Abstract

SYN Flood is one of the most common types of DDoS attacks, this attack utilizes TCP three – way handsake to establish a connection with server which has the purpose of interrupting and rejecting user packets by fulfilling very large target requests. Meanwhile, UDP Lag is an attempt to break connection between client and server. In recent years, research related using machine learning to detect DDoS attacks with different methods. The steps taken to detect SYN Flood attacks are system design, data collection, search, and data analysis.This research is closely related to test metrics such as precision, recall, and accuracy. Value of precision, recall, and accuracy is determined by the selection of the machine learning algorithm used when detecting attacks. Some literatures on SYN Flood and UDP Lag attack detection has a low accuracy value with the algorithm of choice used.With the research conducted by the author in detecting attacks by designing and building a system using 3 choices of machine learning algorithms which include ensemble Learning, logistic regression, and decision tree with the aim of increasing the effectiveness of detection , can overcome the problems that arise in the detection of SYN Flood and UDP Lag attacks in the research carried out with hope this research has achievements 100% precision, 100% recall, and 100% accuracy.

Keywords: SYN Flood, UDP Lag, machine learning, DDoS.