A Novel Cluster-based Intrusion Detection Approach Integrating Multiple Learning Techniques

International Journal of Computer Applications

Foundation of Computer Science (FCS), NY, USA

Volume 166

Number 3

Year of Publication: 2017

Authors:

Hossein Shapoorifard, Pirooz Shamsinejad

10.5120/ijca2017913948

Abstract

In order to make computer systems completely secure, in addition to firewalls and other intrusion protection devices, other systems called intrusion detection systems (IDS) are needed to detect intrusion and provide solutions to counter the intruder if he penetrated through firewall, antivirus and other security devices. Many IDS have been developed based on machine learning techniques. Specifically, advanced detection approaches created by combining or integrating multiple learning techniques have shown better detection performance than general single learning techniques. This paper proposes an improvement for a feature representation approach, namely the cluster center and nearest neighbor (CANN) approach.

References
2. H. Jiawei, M. Kamber, J. Han, M. Kamber, and J. Pei, Data Mining: Concepts and Techniques. 2012.

20. V. Golmah, “An Efficient Hybrid Intrusion Detection System based on C5.0 and SVM.,”

cascading k-Means clustering and C4.5 decision tree algorithm,” in Procedia Engineering, 2012,


Index Terms

Computer Science  Security

Keywords

Intrusion Detection System; Data Mining; Hybrid Intrusion Detection System; anomaly detection;
cluster center, nearest neighbor.