15

28

JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 19 2020

AN EFFICIENT DISTRIBUTED DENIAL OF SERVICE ATTACK DETECTION APPROACH BASED ON SET OF CLASSIFICATION ALGORITHMS USING SPARK

M. Premkumar[1], TVP. Sundararajan[2], S. Shanmugapriya[3], V. Shanmugapriya[4], J. Sowmiya[5], T. Vinitha[6]

[1]Assistant Professor, Department of ECE, SSM Institute of Engineering and Technology, Dindigul, India
[2]Professor, Department of ECE, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India
[3,4,5,6]UG Scholars, Department of ECE, SSM Institute of Engineering and Technology, Dindigul, India

Email: prem53kumar@gmail.com

Received: 14 April 2020 Revised and Accepted: 8 August 2020

ABSTRACT: Distributed Denial of Service (DDOS) attacks pose a serious privacy challenge to conventional or cloud computing services being made public. Innumerable DDOS attacks, waged during the last decade against different agencies, had a major impact on both producers and users. Through integrating classification algorithms with distributed computation, numerous analysts have seeks to resolve the security concern of DDOS attacks. Our formulations are therefore rigid in terms of the classification algorithms used. However, modern DDOS threats have been so dynamic and sophisticated that they can bypass the monitoring programme, while rendering it challenging to spot static solutions. We suggest a versatile intrusion detection mechanism centered on three key aspects in this paper: classification algorithms, a distributed method, and a fuzzy logic System. To efficiently pick an algorithm from a set of prepared classification algorithms that diagnose various DDOS trends, our model uses fuzzy logic. We use as candidate algorithms Logistic Regression, Naive Bayes, Gradient Boosting Decision Tree, Random Forest and Hybrid IDS from among the other candidate classification algorithms. We examined the reliability and delays of classification algorithms, and reviewed the fuzzy logic model. We have analyzed the feasibility of the distributed network and its consequence on the delay in classification algorithms. The results reveal a trade-off between the accuracy level of the classification algorithms used and their delays.

KEYWORDS: DDoS Attack, DDoS Detection, Machine learning, Classification algorithms, hybrid IDS

I. INTRODUCTION

Distributed Denial of Service (DDOS) is a security breach that does not render resources accessible, or just partial. The primary priority of a DDOS attack is to expel the network with a high volume of traffic, thereby disputing legitimate users access to services. There have been countless DDOS attacks against Various entities over the last decade have culminated over depletion of income as well as rising security costs System Accessibility [1].DDOS attacks have been so complex and multifaceted nowadays in that they deployed in a multitude of ways, rendering it tough to identify static solutions [2]. Lots of studies intended at detecting and preventing DDOS attacks incorporating classification algorithms [3–7] and distributed systems [8–10] have been undertaken. However, existing research has many problems, including the performance of the detection system, that is, the success in detecting a DDoS attack, computation cost of detection, as well as the ability to deal with large amounts of data.Therefore, a new method is required for dynamic tracking of DDOS attacks, for effective handling of dynamic DDOS attack trends and massive quantity of data. No DDOS detection method relies on the power of integrating N classification algorithms, distributed system strategy and a fuzzy logic approach to the best of our understanding, and also able to dynamically adjust itself. Within this work, by integrating these guiding criteria, we recommend a reactive DDOS attack detection method: classification algorithms that are operated in a distributed network and driven by a fuzzy logic system. The innovative aspect of this work is the convergence of the three conceptions of classification algorithms, distributed systems, and a fuzzy logic method. Although our process serves N classification algorithms, we included five classification algorithms, namely Logistic Regression, Naive Bayes, Gradient Boosting Decision Tree, Random Forest and Hybrid IDS, for evaluation purposes.Classification algorithms use to recognize the retrieved traffic packets. Choosing these classification algorithms based on a variety of criteria: classification precision, model training period, and classification feature disparities. On the other flip side, the distributed system is based on the framework of Apache Spark and the Hadoop Distributed File System (HDFS), in which they can be provisioned