NFV-compliant Traffic Monitoring and Anomaly Detection based on Dispersed Vantage Points in Shared Network Infrastructures

Adam Pavlidis, Giannis Sotiropoulos, Kostas Giotis, Dimitris Kalogeras, Vasilis Maglaris
Network Management & Optimal Design Laboratory (NETMODE)
School of Electrical & Computer Engineering
National Technical University of Athens

4th IEEE Conference on Network Softwarization (NetSoft 2018)
June 26th, 2018
Montreal, Canada
Modern ICT Infrastructures

Current considerations:

- Ever-growing demand for cloud services and resources
  - Compute, Storage, Network
- Dramatic proliferation of multi-vector cyber attacks
- Need for flexible and adaptive operations

Modern Technologies (SDN, NFV) enable:

- Disassociation of SW from HW (Virtualization)
- Automation and Streamlining of operations (Configurable SW)
- Reduction of CAPEX & OPEX (Reusable COTS)
Monitoring and Analytics

- Important for planning and operations:
  - Emphasis on Multi-Tenant (owner) environments

- Typical Problems:
  - Placement of Monitoring Agents
  - Processing, Storage
  - Access Control

- Environments to consider:
  - Internet Exchanges (e.g. AMS-IX)
  - Data Center Interconnect and Access facilities
  - Virtual Organizations in LAN and WAN environments
Network Monitoring

- Traffic export tools (e.g. NetFlow, sFlow)
  - Data as input to Analysis Tools
  - Sampling: Constant tradeoff (scalability / visibility)
- Hierarchically structured architecture, defining distinct **Vantage Points (VP)**
Network Monitoring

- Traffic export tools (e.g. *NetFlow, sFlow*)
  - Data as input to Analysis Tools
  - Sampling: Constant tradeoff (scalability / visibility)

- Hierarchically structured architecture, defining distinct **Vantage Points (VP)**

Vantage Point:
“A position or place that affords a wide or advantageous perspective.” source: Wikipedia
Network Monitoring

- Traffic export tools (e.g. NetFlow, sFlow)
  - Data as input to Analysis Tools
  - Sampling: Constant tradeoff (scalability / visibility)
- Hierarchically structured architecture, defining distinct **Vantage Points (VP)**
  - Distributed probes (Active/Passive)
    - Route Views
    - RIPE Atlas
    - RIPE Routing Information Service
  - Looking glass tools
NFV-compliant Traffic Monitoring and Anomaly Detection

**Motivation:**

NFV-based, container driven architecture, focused on:

- Collecting Network Monitoring data from multiple vantage points

- Offering related analytics services to users within multi-tenant infrastructures
  - Traffic Analysis and Anomaly Detection services based on varying Monitoring Views
Architectural Components

- Monitoring Data Handler
  - Collect
  - Isolate (tag)
  - Enrichment
  - Export

- Centralized Data Warehouse
  - Store tagged data
  - Expose to consumers

- Customized (Tenantized) Analytics
  - Traffic Visualization
  - Anomaly Detection

- Orchestrator
  - Validate User requests
  - Provision new services
  - Configure live instances
**Monitoring Data Handler**

- **Collector**
  - sFlow (*sflowtool*)
- **sMonNet module (sFlow Monitored Network)**
  - Tagging (Packet Headers, sFlow Agent)
  - Dedicated Enrichment (*MaxMind* datasets)
- **Kafka – Distributed Messaging Platform**
  - Produce/Consume samples
  - Separate topics (ingestion, enrichment jobs)
Centralized Data Warehouse

- **ElasticSearch**
  - Schema-less *documents*
  - Separate tags per *Vantage Points (VP) & User (Tenant)*
  - Full-text search

- **AUTH Middleware**
  - Proxy for *Elasticsearch*
  - Validation of user-provided tags (isolation)
  - Enterprise solutions
    - *X-PACK, Search Guard*
Customized Analytics Services

- **Anomaly Detection per Vantage Point**
  - Lightweight algorithm for Entropy-based Anomaly detection
  - Analyze data from varying VPs

- **Kibana PoC: Traffic Visualization**
  - Provide pre-defined but configurable dashboards
Orchestrator

- **External Facing API**
  - Tornado Web Framework

- **RBAC**
  - User – Tag Association
  - Validation of User Requests
    - AUTH Middleware

- **Provision & Manage**
  - Kubernetes API
  - sMonNet
    - Provision/Scale sMonNet jobs
    - User & VP identifiers and Kafka Topics pub/sub specification
  - Customized Analytics
    - Provisioning and Initialization

