Distributed Denial of Service (DDoS) Detection and Mitigation

Razan El Mais
Department of Electrical & Computer Engineering
American University of Beirut
Beirut, Lebanon
rre30@mail.aub.edu

Kevin Kfoury
Department of Electrical & Computer Engineering
American University of Beirut
Beirut, Lebanon
kjk09@mail.aub.edu

Maurice Haddad
Department of Electrical & Computer Engineering
American University of Beirut
Beirut, Lebanon
mmh152@mail.aub.edu

***Abstract*—In recent years, internet of things (IoT) networks are gaining more popularity as a mean for exchanging information through connected devices over the internet. One of the main attacks in these networks is the devastating Distributed Denial of Service (DDoS) attack, which is the act of targeting system resources to either overwhelm it or causes crashing. Many studies addressed different types of DDoS attacks in the literature, proposing promising detection and mitigation mechanisms. In this paper, we propose a hybrid DDoS detection and mitigation approach by adopting two threshold-based statistical methods namely cosine similarity and counter-based, blocking the malicious packet to reduce the impact. In fact, based on our evaluation results, our approach reached the highest accuracy and F1-score compared to other methods.**

***Index Terms*—Internet fo Things, Denial of Service, Routing Protocol for Low-Power and Lossy Networks, Software defined Network, Intrusion Detection System**

I. Introduction

The rapid rise in internet usage with the fast emerging of internet technologies in our daily lives is a notable global trend. By 2024, approximately 68% of the world's population are estimated to be using the internet with a significant increase from 53% in 2019 [1]. This proliferation of the connected devices, over the internet, introduced a great cyber security challenge for all individuals and enterprises through maximizing the number of attacks on users that impact their information exchange and disclose their sensitive data. The evolution of Cyber threats types are becoming more sophisticated and severe than ever before, compromising one or more of the CIA triad principles that guarantee the security of these IoT networks [2].

DDoS is one of the most destructive attacks that bring massive threats to the connected devices over the network. This attack is intended to interrupt normal functioning of the system by flooding the server with enormous number of malicious requests, so that the system crashes or is overwhelmed. Over the decades, a number of studies addressed this attack's defense, which will be shown in Section 2, but it is still a challenging task that suffers from major gaps, influencing its accuracy and efficiency. For this reason, our objective is to develop an approach that can detect and mitigate DDoS attacks targeting IoT devices effectively by leveraging hybrid threshold-based methods namely cosine similarity and counter-based approaches to ensure node authentication.

The remnant of this paper will be organized as follows: Section 2 provides detailed literature review similar for in-use approaches that call for the existence of our system. System specifications, architecture and simulation are illustrated in the third section. Then, section 4 will presents the results with discussion. Finally, section 4 concludes the findings, along with suggestions for future work and potential enhancements.

II. Related Work

In IoT networks, DDoS attacks are increasing high in fact which calls for intensive attention on the ongoing research in detecting and mitigating them. Many diverse techniques were suggested and proposed in the academia that will be discussed.

An effective novel trust-based solution leveraging fuzzy techniques was proposed in [3] to mitigate DDoS attacks in the RPL protocol, addressing Hello flooding and version number modification attacks. Simulations in Cooja and Contiki OS showed full mitigation of version number modification and partial mitigation of Hello flooding. Despite its effectiveness, challenges like whitewashing and bootstrapping remain.

In [4], the authors proposed DNSguard, a two-level mitigation system for DNS flooding DDoS attacks in IoT smart homes, using MUD compliance to authorize devices and monitor DNS traffic rates within a DQPS limit. It effectively reduces response time, CPU usage, and improves throughput. However, its reliance on MUD limits compatibility with certain IoT devices and may introduce latency with increased device connections.

