An evaluation on KNN-SVM algorithm for detection and prediction of DDoS attack

ABSTRACT

Recently, damage caused by DDoS attacks increases year by year. Along with the advancement of communication technology, this kind of attack also evolves and it has become more complicated and hard to detect using flash crowd agent, slow rate attack and also amplification attack that exploits a vulnerability in DNS server. Fast detection of the DDoS attack, quick response mechanisms and proper mitigation are a must for an organization. An investigation has been performed on DDoS attack and it analyzes the details of its phase using machine learning technique to classify the network status. In this paper, we propose a hybrid KNN-SVM method on classifying, detecting and predicting the DDoS attack. The simulation result showed that each phase of the attack scenario is partitioned well and we can detect precursors of DDoS attack as well as the attack itself.

Keyword: Distributed Denial of Services (DDoS); Machine learning classifiers; Security; Intrusion detection; Prediction; Support Vector Machine (SVM); k-nearest neighbor (KNN); KNN-SVM