Abstract

Data mining has been used extensively and broadly by several network organizations. Classification based algorithms provide a significant advantage in order to detect attacks in the training data. Network applications usage is being increased every day as the internet usage is exponentially increasing. In the same way, Network attacks detection is gradually decreased as data source is increasing. There is a need to develop some robust decision tree in order to produce effective decision rules from the attacked data. In this paper improved, decision tree is implemented in order to detect network attacks like TCP SYN, Ping of Death, ARP Spoof attacks. This improved tree is also tested on famous network intrusion dataset Kddcup 99 dataset. Experimental result shows this improved decision tree classifier gives effective decision rules compare to existing decision tree techniques like ID3 and C45 algorithms. Finally, this robust decision tree evaluates less false positive and true negative alarm rates compare to existing algorithms.

References

- Ian H. Witten, Eibe Frank, Len Trigg, Mark Hall, "Weka: Practical Machine Learning Tools and Techniques with Java Implementations;"

**Index Terms**

Computer Science  
Network Security

**Keywords**

Ddos  Tcp  Upd  C45