The authors in [5] proposed an SDx-based framework for SD-IoT, separating the control plane from the data plane with components including a controller pool, data layer switches, and IoT devices. It uses cosine similarity of packet-in

message rates to detect and block DDoS attacks at the source. Simulations demonstrated improved IoT security by effectively identifying and quickly mitigating malicious devices. The study in [6] examines how SDN enhances IoT security against DDoS attacks by employing packet discarding, port blocking, IP modification, and traffic redirection techniques. Challenges include IoT resource constraints, data flow issues, and spoofing attempts. Simulations show SDN's improved security but highlight the need to balance legitimate traffic and enhance packet inspection for IoT-specific requirements.

In [7], the authors presented a new firewall model using queueing theory to analyze network behavior with a single window and limited queue for packets arriving via a Poisson process. The approach supports multi-tiered firewalls and enhances concurrent service handling in IoT networks. While it improves response times, the single-window limitation poses challenges under high-traffic conditions.

An effective survivability model for IoT devices based on a semi-Markov process was proposed in [8] to assess resource exhaustion from DDoS attacks. Using statistical methods like the Mann-Kendall Test and Theil-Sen procedure, the model identifies resource depletion trends to schedule maintenance proactively. This approach serves as an extremely beneficial mindset as it reduces system downtime and costly failures by enabling timely preventative actions.

The authors of [9] proposed an FPGA-based solution for detecting and mitigating DDoS attacks using a Packet Validation Unit (PVU) and Intrusion Detection Unit (IDU) to validate packet attributes like IP, TTL, and payload. The FPGA, acting as an IoT router, is efficient with low resource overhead, relying on bitwise operations to detect attacks. However, its simplistic checks may be bypassed by sophisticated DDoS attacks that mimic legitimate traffic.

In [10], Bhayo et al. introduced the Counter-Based DDoS Attack Detection (C-DAD) framework for SD-IoT networks, utilizing SDN principles to detect anomalies using metrics like packet payload and traffic load. Tested on Cooja with Contiki OS, the framework showed high detection efficiency with minimal resource usage. It effectively mitigates DDoS attacks while maintaining normal network performance, making it ideal for resource-constrained IoT devices.

In [11], Doshi et al. proposed a robust anomaly-based IDS capable of detecting and mitigating stealthy DDoS attacks in IoT networks. The IDS employs an ODIT mechanism to identify low-rate, widely distributed DDoS traffic often missed by traditional filters. Unlike signature-based methods, it adapts to anomalies without relying on predefined patterns, addressing challenges like high dimensionality and unknown attack types. Simulation demonstrate its real-time detection and mitigation effectiveness with minimal disruption. However, further work is needed to enhance adaptability for large-scale IoT networks.

III. Proposed Hybrid Approach

Although these current methods showed a fair and consistent defense performance against DDoS attacks, they still suffer from some limitations that hinder their success and full coverage. Therefore, it is effective to spot the strengths and the shortcomings of each strategy and move forward for developing more sophisticated and enhanced one. Our suggested approach will be a hybrid two-line defense mechanism where cosine similarity along with counter-based methods will be applied to detect and mitigate such attack in SD-IoT networks.

A. Implementation

The proposed approach is threshold-based comparison with the computed statistics measures known as statistical-based analysis. This type of analysis is considered as one of the most vigorous detection methods for DDoS [12]. We used hybrid statistical measures to differentiate between normal and abnormal traffic, ensuring more robust, effective and reliable detection. Both cosine similarity pattern recognition and counter-based threshold analysis are combined to play valuable and benefitable complementary roles in such an accurate detection model.

