World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:12, No:06, 2018

# Hybrid Anomaly Detection Using Decision Tree and Support Vector Machine

**Authors :** Elham Serkani, Hossein Gharaee Garakani, Naser Mohammadzadeh, Elaheh Vaezpour

**Abstract :** Intrusion detection systems (IDS) are the main components of network security. These systems analyze the network events for intrusion detection. The design of an IDS is through the training of normal traffic data or attack. The methods of machine learning are the best ways to design IDSs. In the method presented in this article, the pruning algorithm of C5.0 decision tree is being used to reduce the features of traffic data used and training IDS by the least square vector algorithm (LS-SVM). Then, the remaining features are arranged according to the predictor importance criterion. The least important features are eliminated in the order. The remaining features of this stage, which have created the highest level of accuracy in LS-SVM, are selected as the final features. The features obtained, compared to other similar articles which have examined the selected features in the least squared support vector machine model, are better in the accuracy, true positive rate, and false positive. The results are tested by the UNSW-NB15 dataset.

**Keywords :** decision tree, feature selection, intrusion detection system, support vector machine
**Conference Title :** ICESCE 2018 : International Conference on Electronics System and Computer Engineering
**Conference Location :** Vienna, Austria
**Conference Dates :** June 14-15, 2018