Machine-Learning Detection of DDoS Attacks

Đào Văn Hiếu
Thai Nguyen University of Information and Communication Technology
Thai Nguyen University, Thai Nguyen, Vietnam
student636@ictu.edu.vn

***Abstract*—This undergraduate thesis investigates machine-learning detection of distributed denial-of-service attacks. Network intrusion detection requires labelled traffic and comparison of models across attack types. The student surveys DDoS traffic and public datasets, evaluates four machine-learning algorithms on the CIC-DDoS-2019 dataset, and compares per-attack classification outcomes. The thesis reports that Random Forest performed best among the tested algorithms on its dataset and presents accuracy comparisons by attack category. These are source-reported results within its selected experimental setup. The study does not establish performance on live institutional traffic or newly collected attack streams. The author identifies dataset expansion and more realistic traffic capture as future work. The contribution is a documented student study or prototype whose stated scope can guide further testing.**

***Index Terms*—DDoS detection, machine learning, Random Forest, CIC-DDoS-2019**

I. Introduction

Network intrusion detection requires labelled traffic and comparison of models across attack types. This thesis investigates machine-learning detection of distributed denial-of-service attacks. It begins from a practical engineering need and explains the technologies and workflow chosen for the case. The objective is to document a student implementation or comparative investigation, together with the evidence available in the manuscript. Broader operational or economic effects require separate measurements and are not assumed from the existence of a prototype [1]. Earlier ICTU student work on related designs is included here for context [2], [3]. Related published studies provide context for the subject and methods [4], [5], [6], [7], [8], [9], [10]. These contextual works were selected for this English summary; they are not asserted to appear in the original thesis bibliography.

II. Methods

The student surveys DDoS traffic and public datasets, evaluates four machine-learning algorithms on the CIC-DDoS-2019 dataset, and compares per-attack classification outcomes. The source is summarized through its stated design, implementation material, examples, and conclusion. Features shown in the manuscript are distinguished from proposals for later development. This review does not add a new experiment, fill missing measurements with estimates, or treat a planned capability as an observed result. The source thesis remains the provenance for the reported work [1].

Supervisor: Vũ Việt Dũng, Thai Nguyen University of Information and Communication Technology (vvdung@ictu.edu.vn).

III. Results

The thesis reports that Random Forest performed best among the tested algorithms on its dataset and presents accuracy comparisons by attack category. These are source-reported results within its selected experimental setup. The report's screens, configurations, examples, or measurements constitute the evidence for this summary. A capability described only as a design intention is not counted as a validated operational outcome. No additional performance, adoption, financial, or safety figure has been introduced here. The result is interpreted within the scope of the student's documented setup [1].

IV. Discussion

The study does not establish performance on live institutional traffic or newly collected attack streams. The author identifies dataset expansion and more realistic traffic capture as future work. Further work could document an independent test split, compare model behavior on later traffic, and report false-positive and throughput measures before operational use. These limitations affect how the evidence should be read. The current manuscript can support understanding of the design and reported demonstration, while independent tests would be needed for stronger claims. Any later deployment should document its environment and separate observed outcomes from intended benefits [1].

V. Conclusion

The thesis documents machine-learning detection of distributed denial-of-service attacks. The thesis reports that Random Forest performed best among the tested algorithms on its dataset and presents accuracy comparisons by attack category. These are source-reported results within its selected experimental setup. The study does not establish performance on live institutional traffic or newly collected attack streams. The author identifies dataset expansion and more realistic traffic capture as future work. Further work could document an independent test split, compare model behavior on later traffic, and report false-positive and throughput measures before operational use. Accordingly, the present contribution is a source-grounded account of the student work and its tested or illustrated scope. Claims about broader effectiveness should be assessed in later work using explicit evaluation conditions [1].

References

[1] Đào Văn Hiếu, ”Machine-Learning Detection of DDoS Attacks,” internal undergraduate thesis (original in Vietnamese), Thai Nguyen University of Information and Communication Technology, 2024.

[2] ICTU Student 102, ”Development of an Intrusion Detection System Based on Data Mining Techniques,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[3] ICTU Student 129, ”Construction of a Network Security System for the Commercial Bank of Vietnam Hanoi Branch,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[4] Jiangtao Pei et al., ”A DDoS Attack Detection Method Based on Machine Learning,” Journal of Physics: Conference Series, 2019. doi:10.1088/1742-6596/1237/3/032040.

[5] Tiffany Tu, ”DDoS Analysis and Detection with Machine Learning Algorithms,” Scholarly Review Journal, 2023. doi:10.70121/001c.121699.

[6] Doan Trung Son et al., ”Machine learning approach detects DDoS attacks,” Journal of Science and Technology on Information security, 2022. doi:10.54654/isj.v1i15.850.

[7] Yeefong Wu, ”DDos attack detection method based on machine learning,” Applied and Computational Engineering, 2023. doi:10.54254/2755-2721/18/20230968.

[8] Mohammad Najafimehr et al., ”DDoS attacks and machine□learning□based detection methods: A survey and taxonomy,” Engineering Reports, 2023. doi:10.1002/eng2.12697.

[9] Abdul Raoof Wani et al., ”Machine Learning Solutions for Analysis and Detection of DDoS Attacks in Cloud Computing Environment,” International Journal of Engineering and Advanced Technology, 2020. doi:10.35940/ijeat.b3402.029320.

[10] Kishore Babu Dasari et al., ”Detection of DDoS Attacks Using Machine Learning Classification Algorithms,” International Journal of Computer Network and Information Security, 2022. doi:10.5815/ijcnis.2022.06.07.