1) Cosine Similarity for pattern recognition: evaluates the similarity between vectors representing network traffic, comparing with baseline legitimate profiles then calculating dot product and normalizing by their weights. The output value is compared with threshold value to classify the tested traffic and determine anomalies indicative of DDoS. If the value is less than the threshold, DDoS attack is detected. Else, the traffic is likely to be normal. The selection of threshold is critical for ensuring efficient performance. thus, a value of 0.7 is selected to be the best value referring to the discussion made by work [5]. We obtained the cosine similarity of two vectors by the following equation:
   The cosine similarity between two vectors $\mathbf{A}$ and $\mathbf{B}$ is given by:
$$\text{cosine similarity} = \cos(\theta) = \frac{\mathbf{A} \cdot \mathbf{B}}{\|\mathbf{A}\|\|\mathbf{B}\|}$$
   Where:
   - $\mathbf{A} \cdot \mathbf{B}$ is the dot product of the vectors $\mathbf{A}$ and $\mathbf{B}$,
   - $\|\mathbf{A}\|$ and $\|\mathbf{B}\|$ are the magnitudes (Euclidean norms) of $\mathbf{A}$ and $\mathbf{B}$.
2) Counter-based threshold analysis: involves maintaining counters for specific metrics as number of packets per unit time. Then comparing this count with historical threshold value of expected normal behavior, Sudden spikes in counters beyond these thresholds are flagged as potential DDoS activity.

The above two strategies block packets during anomalies or DDoS attack patterns, mitigating their impact in SD-IoT networks. Our proposed hybrid approach uses two parallel statistical analyses with separate threshold detection, combining results through an AND voting operation for the final decision. Figure 1 represents the workflow of this procedure.

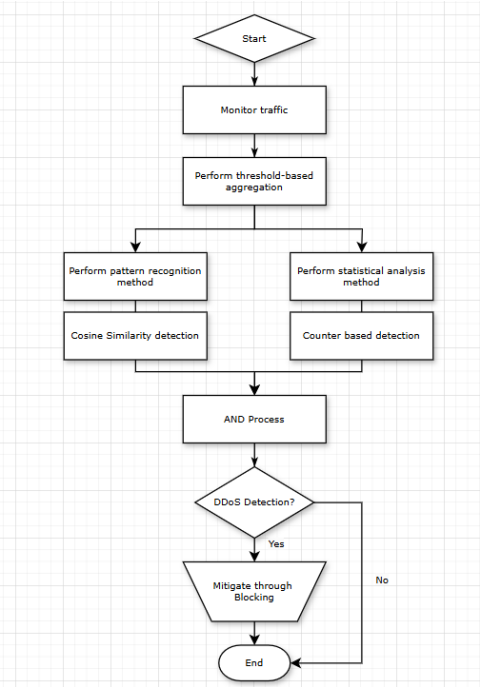

Fig. 1: Workflow of the proposed hybrid approach

B. DDoS Attacks: UDP Flooding

Our approach will be addressing only UDP flooding DDoS attck for being a simplified demonstration of DDoS by effectively demonstrating the core principle of a DDoS attack: overwhelming a target system with excessive traffic, leading to resource exhaustion or service unavailability. Adding to this, the prevalence in real-world attacks through exploiting its stateless nature, making it easy to overwhelm server with distinctive high volume traffic. Also, the common fact of the UDP protocol being widely used in many applications like streaming, VoIP and DNS.

C. Simulation

To simulate the proposed work, we set up a virtual network using Cooja network simulator for low-power IoT devices, configuring devices to represent regular IoT traffic. This process involves the following steps:

1) Environment Setup:Cooja simulator is used in Ubuntu virtual machine.
2) Script Development: IPv6, UDP and the lightweight RPL protocol were utilized suiting well for low-constrained IoT devices.
3) Defense Integration: Defense measures deployed on the centralized SDN-Controller device that separates the network's logic from the forwarding nodes. This includes monitoring traffic and implementing both the cosine similarity algorithm and the counter-based approach to efficiently detect DDoS attacks, blocking any suspicious device's packet.

The network topology is shown in figure 2. Figure 3 shows how the controller block the node when detected as an attack by enclosing the malicious node in red circles.

