Abstract

Inconsistency or Anomaly extraction refers to the automatically finding a large set of flows observed during an anomalous time interval, the flows associated with anomalous events. It is valuable for root causes analysis, network forensics, anomaly modeling, and attack mitigation. In this paper, histogram based detectors are used which provide a meta-data which is useful for identifying suspicious flows and then apply association algorithm like Advanced FP-Growth Algorithm to summarize and find anomalous flows. Using rich traffic data from a network, Paper show that a technique efficiently finds the flows associated with anomalous events. In addition, an algorithm reduces the both in runtime and the main memory consumption. The inconsistency extraction method significantly reduces the working hours needed for anomaly detection system more practical.

References


**Index Terms**

- Computer Science
- Algorithms
Keywords
Association rules  computer network  data mining  FP-Growth  compound single linked list