Abstract

Denial of Service (DoS) is attack where an attacker spends computer network resources. The impact of a DoS attack causes the computer not to function normally. Intrusion Detection System (IDS) serves as a detection of various types of attacks on computer networks including DoS. IDS identifies attacks based on network data classification. Non-machine learning Intrusion Detection System (IDS) methods are currently not very accurate, so the IDS method with machine learning is more accurate in detecting attacks. To address this problem, the study compares the Naïve Bayes and Probabilistic Neural Network (PNN) methods to optimally detect DoS attacks. In this study, implementations used Naïve Bayes and PNN methods in detecting DoS attacks using NSL-KDD datasets with 13 features from 41 features. The result of this study is that Naïve Bayes has higher accuracy with an accuracy value of 100% than that of PNN which only has an accuracy value of 91,93% in detecting DoS attacks.

Keywords : Computer Network Security, *Naïve Bayes*, *Probabilistic Neural Network* (PNN), *Denial of Service*.