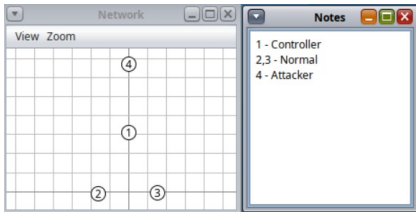

Fig. 2: Network Topology of the proposed hybrid approach

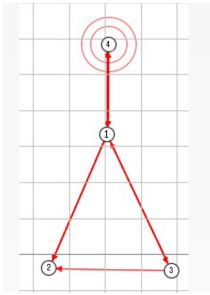

Fig. 3: Blocking detected node packet

IV. Results and Evaluation

The fusion of the two threshold-based measures are used in our study and the results are compared with each of the two baseline measure methods namely Cosine similarity detection and Counter-based detection Algorithms.Two metrics were chosen for this comparison: Accuracy and F1-Score. Notably, the F1-Score encapsulates both precision and recall, providing a comprehensive measure of performance. Table I shows the records of each performance metric for each approach highlighting the out performance of our proposed approach on the others. This justifies the remarkable enhancements of hybridization of statistical methods.

Method	Accuracy (%)	F1-Score (%)
Cosine Similarity	33.33	50
Counter-based	78.47	87.93
Our hybrid approach	100	100

TABLE I: Performance metrics for different methods.

V. CONCLUSION

This paper proposes an enhanced DDoS detection and mitigation strategy for IoT networks, integrating two primary measures as a two-layer defense mechanism. This approach strengthens the security of IoT devices, reducing the likelihood of misclassified malicious traffic. It ensures robust authentication while delivering highly accurate and efficient results. Future improvements could involve incorporating more statistical methods and addressing diverse types of DDoS attacks.

References

[1] DataReportal, *Internet use in 2024: Global digital insights*, Accessed: 2024-12-05, 2024. [Online]. Available: https://datareportal.com.

[2] M. Hassan, K. Metwally, and M. A. Elshafey, "Zf-ddos: An enhanced statistical-based ddos detection approach using integrated z-score and fast-entropy measures," in *2024 6th International Conference on Computing and Informatics (ICCI)*, IEEE, 2024, pp. 145–152.

[3] F. Azzedin, "Mitigating denial of service attacks in rpl-based iot environments: Trust-based approach," *IEEE Access*, vol. 11, pp. 129 077–129 089, 2023.

[4] S. Datta, A. Kotha, K. Manohar, and U Venkanna, "Dnsguard: A raspberry pi-based ddos mitigation on dns server in iot networks," *IEEE Networking Letters*, vol. 4, no. 4, pp. 212–216, 2022.

[5] D. Yin, L. Zhang, and K. Yang, "A ddos attack detection and mitigation with software-defined internet of things framework," *IEEE Access*, vol. 6, pp. 24 694–24 705, 2018.

[6] F. A. Munmun and M. Paul, "Challenges of ddos attack mitigation in iot devices by software defined networking (sdn)," in *2021 International Conference on Science & Contemporary Technologies (ICSCT)*, IEEE, 2021, pp. 1–5.

[7] V. S. Stuma and T. E. Mathonsi, "A security algorithm to prevent denial of service attacks in the internet of things devices," in *2024 International Conference on Electrical, Computer and Energy Technologies (ICECET*, 2024, pp. 1–6. DOI: 10.1109/ICECET61485.2024.10698594.

[8] R. Pietrantuono, M. Ficco, and F. Palmieri, "Survivability analysis of iot systems under resource exhausting attacks," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 3277–3288, 2023. DOI: 10.1109/TIFS.2023.3278449.

[9] M. Sanlı, "Detection and mitigation of denial of service attacks in internet of things networks," *Arabian Journal for Science and Engineering*, pp. 1–11, 2024.

[10] J. Bhayo, S. Hameed, and S. A. Shah, "An efficient counter-based ddos attack detection framework leveraging software defined iot (sd-iot)," *IEEE Access*, vol. 8, pp. 221 612–221 631, 2020.

[11] K. Doshi, Y. Yilmaz, and S. Uludag, "Timely detection and mitigation of stealthy ddos attacks via iot networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2164–2176, 2021.

[12] S. Batool, F. Zeeshan Khan, S. Qaiser Ali Shah, *et al.*, "[retracted] lightweight statistical approach towards tcp syn flood ddos attack detection and mitigation in sdn environment," *Security and Communication Networks*, vol. 2022, no. 1, p. 2 593 672, 2022.