Abstract

Increasing internet usage and connectivity demands a network intrusion detection system combating cynical network attacks. Data mining therefore is a popular technique used by intrusion detection system to prevent the network attacks and classify the network events as either normal or attack. Our research study presents a wrapper approach for intrusion detection. In this framework Feature selection technique eliminate the irrelevant features to reduce the time complexity and build a better model to predict the result with a greater accuracy and Bayesian network works as a base classifier to predict the types of attack. Our experiment shows that the proposed framework exhibits a superior overall performance in terms of accuracy which is 98.2653, error rate of 1.73 and keeps the false positive rate at a lower rate of 0.007. Our model performed better than other leading state-of-the-arts models such as KNN, Boosted DT, Hidden NB and Markov chain. The NSL-KDD is used as benchmark data set with
Weka library functions in the experimental setup.

References

A Network Intrusion Detection Framework based on Bayesian Network using Wrapper Approach


Index Terms

Computer Science  Pattern Recognition

Keywords

Intrusion Detection System, Feature Selection, Genetic Search, Bayesian Network, Weka, NSL-KDD.