Fast Hierarchical Relevance Vector Machine towards Network Intrusion Detection System

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 127
- Number 1

Year of Publication: 2015

Authors:
V. Jaiganesh

10.5120/ijca2015906312

Abstract

Internet becomes very essential needs in today’s life because internet has become a public network world wide. The art of detecting inappropriate, incorrect, or anomalous activity is Intrusion Detection (ID). It is a security service which monitors and analyzes system events for finding, and creating a real-time or near real-time scenario, trials to access system resources in an unauthorized manner. In the proposed Fast Hierarchical Relevance Vector Machine (FHRVM), Analytical Hierarchy Process Method (AHP) is used to select the input weights and hidden biases. The algorithm is used to analytically determine the output weights and the Iterative Learning Mechanism (ILM) algorithm is employed in order to learn the network through Relevance Vector Machine (RVM). It is established by developing a probabilistic Bayesian learning structure which is capable enough to derive accurate prediction models. Such prediction models will exploit considerably fewer basis functions. These incorporate the benefits of valid predictions; elimination of non-impact attributes along with it will facilitate usage of arbitrary functions. Simulation has been carried out using Math works MATLAB R2012a. KDD Cup 1999 dataset is taken for testing the performance of the proposed work and the results
indicate that FHRVM has achieved higher detection rate and low false alarm rate than that of existing RVM algorithm.

References


Index Terms

Computer Science

Security

Keywords

Intrusion Detection System (IDS), Relevance Vector Machine (RVM), Levenberg Marquardt and Analytical Hierarchical Process.