Detection of Distributed Denial of Service (DDoS) with Linear Support Vector Machine

By

Yisa Rhoda Nnaba and Morufu Olalere

Abstract

One of the major security challenges in the current Internet, is the distributed-denial-of service (DDoS) attack. This attack always attempts to stop the people from serving authorize users thereby causing a serious danger to the Internet operation. Many companies and organizations that are connected to internet have been the victims of Distributed Denial of Service (DDoS) attacks; this attack is a serious threat to any network server. Consequently, many researchers have proposed different techniques for the detection of this attack. Meanwhile, achieving high accuracy and low False Positive Rate (FPR) with high True Positive Rate (TPR) remains issue in this area of research. However, this study proposed machine learning based detection system for DDoS attack. Linear Support Vector Machine based DDoS attack detection system is presented in this study. For experimentation purpose, NSL-KDD dataset was used to run our experiment in MatLab environment. The performance of the Linear Support Vector Machine was evaluated using previously used performance metrics in this area of research. These metrics are Accuracy, TPR and FPR. Our experimental results revealed high accuracy of 99.83%, high TPR of 99.85% with a low FPR of 0.0019.