Abstract

Today network security, uptime and performance of network are important and serious issues in computer network. Anomaly is deviation from normal behavior affecting network security. Anomaly Extraction is identification of unusual flow from network, which is need of network operator. Anomaly extraction aims to automatically find the inconsistencies in large set of data observed during an anomalous time interval. Extracted anomalies will be important for root cause analysis, network forensics, attack mitigation and anomaly modeling. Frequent pattern mining technique namely Efficient-Web Miner Algorithm will be used to generate the set of association rules applied on metadata. Using network traffic log data, algorithms effectively finds the flow associated with the anomalous event(s). Efficient-Web Miner Algorithm triggers a very small number of false positives. Efficient-Web Miner has much better performance in terms of time and space complexity than Apriori Algorithm and its variations like Apriori All algorithm. for large data sets This anomaly extraction method significantly reduces the time needed for analyzing alarms, making anomaly detection systems more practical, simple and realistic. System makes an effort to mitigate the anomaly so detected without human intervention. Proposed system provides human overrides in mitigation process and inculcates self-learning approach which is advantageous.

Index Terms
Computer Science  Algorithms

Keywords
Anomaly Extraction  Association rule mining  data mining  detection algorithms  Efficient-Web Miner Algorithm