A data analysis for intrusion detection using principal component

Abstract

Nowadays Intrusion detection systems (IDS) are very important for every information technology company which is concerned with security and sensitive systems. Even if a lot of research was already done on this topic, the perfect IDS has still not been found and it stays a hot and challenging area in computer security research. This paper presents a simple and robust method for intrusion detection in computer networks based on principal component analysis (PCA) where each network connection is transformed into an input data vector. PCA is then employed to reduce the high dimensional data vectors and thus, detection is handled in a low dimensional space with high efficiency and low use of system resources. Our experiments with the KDD Cup 99 dataset, although not yet completed, have shown that this approach is promising in terms of detection accuracy. It is also effective to identify most known attacks as well as new attacks. However, a frequent update for both user profiles and attacks databases is crucial to improve the identification rates.