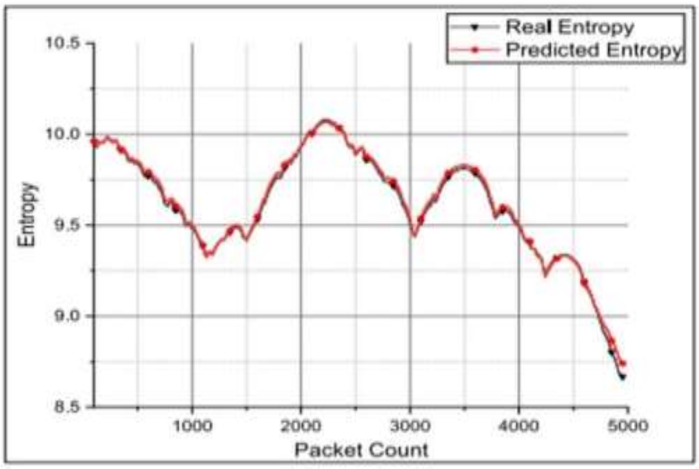

Figure 1: Background entropy filter using LSTM.

Fig. 1 shows the real entropy data and its LSTM-predicted data. We can see irregular but legal serrations in the real blue entropy line and the highly-coincident predicted red line. We let the LSTM prediction model continuously predict the future entropy with a input.

3.3: SDN and Algorithm flowchart

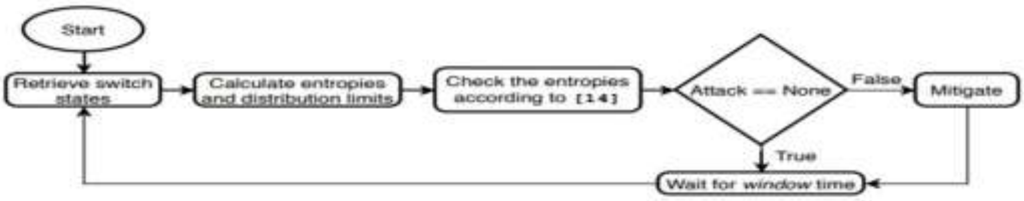

Figure 1: the flow chart of the entropy-based algorithm

3.4: Honey pots and ML Algorithm

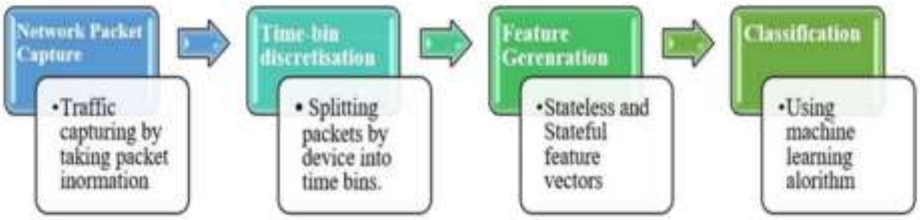

Figure 1. Process flow for machine learning based DDoS detection

The feature extraction process is responsible for generating stateless and stateful features for each packet depending upon the IoT device behaviour. Stateless features are lightweight features derived from flow independent characteristics of each sent packet that is they are actually generated without splitting the incoming traffic stream by IP Address.

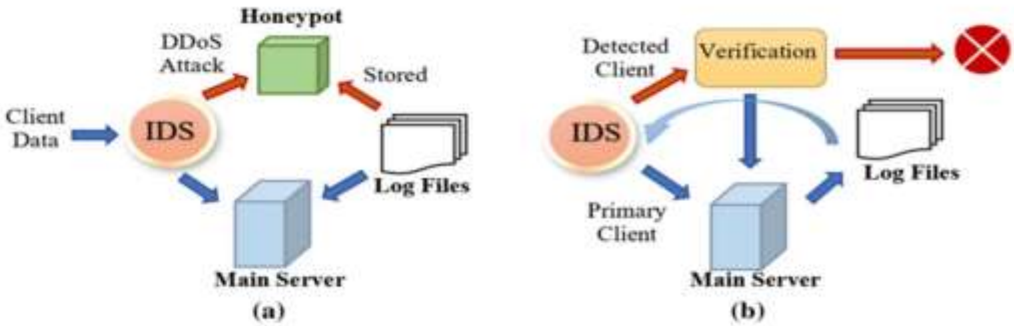

Figure 2. a. Honeypot is used to collect into log files in case of DDoS attack. **b. Log files are used for matching attack features against further suspected intrusions**

In a honeypot model, a decoy system is used to avoid the whole IoT system from being shut down due to a DoS attack. Honeypots are a type of trap that can be used to interact with potential attackers to deflect, detect, or prevent such attacks and ensure continuous availability of service123.

4.RESULTS AND DISCUSSION

4.1: DDoS Detection algorithm by Entropy based solution.

window - θ	Detection Rate	False Positive Rate	Mean (ms)	Standard Deviation (ms)
3 - 1	100%	90%	16.32	2.17
3 - 2	100%	20%	20.20	6.38
3 - 3	90%	20% *	19.06	9.27
5 -1	100%	70%	19.09	8.30
5 - 2	100%	70%	20.96	7.04
5 - 3	100%	20% *	19.30	3.66
10 - 1	100%	60%	22.82	10.38
10 - 2	100%	60%	21.41	7.25
10 - 3	100%	20% *	21.27	8.56
20 - 1	100%	80%	26.93	13.45
20 - 2	100%	40%	24.03	14.14
20 - 3	80%	20% *	26.98	10.89

TABLE 1. Results of experimentation with IoT traffic for different window and θ values

