Abstract

Intrusion Detection System (IDS) has been developed since the 1980s. Many algorithms and techniques have been proposed, both feature-traction algorithms, feature selection, and classification. Several IDS-related studies using popular classification algorithms, such as: IVM, SVM, and KNN, show that the attack detection time is still long, accuracy is still low, and the mean squared error (MSE) is still large. On the other hand LVQ algorithm is proven to recognize hiragana letter well. Nevertheless LVQ has never been used for IDS. In relation to the above, this final task study compares the popular algorithm for IDS with LVQ to get the best performance algorithm in terms of detection time, attack accuracy, and MSE. Besides, it also performs optimization study of the best algorithm parameters. The objectives of the research can be achieved by analyzing the methods of IVM, SVM, KNN, and LVQ using NSL_KDD data, mainly against the three metrics mentioned above. This research also analyzes the influence of some of the best algorithm input parameters such as Alpha and Constants to get more optimal results. Experimental results show that LVQ has the best performance with the fastest detection time compared to IVM, SVM, and KNN. LVQ's accuracy is 87.4425% and MSE 0.121775. After tuning the input parameters, the LVQ performance increased, the detection time reached eight times faster than SVM, 90.1275% accuracy, and MSE 0.0.09875.

Keywords: LVQ, Classification, IDS, NSL-KDD, attack accuracy, detection time