

ABSTRACT

In Internet, Distributed Denial of Service (DDoS) is one of many form of attack which is popular nowadays. DDoS's affect user access right by preventing user from accessing certain information, thus giving disadvantage to the user and service provider. Similar to DDoS's effect is phenomenon so-called flash crowds which is categorized as anomaly because it occurs on product launching or big news which is happened naturally due to increasing of number of access gradually.

Detecting network anomaly can be done using Intrusion Detection System (IDS). To make sure the IDS recognize latest anomaly type, IDS could be built in anomaly-based by using unsupervised learning clustering which need no database.

Algorithm used in building the IDS is K-Means algorithm which can be modified and developed in many possible way. K-Means Algorithm will be using Random Initialization and combined with Landmark Window to produce cluster which distinguish *normal* to *anomaly traffic* and will be reviewed by several parameter, Detection Rate (DR), Accuracy (ACC), and False Positive Rate (FPR).

Keywords : Network, Anomaly, Clustering, K-Means, Random Initialization, Landmark Window.