Dynamic Network Health Management System

Hyong Kim, Mark Poepping, et al. for the SAFE Center at Carnegie Mellon

Motivation

→ Networks are constantly evolving

- Network elements are frequently added (e.g. to offer new capabilities)
- Configurations are continuously updated (e.g. to satisfy customers' requests)
- Novel applications keep emerging

→Such dynamics make networks difficult to manage and vulnerable

- Network attacks can disrupt service and steal resources by exploiting vulnerabilities
- Misconfigurations can affect connectivity, violate policies and disclose confidential data

Proposed Approach

→ Situational awareness for networks

i) learn about the current environment,

ii) discover weaknesses and attacks

iii) suggest corrective actions.

→ **Initial phase** focuses on detection of router and network-wide misconfigurations.

1. Collect network data/metrics through EDDY
2. Apply data mining techniques to analyze router configurations vulnerability
3. Correlate collected data and analyze results

→ New approach

- Correlation of static and dynamic data to discover misconfigurations and violations.
- Detection of misconfiguration through data mining techniques.
- Proactive approach: Misconfigurations and vulnerabilities are often learned after incidents happen. Instead, proposed approach pro-actively detects weaknesses in network.

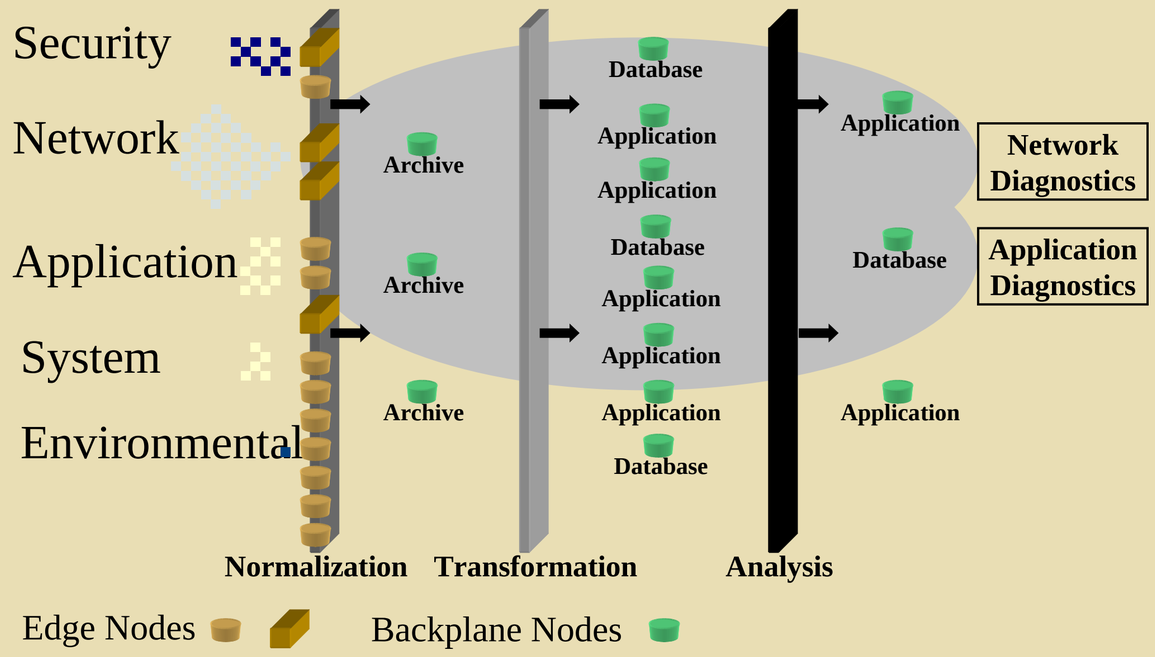
Research Impact

- Early detection of network weaknesses
- Enhanced reliability and stability (address hijacks often come from misconfigurations)
- Increased communication and protocol performance (misconfigurations increase BGP churn which in turn delays convergence time)

  → Enabler for new services and continued innovation

EDDY: Data Collection & Monitoring

- Activity audit ledger providing telemetry for layered and interdependent services analysis (e.g., faults, anomalies)



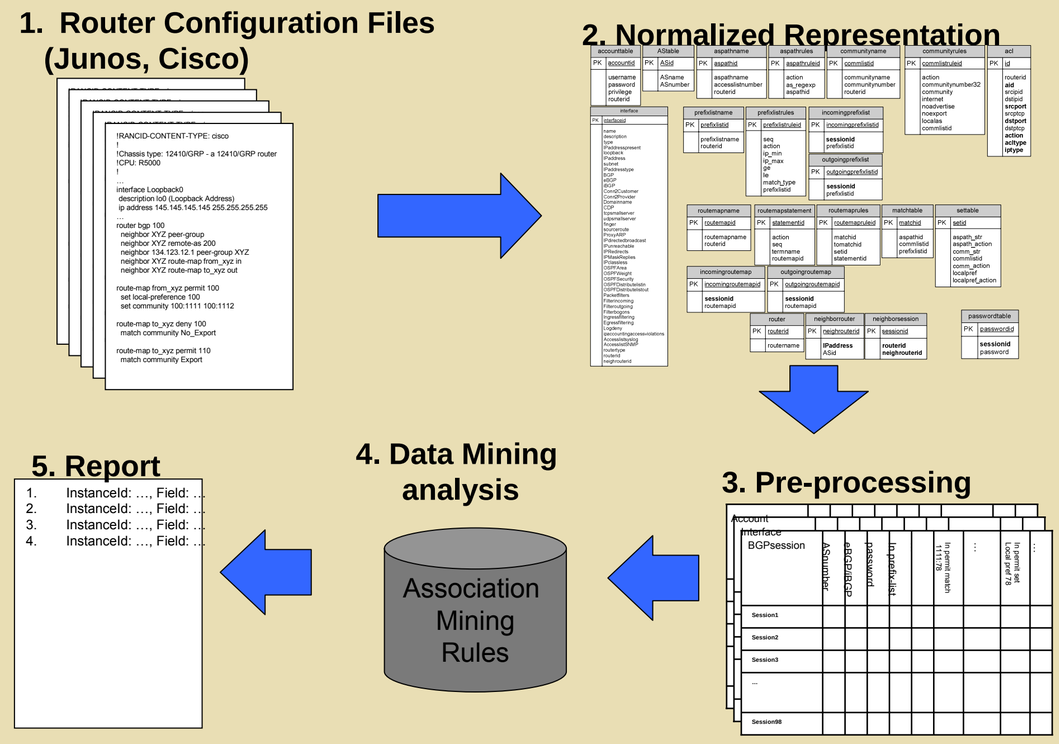
Minerals: analysis using data mining

→ *Why Data Mining?*

- Analyzes data to discover patterns
- Often, can outperform humans and other traditional computational algorithms

→ *Explored application of association rules mining to detect misconfigurations*

- Infers local policies by searching for causal relations (X → Y) in the data set.
  - user's privilege = 15 → password = 1
- Violations of these "rules" would indicate misconfigurations



→ *Analysis run on three operational networks*

- One ISP (45 routers), one stub network (65 routers), one research network (8 routers)

→ *Detected a number of misconfigurations*

- Missing/incorrect filters (e.g., prefix-list)
- Erroneous community
- Missing user password on super user accounts
- Lacking routing policies
- Missing MD5 security protection on eBGP

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Cyber Trust Principal Investigators Meeting
January 28-30, 2006
Atlanta, Georgia