

ABSTRACT

Along with the increasing development and the role of the internet today, also resulted in increased type of intrusion or attacks to Internet users, like Distributed Denial of Service (DDoS). DDoS is a type of Denial of Service attack where attackers use multiple hosts simultaneously to transmit data repeatedly with the aim that the target can not use their right to access network service. Many studies related to the DDoS attack detection methods, but most studies are limited to use the algorithms that often do not provide optimal detection results when tested using various forms of different datasets. So we need a detection system that consists of several algorithms that can adapt to various forms of datasets in order to provide optimal detection results.

In this final project the system will grouping the type of attack and simultaneously labeling that attack. Grouping data using algorithms Minkowski Weighted K-means that make data group based on the similarity. Data that have been grouped will be classified and labeled using Decision Tree.

Based on Minkowski Weighted K-means algorithm adaptability in grouping the data into several clusters optimized and augmented the effectiveness of Decision Tree method in process of labeling each processed data, accuracy obtained in this research was 94.78% with 0.26% false positive rate and 99.98% detection rate. By comparison of multiple scenarios shows that the p-value for the Minkowski distance that gives the most optimal result was 2.5.

Keyword : Minkowski Weighted K-means, Decision Tree, DDoS