Network Anomaly Detection with Bayesian Self-Organizing Maps

Emiro de la Hoz Franco[1,3], Andrés Ortiz García[2], Julio Ortega Lopera[1], Eduardo de la Hoz Correa[1,3], and Alberto Prieto Espinosa[1]

1 Computer Architecture and Technology Department, CITIC University of Granada, 18060 Granada, Spain

2 Department of Communications Engineering University of M´alaga, 29071 Málaga, Spain

3 Systems Engineering Program Coast University, Barranquilla, Colombia

Abstract. The growth of the Internet and consequently, the number of interconnected computers through a shared medium, has exposed a lot of relevant information to intruders and attackers. Firewalls aim to detect violations to a predefined rule set and usually block potentially dangerous incoming traffic. However, with the evolution of the attack techniques, it is more difficult to distinguish anomalies from the normal traffic. Different intrusion detection approaches have been proposed, including the use of artificial intelligence techniques such as neural networks. In this paper, we present a network anomaly detection technique based on Probabilistic Self-Organizing Maps (PSOM) to differentiate between normal and anomalous traffic. The detection capabilities of the proposed system can be modified without retraining the map, but only modifying the activation probabilities of the units. This deals with fast implementations of Intrusion Detection Systems (IDS) necessary to cope with current link bandwidths.

Keywords. Gaussian Mixture Model, Intrusion Detection System, Receiver Operating Curf Curve, Best Match Unit, Receiver Operating Curf