Abstract

DoS or Denial of service is an attack which make a computer or device error that disturb system network in that computer. DoS attack can be detected by using IDS method or Intrusion Detection System which can detect DoS attack. IDS will classificate every data in a network. To improve the IDS method, this research use Relevance Vector Machine algorithm to get accuration score when detecting DoS attack with Feature Selection, One-hot Encoding, and Feature Scaling. In this research the dataset we use is NSL-KDD dataset. NSL-KDD is a dataset which has been improved from its predecessor, KDDCUP'99. Based on the results of this research, the accuration score result when using 9 features is 93.27% while for 41 features the accuration score is 89.08%
Keywords: DoS, Denial of Service, Intrusion Detection System, Relevance Vector Machine, Feature Selection, One-hot Encoding, Feature Scaling, NSL-KDD, accuration