

Neural Networks as Tool to Improve the Intrusion Detection System

Esmeral Ernesto; Mardini Johan; Salcedo Dixon; De La Hoz Franco Emiro; Avendaño

Inirida; Henriquez Carlos

Abstract

Nowadays, computer programs affecting computers both locally and network-wide have led to the design and development of different preventive and corrective strategies to remedy computer security problems. This dynamic has been important for the understanding of the structure of attacks and how best to counteract them, making sure that their impact is less than expected by the attacker.

For this research, a simulation was carried out using the DATASET-KDD NSL at 100%, generating an experimental environment, where processes of pre-processing, training, classification, and evaluation of model quality metrics were carried out. Likewise, a comparative analysis of the results obtained after implementing different feature selection techniques (INFO.GAIN, GAIN RATIO, and ONE R), and classification techniques based on neural networks that use an unsupervised learning algorithm based on self-organizing maps (SOM and GHSOM), with the purpose of classifying bi-class network traffic automatically. From the above, a 97.09% hit rate was obtained with 21 features by implementing the GHSOM classifier with 10-fold cross-validation with the ONE R feature selection technique, which would improve the efficiency and performance of Intrusion Detection Systems (IDS).

Keywords

SOM neural networks GHSOM neural networks NSL_KDD IDS