Abstract

In this work, the continue from the last research work done [20], thus it is proposed a data mining based anomaly detection system, aiming to detect volume anomalies, using Simple Network Management Protocol (SNMP) monitoring. The method is novel in terms of combining the use of Digital Signature of Network Segment (DSNS) with the evolutionary technique called Particle Swarm Optimization (PSO)[5] and neural network training, applied in a real data set. PSO is a high efficient heuristic technique with low computational complexity, developed in 1995 by Kennedy and Eberhart [1] inspired by social behavior of bird flocking. The DSNS is a baseline that consists of different normal behavior profiles to a specific network device or segment, generated by the GBA tool (Automatic Backbone Management), using data collected from SNMP objects. The proposed anomaly detection system uses the SVM in order to clusterize the traffic collected by SNMP agents and its respective DSNS. The PSO is combined with the SVM in order to improve performance and quality of the solution in the clusterization and calculation of clusters centroids. Tests were carried out using a real network environment in the Techno India University, Kolkata. Numerical results have been shown that the obtained detection and false alarm rates are promising. It is also implemented the deterministic method proposed in order to detect anomalies on the same dataset, so that both methods could be compared.
References
- Y. Shi and R. C. Eberhart, "Parameter selection in particle swarm..."
Network Anomaly Detection using PSO-ANN

optimization.


Index Terms

Computer Science  Networks

Keywords

Artificial Neural Network  Back Propagation  Intrusion Detection and Prevention  Network Attack.