Chapter 6
Holistic View on Detecting DDoS Attacks Using Machine Learning

Eduardo Barros
https://orcid.org/0000-0002-5309-1394
Instituto Superior Técnico, Portugal

Victor Lobo
NOVA Information Management School (NOVA-IMS), NOVA University Lisbon, Portugal & Naval Academy, Portugal

Anacleto Correia
https://orcid.org/0000-0002-7248-4310
CINAV, Portuguese Naval Academy, Portugal

ABSTRACT

Distributed denial of service (DDoS) attacks are an enormous threat, mainly because of the extension they can reach, the ease of deployment, the losses that it can cause, and the effort it can take to detect and stop this type of attack. Machine learning techniques have been and are widely used to prevent DDoS attacks. As a matter of fact, many gigantic intrusion detection systems (IDS) have been proudly utilising machine learning techniques to help the conventional signature detection system by adding another layer of "intelligent" thinking. This chapter provides a context of the techniques used for detecting DDoS attacks using machine learning, and in demonstrating why the merge of these concepts have huge potential for the defence of a given system. To that matter, some studies that use machine learning approaches for DDoS detection are analysed. Finally, this chapter provides a high-level view of the types of DDoS attacks that are considered a threat, the machine learning approaches to detect these attacks, and why these approaches are cohesive.

DOI: 10.4018/978-1-7998-9430-8.ch006

Copyright © 2022, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Nowadays, most enterprises depend on the use of technologies, particularly, networked technologies. Not only is this a great opportunity for organisations to leverage and enhance their business, but also for threat agents to achieve their goals by damaging these systems. In order to ensure the security of network services it is essential that, at the very least, the 3 pillars of information security (CIA triad) - integrity, confidentiality and availability -, are met.

This chapter will focus on the *availability* pillar of the CIA triad and its biggest threat, the Distributed Denial of Service (DDoS) attacks. The way this attack operates is by flooding the target with malicious traffic, depleting its bandwidth and/or computing resources in order to create total unavailability or some disruption of a network asset. One of the hardest tasks for an Intrusion Detection System (IDS) is to mitigate a DDoS. This type of attack has some peculiarities, among other characteristics described in the next section: (i) the DDoS might be originate from thousands of *legitimate* devices; (ii) the requests may not contain any malicious content; (iii) the attacker can exploit a vulnerability in the attacked service but also in an external service to conduct the attack.

Unlike the vast majority of attacks, where only one malicious request is needed for it to be successful, a DDoS generally requires multiple requests, so, it might be possible to identify patterns shared by malicious packets. This characteristic is key and allows the use of machine learning for the purposes of identifying recurrent patterns in a DDoS. The aim of this chapter is to demonstrate that the use of machine learning for DDoS detection has great potentialities, but it is also intended to demonstrate how this can be done, introducing important concepts for the creation of a model capable of predicting DDoS requests.

To accomplish our propose, this chapter was designed as follows: the *Background* section is intended to provide a context to this subject by explaining how modern DDoS attacks work, to briefly introduce what machine learning is, and how it can be applied to detect DDoS attacks. In *Literature Review* section, in order to have an overview of what is currently being done regarding this matter, some studies that use machine learning approaches for DDoS detection are surveyed. The *Results Disussion* section, summarise and discuss the details and procedures of the surveyed articles such as: the types of DDoS attacks used, the machine learning approaches to detect these attacks, and why these approaches are cohesive. Also in this section, we present a high-level detection model based on machine learning that we consider effective. Finally, The *Conclusion* section makes a retrospective of the whole chapter, and draw conclusions about the use of machine learning for DDoS attack detection and the role it is going to play out in the future.

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/holistic-view-on-detecting-ddos-attacks-using-machine-learning/311374

Related Content

Intelligent System for Credit Risk Management in Financial Institutions
Philip Sarfo-Manu, Gifty Siawand Peter Appiahene (2019). *International Journal of Artificial Intelligence and Machine Learning (pp. 57-67).*
www.irma-international.org/article/intelligent-system-for-credit-risk-management-in-financial-institutions/238128

Usage of the Basic Facebook Features as Befitting Marketing Tools
Fahima Khanam, Muhammad Omar Al-Zadidand Mahmud Ullah (2023). *Encyclopedia of Data Science and Machine Learning (pp. 2918-2934).*
www.irma-international.org/chapter/usage-of-the-basic-facebook-features-as-befitting-marketing-tools/317724

The Role and Applications of Machine Learning in Future Self-Organizing Cellular Networks
Paulo Valente Klaine, Oluwakayode Onireti, Richard Demo Souzaand Muhammad Ali Imran (2022). *Research Anthology on Machine Learning Techniques, Methods, and Applications (pp. 1494-1516).*
www.irma-international.org/chapter/the-role-and-applications-of-machine-learning-in-future-self-organizing-cellular-networks/307523

Efficient Closure Operators for FCA-Based Classification
Nida Meddouriand Mondher Maddouri (2020). *International Journal of Artificial Intelligence and Machine Learning (pp. 79-98).*
www.irma-international.org/article/efficient-closure-operators-for-fca-based-classification/257273

Autonomous Last Mile Shuttle ISEAUTO for Education and Research
Raivo Sell, Mairo Leier, Anton Rassõlkinand Juhan-Peep Ernits (2020). *International Journal of Artificial Intelligence and Machine Learning (pp. 18-30).*
www.irma-international.org/article/autonomous-last-mile-shuttle-iseauto-for-education-and-research/249250