QOZEEM ADESHINA

STUDENT, MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

EVALUATION AND DEVELOPMENT OF MACHINE LEARNING BASED ALGORITHMS FOR PREDICTING DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)

The IT space is growing in all aspects ranging from bandwidth, storage, processing speed, machine learning and data analysis. This growth has consequently led to more cyber threat and attacks which now requires innovative and predictive security approach that uses cutting-edge technologies in order to fight the menace. The patterns of the cyber threats will be observed so that proper analysis from different sets of data will be used to develop a model that will depend on the available data. Distributed Denial of Service is one of the most common threats and attacks that is ravaging computing devices on the internet.

This research evaluates the performance of different machine learning based classifiers to detect DDoS attacks before it eventually happens. We utilize the benchmark KDD Cup 1999 DDoS attack data in our experiment. The data consists of three different features: basic, content, and traffic features. We implemented three different types of feature selection techniques: filter, wrapper, and embedded methods to select important features in the context of DDoS detection. Experimental results demonstrate that domain knowledge can guide machine learning algorithms in predicting DDoS Detection. On the other end of the spectrum, feature selection techniques can help domain experts to understand the hidden important patterns and features in the intrusion system.

The proposed model learns to understand the normal network traffic so that it can detect future ICMP, TCP and UDP DDoS traffic when they arrive. Experimental results demonstrate that data-driven, intelligent, and decision-making machine learning algorithms could successfully categorize normal and DDoS traffic. This research has long standing outcomes in various fields, such as national defense, financial institutions, healthcare, other industries that urges advanced intrusion detection techniques. In future, we would like to implement deep learning algorithms to predict DDoS attack.

Research Advisor: Dr. Baidya Nath Saha