AUTOMATED ADAPTIVE QUALITY AND SECURITY MONITORING IN 5G NETWORKS

Presented by Tommi Pernilä and Markku Suominen
Who are we

• Markku Suominen
  • 30+ years IT experience
  • Programmer/architect/security consultant

• Tommi Pernilä
  • 10+ years of IT security
  • Security consultant
Why do we need this kind of tool

- Unknown amorphous network structure
- How to find order from chaos?
SDN NFV

- Software Defined Network
- Network Function Virtualization
- Amorphous network structure
Why are we here

• 5G-ENSURE
• New problem => New tools
• Small network - Humans can analyze the data
• Complex network - Humans do not scale
  - Computers can scale
5G

- SDN NFV
- New protocols – Unknown to parsers
- Encrypted connections
- Major fluctuations
How does the tool work

- Capture network traffic
- Analyzes network data
- Finds patterns
- Classifies
- Visualizes
General architecture

Data sources

Packet collectors
Event sources

Input stage

Event processing
Packet processing
General architecture

Data sources → Input stage → Event broker

Communication bus for event-data
Events in this case meaning topology changes
General architecture

- Data sources
- Input stage
  - Classifies nodes
  - Clients, servers
  - Sets node trust levels
- Node classifier
- Event broker
General architecture

- Data sources
- Node state database
- Input stage
- Event broker
- Node classifier

Keeps the state of nodes and their connection status
General architecture

Data sources → Input stage → Event broker → Output stage

- Node state database
- Output stage: Outputs data, Alerts, Topology, Statistics, Events
General architecture

Data sources

Provides communication
Network state analysis - Intelligence
Sets alarms
Refines observations

Output stage

Observer agents

Event broker

Node state database

Node classifier

Observer agents
General architecture

Data sources

Node state database

Input stage

Output stage

Observer agents

Shadow nodes

Shadow node is a model of a node
Based on classification and state
It follow its counterpart and reports unexpected behaviour
Used technologies

- Bro – Network Security Monitor
- Gephi - The Open Graph Viz Platform
- Mosquitto - MQTT Broker
- Python libraries - scikit-learn
Machine learning

• Gives "computers the ability to learn without being explicitly programmed." –Arthur Samuel
• A must in complicated and dynamic system
• Predefined description and rules are not feasible
• Teaching the machine
  • Teaching data / Actual data
Algorithm used for learning

- Random forests
- Unsupervised learning
Screenshots
Screenshots
Summary

- Created a new tool
- Tuning unsupervised learning
- Gephi for visualization - not the best in this case
Thank You!

Q&A