A NOVEL APPROACH FOR NETWORK INTRUSION DETECTION USING EXTREME GRADIENT BOOSTING AND LONG SHORT-TERM MEMORY RECURRENT NEURAL NETWORKS

R. E. Ratnayake

Department of Statistics and Computer Science, University of Peradeniya, Peradeniya, Sri Lanka

A novel approach for network intrusion detection was presented using Extreme Gradient Boosting (XGBoost) for feature selection and then using the selected features in a Long Short-Term Memory (LSTM) Recurrent Neural Network (RNN) classifier. The purpose of this research was to create a number of minimal feature sets using XGBoost and study the effects of using them in a LSTM RNN model for detecting whether or not the network features belong to an attack. NSL-KDD dataset, which is an improved version of KDD Cup '99 dataset was used. After preprocessing all the features in the dataset, they were fed into XGBoost and feature importance was calculated. Based on the scores for importance obtained by the features, minimal feature sets were created. Then, LSTM recurrent neural network classifier was applied using all the features in the dataset and the minimal feature sets, separately. The results of applying the LSTM on all the features and only the feature sets created using XGBoost were finally compared. According to the experimental results, it was observed that XGBoost feature selection could be used to create minimal feature sets with very high feature reduction ratios to use in a LSTM RNN model for network intrusion detection to achieve a good accuracy value close to that achieved using all the features in the dataset. The findings of this study can be used for building better network intrusion detection systems using deep neural networks for real-time network intrusion detection. Also, they can be utilized to develop a first layer of defense for alerting the users about possible threats in real-time.