Abstract

Security is a key issue to both computer and computer networks. Intrusion detection System (IDS) is one of the major research problems in network security. IDSs are developed to detect both known and unknown attacks. There are many techniques used in IDS for protecting computers and networks from network based and host based attacks. Various Machine learning techniques are used in IDS. This study analyzes machine learning techniques in IDS. It also reviews many related studies done in the period from 2000 to 2012 and it focuses on machine learning techniques. Related studies include single, hybrid, ensemble classifiers, baseline and datasets used.

References


Analysis of Machine Learning Techniques for Intrusion Detection System: A Review

on industrial and engineering applications of artificial intelligence and expert systems (IEA/AIE), Lecture notes in computer science (Vol. 3029), Springer, 2004.


- X. Arau, R. de-Oliveira, E. -W. Ferreira, A. A. Shinode and B. Bhargara, "Identifying important characteristics in the KDD99 intrusion detection dataset by
- C. Chi, T. Wee-Peng H. Guang-Bin, &quot;Extreme learning machines for intrusion detection,&quot; The 2012 International Joint Conference on Neural Networks (IJCNN), 2012.
- G. Chunhua, and Z. Xueqin, &quot;A Rough Set and SVM Based Intrusion Detection Classifier,&quot; Second International Workshop on Computer Science and Engineering (WCSE &apos;09), 2009.

**Index Terms**

Computer Science  
Security

**Keywords**

Security  
Intrusion detection  
Machine learning techniques  
Classification.