ABSTRACT

Anomaly detection refers to the problem of finding patterns in data that do not conform to expected behavior. These non-conforming patterns are often referred to as anomalies or outliers. Intrusion detection in computer networks is the process of monitoring for and identifying attempted unauthorized system access or manipulation. This project examines the application of Statistical Modeling for detecting intrusions in computer networks.

Currently, a rule based Network Intrusion Detection System (NIDS) relies on the details of previously known attacks. By knowing the attack vector, rules can be implemented in the firewall and/or other defense tools to recognize the attack and appropriately counter it. However the main drawbacks of this system are - New unknown attacks cannot be countered effectively till encountered and Damage to the system rendering any future counters to the attack useless.

We propose a small lightweight NIDS, which is a method to detect and identify attacks in real time. It will concentrate on a limited category of attacks from standard datasets containing well established and tested attack vectors, with considerations to latency. The network will be modeled by the NIDS using machine learning algorithms based on Naive Bayes Models.