Integrated Alert Correlation Approach Based on PCA and Levenberg-Marquardt Backpropagation Neural Network

Abstract

Since the internet becomes popular and files sharing is a must task in everyday life, organizations started to search for solutions to secure their confidential information. A popular solution to optimally monitor and detect any intrusion or threat in the network is the installation of multiple network-based Intrusion Detection Systems (NIDSs). Such distribution of NIDSs produces an enormous number of alerts in different kinds of format. This is due to a large amount of false positive alerts and the increment of new network attacks. Analyzing those alerts via correlation is important to discover the attack stages of a multi-stages network attack. But, manual analysis is unfeasible, labor intensive and time consuming. Thus, we propose a new alert correlation (AC) approach that can automatically recognize the pattern of known and new alerts to reveal the memberships of the attack stages. The new PcaLM integrates Principal Component Analysis (PCA) and Levenberg-Marquardt (LM) supervised learning algorithm on two-layer backpropagation neural networks for optimal correlation. The PCA aims to reduce the dimensionality of raw alerts and the LM responsibles to classify the alerts into the corresponding attack stages. Eventually, automated PcaLM can discover the relationships among alerts in terms of the cause of the attack stages. This can save much extra efforts spent on manual analysis of a huge volume of raw alerts. The empirical results show that the proposed approach gives better results in terms of classification accuracy and error rate than original LM even with large scale and highly redundant training dataset.