---

**A. MONITORING DATA HANDLER**

- sMonNet Pipeline
  - Data Identification
  - Data Enrichment
  - Authenticator

**B. CENTRALIZED DATA WAREHOUSE**

- Elasticsearch
  - Anomaly Detection
  - Traffic Visualization

**C. CUSTOMIZED ANALYTICS**

- D. ORCHESTRATOR
  - Web UI
  - RBAC
  - Provision & Manage

---

**Docker Containers managed by Kubernetes**

(i) - Export
(ii) - Ship data
(iii) - Ethernet Switch
(iv) - Kafka Cluster - KC
(v) - Samples

**PROVISION & MANAGE**

- Kubernetes API
- sMonNet
  - Provision/Scale sMonNet jobs
  - User & VP identifiers and Kafka Topics pub/sub specification
- Customized Analytics
  - Provisioning and Initialization
**Orchestrator**

- **External Facing API**
  - Tornado Web Framework

- **RBAC**
  - User – Tag Association
  - Validation of User Requests
    - AUTH Middleware

- **Provision & Manage**
  - Kubernetes API
  - sMonNet
    - Provision/Scale sMonNet jobs
    - User & VP identifiers and Kafka Topics pub/sub specification
  - Customized Analytics
    - Provisioning and Initialization

Diagram:

- **A. MONITORING DATA HANDLER**
  - sMonNet Pipeline
    - Data Identification
    - Data Enrichment
  - Job 1
  - Kafka Cluster - KC

- **B. CENTRALIZED DATA WAREHOUSE**
  - Elasticsearch

- **C. CUSTOMIZED ANALYTICS**
  - Anomaly Detection
  - Traffic Visualization

- **D. ORCHESTRATOR**
  - Web UI
  - REST API
  - RBAC
  - Provision & Manage

- **E. ORCHESTRATOR**
  - AUTH Middleware

- **NETMODE testbed**
  - (GRNET)

- **~okeanos IaaS**
  - (GRNET)

- **NETSOFT**
  - (NTUA LAN)
Case Study

Lightweight anomaly detection on data gathered from different VPks.

**Aim:** to improve detection of different types of network anomalies

**Data from NTUA Campus LAN:**

- **Benign Traffic:**
  - Traces from an access switch
  - Traces from a core switch/router

- **Attack Traffic:**
  - Worm Propagation
  - Port Scanning attack
Experimental Results

Worm Propagation:
Increased visibility in Access VP
- Granular network view for localized characteristics
- Scalability via Kafka Pipeline
  - many access devices

Port Scanning:
Increased visibility in Core VP
- Good overview, suitable for infrastructure-wide anomalies
- Fewer strategic observation points (VPs) aggregating large volumes of traffic
Experimental Results

Worm Propagation:
Increased visibility in Access VP
- Granular network view for localized characteristics
- Scalability via *Kafka* Pipeline
  - many access devices

Port Scanning:
Increased visibility in Core VP
- Good overview, suitable for infrastructure-wide anomalies
- Fewer strategic observation points (*VPs*) aggregating large volumes of traffic
Experimental Results

Worm Propagation: Increased visibility in Access VP

- Granular network view for localized characteristics
- Scalability via Kafka Pipeline
  - many access devices

Port Scanning: Increased visibility in Core VP

- Good overview, suitable for infrastructure-wide anomalies
- Fewer strategic observation points (VPs) aggregating large volumes of traffic
Experimental Results

Worm Propagation: Increased visibility in Access VP
- Granular network view for localized characteristics
- Scalability via Kafka Pipeline
  - many access devices

Port Scanning: Increased visibility in Core VP
- Good overview, suitable for infrastructure-wide anomalies
- Fewer strategic observation points (VPs) aggregating large volumes of traffic
Considerations for Future Work

- Explore applicability in multi-tenant cloud environments

- Investigate algorithms tailored to specific attack profiles:
  - Dynamically Select Vantage Points
  - Adaptively tune monitoring Sampling Rates and alarm thresholds
  - Select appropriate network identifiers (e.g. L2/L4 attributes)

- Integrate standardized MANO and Automation Frameworks:
  - OSM, ONAP, CORD
  - Ansible, SaltStack, Napalm (Vantage Point configuration)
THANK YOU!

Adam Pavlidis
apavlidis@netmode.ntua.gr