Network anomaly classification by support vector classifiers ensemble and non-linear projection techniques

De La Hoz Eduardo, Ortiz Andrés, Ortega Julio, De la Hoz Franco Emiro.

Abstract

Network anomaly detection is currently a challenge due to the number of different attacks and the number of potential attackers. Intrusion detection systems aim to detect misuses or network anomalies in order to block ports or connections, whereas firewalls act according to a predefined set of rules. However, detecting the specific anomaly provides valuable information about the attacker that may be used to further protect the system, or to react accordingly. This way, detecting network intrusions is a current challenge due to growth of the Internet and the number of potential intruders. In this paper we present an intrusion detection technique using an ensemble of support vector classifiers and dimensionality reduction techniques to generate a set of discriminant features. The results obtained using the NSL-KDD dataset outperforms previously obtained classification rates.

Keywords