Abstract

Intrusion detection has gain a broad attention and become a fertile field for several researches, and still being the subject of widespread interest by researchers. The intrusion detection community still confronts difficult problems even after many years of research. Reducing the large number of false alerts during the process of detecting unknown attack patterns remains unresolved problem. However, several research results recently have shown that there are potential solutions to this problem. Anomaly detection is a key issue of intrusion detection in which perturbations of normal behavior indicates a presence of intended or unintended induced attacks, faults, defects and others. This paper presents an overview of research directions for applying supervised and unsupervised methods for managing the problem of anomaly detection. The references cited will cover the major theoretical issues, guiding the researcher in interesting research directions.
- Kumar, G. Kumar, K. and Sachdeva, M. 2010. The use of artificial intelligence based techniques for intrusion detection: a review.
- Moore, D. 2005. "Internet Traffic Classification Using Bayesian Analysis"
Techniques. in Proceedings of ACM SIGMETRICS.
Machine Learning Techniques for Anomaly Detection: An Overview


Index Terms

Computer Science
Security

Keywords

Supervised Machine Learning Unsupervised Machine Learning Network Intrusion Detection