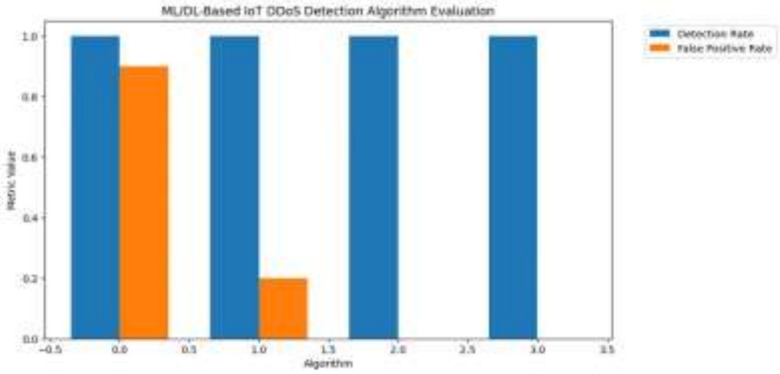

Figure 2.Detection rate and false positive rate using ddos detection algorithm

4.2 J48, RANDOM FOREST, SVM, KNN For accuracy and precision.

TABLE1: J48, RANDOM FOREST, SVM, KNN comparision

Algorithm	Recall	F-Score	Kappa Statistic	Root mean squared error	Training Time (Sec)	Testing Time (Sec)	Sensitivity	Specificity	Precision	Accuracy
J48	1	1	1	0.0001	17.43	3.03	1	1	1	1
RF	1	1	1	0.0914	171.11	5.19	1	1	1	1
SVM	1	1	1	0	168.59	1.97	1	1	1	1
K-NN	1	1	1	0	0.13	15957.7	1	1	1	1

4.3 Using QuinDC performance by TFOR.

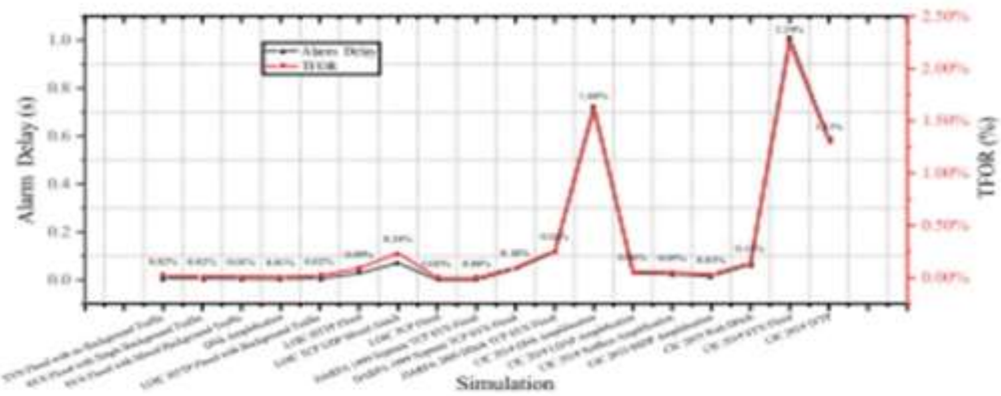

Fig 1. TFOR of different DDoS attacks using QuinDC.

The TPR of modern DDoS detection is 100%, and the TPR of attacking packets detection is over 90%, with a low FPR of less than 3%. Furthermore, we redesigned another indicator of Temporal False Omission Rate to evaluate the time performance of response.

5.CONCLUSION

Distributed Denial of Service (DDoS) attacks on Internet of Things (IoT) devices represent a growing and concerning threat in the digital landscape. These attacks exploit the interconnected nature of IoT devices, leveraging their collective computing power to overwhelm and incapacitate targeted systems. The consequences of such attacks are farreaching, extending beyond mere disruption to potentially compromising data integrity, privacy, and even physical safety in critical sectors. As the number of IoT devices continues to proliferate across various industries, the attack surface for potential DDoS threats expands exponentially. The lack of robust security measures in many IoT devices leaves them vulnerable to exploitation, making them unwitting participants in large-scale botnets orchestrated by malicious actors. This not only disrupts the normal functioning of these devices but also poses serious challenges to the overall reliability and resilience of the connected infrastructure. Mitigating the impact of DDoS attacks on IoT devices requires a multi-faceted approach. Strengthening security protocols, implementing regular updates and patches, and fostering collaboration among stakeholders are crucial steps. Additionally, the development of industry-wide standards for IoT security is imperative to ensure a unified and effective defense against these threats. As technology continues to advance, it is essential for manufacturers, policymakers, and cybersecurity experts to work in tandem to address the evolving landscape of cyber threats. Only through proactive measures, robust security practices, and a collective commitment to safeguarding IoT devices can we hope to thwart the growing menace of DDoS attacks on these interconnected systems.

6. REFERENCES

[1] Zeeshan , M., Riaz, Q., Bilal, M. A., Shahzad, M. K., Jabeen, H., Haider, S. A., & Rahim, A. (2021). Protocol-based deep intrusion detection for dos and ddos attacks using unsw-nb15 and bot-iot data-sets. IEEE Access, 10, 2269-2283.

[2] Rahman, O., Quraishi, M. A. G., & Lung, C. H. (2019, July). DDoS attacks detection and mitigation in SDN using machine learning. In 2019 IEEE world congress on services (SERVICES) (Vol. 2642, pp. 184-189). IEEE.

[3] Li, J., Liu, M., Xue, Z., Fan, X., & He, X. (2020). RTVD: A real-time volumetric detection scheme for DDoS in the Internet of Things. IEEE Access, 8, 36191-36201.

[4] Galeano-Brajones, J., Carmona-Murillo, J., Valenzuela-Valdés, J. F., & Luna-Valero, F. (2020). Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: An experimental approach. Sensors, 20(3), 816.

[5] Vishwakarma, R., & Jain, A. K. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommunication systems, 73(1), 3-25.