A Robust and Efficient Real Time Network Intrusion Detection System Using Artificial Neural Network In Data Mining

Abstract

Today, intrusion detection is one of the major concern in the task of network administration and security. There is a need to safeguard the networks from known vulnerabilities and at the same time take steps to detect new and unseen, but possible, system abuses by developing more reliable and efficient intrusion detection systems.

The system must be accurate in detecting attacks with the minimum number of false alarms(wrong detections). Thus an Artificial Neural Network based NIDS is been developed so that the accuracy at which the intrusions are detected increases. In this network intrusion detection system, by using the concept of ensemble binary classification and multiboosting simultaneously it efficiently detects the attack with the low false alarm rate and even at high network traffic.

With the use of the Dynamic multiboosting and the database storage the time taken to detect the attacks has been decreased efficiently. By combining the concepts of the Artificial Neural network and the Data mining technique of classification the drawbacks of the later is overcome.