Abstract

In a world where critical equipments are connected to internet, hence protection against professional cyber criminals is important. Today network security, uptime and performance of network are important and serious issue in computer network. Anomaly is deviation from normal behavior which is factor that affects on network security. So Anomaly Extraction which detects and extracts anomalous flow from network is requirement of network operator. Using Histogram based detector to identify anomalies and then applying Association rule mining, anomalies will extracted. Apriori algorithm will use to generate the set of rule applied on metadata. Identification and Extraction of anomalous flow can be used for useful application e. g. Root cause analysis, Network forensics, Modeling anomalies etc.

References

- Paul Barford, Jeffery Kline, David Plonka and Amos Ron. A Signal Analysis of Network Traffic Anomalies, IMWapos;02, Nov. 6-8, 2002, Marseille, France.

Index Terms

Computer Science
Artificial Intelligence

Keywords

Anomaly Detection Anomaly Extraction Association Rule Data Mining