Comparative Analysis of Machine Learning Algorithms along with Classifiers for Network Intrusion Detection

Objective: To detect network intrusion use of machine learning through data mining.

Motivation: To monitor network for any harmful activity. And the data is large so data mining was used.

Proposed methodology: Weka was used for 9 different classifier's performance measurement and the performance was compared.

Contribution: From this work we can get the assessment for which classifier can possibly give the best accuracy.

Lacking: I don't see any big lacking in this work, but it would be better if there was also comparison how these classifiers work with different amounts of data.

This work gives the assessment of classifiers accuracy. This work will help us by giving the idea of what should we asses and the methodology give us knowledge to some extent.

Comparative Analysis of Five Machine Learning Algorithms for IP Traffic Classification

Objective: Analysis of different machine learning algorithms for real-time IP traffic classification.

Motivation: The motivation was to see how which machine learning algorithm gives the better result with real-time internet traffic classification.

Proposed methodology: Dataset was created by capturing internet traffic and 5 different algorithms were used to find the accuracy.

Contribution: This work gives a comparative analysis how ML algorithm performs with dynamic IP classification.

Lacking: With the ML algorithm comparison, the real-time dataset was also a important part of this work, so it would be better if the data was captured from different high network traffic places.

This work gives us knowledge on how the algorithm and data can be analyzed with the comparison result.