Abstract

Intrusion detection continues to be an active research field. Even after 20 years of research, the intrusion detection community still faces several difficult problems. Detecting unknown patterns of attack without generating too many false alerts remains an unresolved problem. Although recently, several results have shown that there is a potential resolution to this problem. Anomaly detection is a key element of intrusion detection in which perturbations of normal behavior suggest the presence of intentionally or unintentionally induced attacks, faults, and defects. This paper proposes a hybrid machine learning model based on combining the unsupervised and supervised classification techniques. Clustering approach based on combining the K-means, fuzzy C-means and GSA algorithms to obtain the normal patterns of a user’s activity, the technique is used as the first component for pre-classification to improve attack detection. Then, a hybrid classification approach of Support Vector Machine (SVM) and Gravitational Search Algorithm (GSA) algorithm will be used to enhance the detection accuracy. This research used the KDD CUP 1999 to get initial results, which were encouraging.
An Adaptive Intrusion Detection Model based on Machine Learning Techniques

References

Proceedings of the 7th USENIX security symposium.

Index Terms

Computer Science
Security

Keywords
An Adaptive Intrusion Detection Model based on Machine Learning Techniques

Supervised Machine Learning  Unsupervised Machine Learning  Network Intrusion Detection