Building a DDoS attack detection system using Suricata combined with a machine learning model.

Ma Van Dao

Abstract: In the context of communication networks becoming increasingly important, protecting systems against DDoS (Distributed Denial of Service) attacks has become an urgent need. This project aims to build and deploy a DDoS attack detection system using Suricata, combined with machine learning models to enhance the accuracy and performance of attack identification. The research methodology includes evaluating and selecting suitable machine learning algorithms, integrating them into Suricata via API, and conducting practical tests on sample data. The expected results will provide an effective solution for network security protection and make a significant contribution to the research field of DDoS attack detection.

Keywords: Suricata, Machine learning model, DDoS attack detection, Network security, DDoS attack