Network anomaly detection using big data analysis

Analyzing network failure/cyber attacks and their root causes

Abstract—Network anomalies including network failures and cyber attacks are major concerns for both network and security operators, and their rapid detection is crucial to the provision of safe and reliable services. We are developing technologies for the rapid detection of such events via log messages from security appliances, network equipment, and servers or social media information such as Twitter messages. Since such information is atypical and its volume can be huge, we adopt machine learning methods, for example, mining temporal/host correlations in logs to detect network failure events or malicious hosts. By employing these technologies, we will help to provide safe and reliable communication services for our customers.

Related works


Contact

Keisuke Ishibashi
Communication Traffic & Service Quality Project
NTT Network Technology Laboratories
E-mail: ishibashi.keisuke(at)lab.ntt.co.jp

Mitsuaki Tsunakawa
Security Management & Operations Project
NTT Secure Platform Laboratories
E-mail: tsunakawa.mitsuaki(at)lab.ntt.co.jp

*1 SIEM: Security Information and Event Management
*2 SOC: Security Operation Center
*3 SIGINT: Signal Intelligence
*4 HUMINT: Human Intelligence

[Please replace (at) with @]