Abstract

The security of computer networks is of great importance. But, with the proliferation of electronic devices and the internet, there has been an exponential rise in malicious activities. The security perpetrators take the advantage of the intricacy of the internet and carry out intrusions. There have been certain researches to find out solutions for detecting intrusions. In this paper, the research has been the application of machine learning techniques to the field of network intrusion detection. Machine learning techniques can learn normal and anomalous patterns from training data and generate classifiers which can be used to detect intrusions in a network. The machine learning techniques used are Naïve Bayes Tree algorithm and the Voting Feature Intervals algorithm. Also, Feature Selection Methods to improve the performance of these algorithms were used because the input to classifiers is in a high dimension feature space, but all features available are not relevant for classification. Two approaches were taken into consideration for feature selection, Chi Square and Gain Ratio. Using these feature selection approaches a comparative study of the two algorithms NBTree and VFI as classifiers has been done. The NSL-KDD data set has been used to train and test the classifiers.
Comparison of NBTree and VFI Machine Learning Algorithms for Network Intrusion Detection using Feature Selection

Comparison of NBTree and VFI Machine Learning Algorithms for Network Intrusion Detection using Feature Selection

- Jiawei Han, Micheline Kamber. 2006. Data Mining: Concepts and Techniques, Harcourt India Pvt Ltd.
- Weka Machine Learning Project.

Index Terms

Computer Science  Security

Keywords

Machine learning  NBTree  VFI  Feature selection  Chi Square  Gain Ratio.