PCA filtering and probabilistic SOM for network intrusion detection

De la Hoz, E.a, De La Hoz, E.a, Ortiz, A.b, Ortega, J.c, Prieto, B.c

Abstract

The growth of the Internet and, consequently, the number of interconnected computers, has exposed significant amounts of information to intruders and attackers. Firewalls aim to detect violations according to a predefined rule-set and usually block potentially dangerous incoming traffic. However, with the evolution of attack techniques, it is more difficult to distinguish anomalies from normal traffic. Different detection approaches have been proposed, including the use of machine learning techniques based on neural models such as Self-Organizing Maps (SOMs). In this paper, we present a classification approach that hybridizes statistical techniques and SOM for network anomaly detection. Thus, while Principal Component Analysis (PCA) and Fisher Discriminant Ratio (FDR) have been considered for feature selection and noise removal, Probabilistic Self-Organizing Maps (PSOM) aim to model the feature space and enable distinguishing between normal and anomalous connections.

Keywords

Bayesian SOM, IDS, PCA filtering, Probabilistic SOM, Self-organizing maps