LFNETWORKING
Developer & Testing Forum

Revolutionizing Network Monitoring: Unleashing AI/ML for Management and Network Orchestration

Maggie Cogdell

Laboratory for Advanced Cybersecurity Research (LACR)

NSA Research

mccogde@uwe.nsa.gov

Yatis K. Dodia

Georgia Tech Research Institute

yatis.dodia@gtri.gatech.edu

https://lfnetworking.org

Agenda

Background
Problem Motivation
Slice Threat Modeling
SD-Core and Data Generation
DCAE
Closing the Loop

LF NETWORKING

LFN Developer & Testing Forum

Background

Problem Motivation

Slice Threat Modeling

SD-Core and Data Generation

DCAE

Closing the Loop

Maggie Cogdell

5G Slice Security and Orchestration

LFN Developer & Testing Forum

- Goal: Create a comprehensive capability to obtain real-time insights into the security of 5G networks.

- Objectives:
  - Create testbed collect and classify relevant data
  - Identify performance and fault metrics that indicate abnormal network behavior
  - Apply to the Distributed Slice Mobility (DSM) attack
  - Demonstrate Closed Loop proof of concept
  - Contribute model and lessons learned to the Linux Foundation

Progress update and background

- 5G Open Source Testbed
  - Define relevant data sources and capture data sets (this is hard!)
  - Define performance metrics for monitoring / instrumentation of the network and compute resources
  - Implement programmatic hooks for 5G Core and ONAP
- Data ingestion and model construction
  - Data gathering and packaging
  - Training & analysis
- ML model building, testing, analysis e.g.
  - Deep learning for anomaly detection
  - Reinforcement learning for response

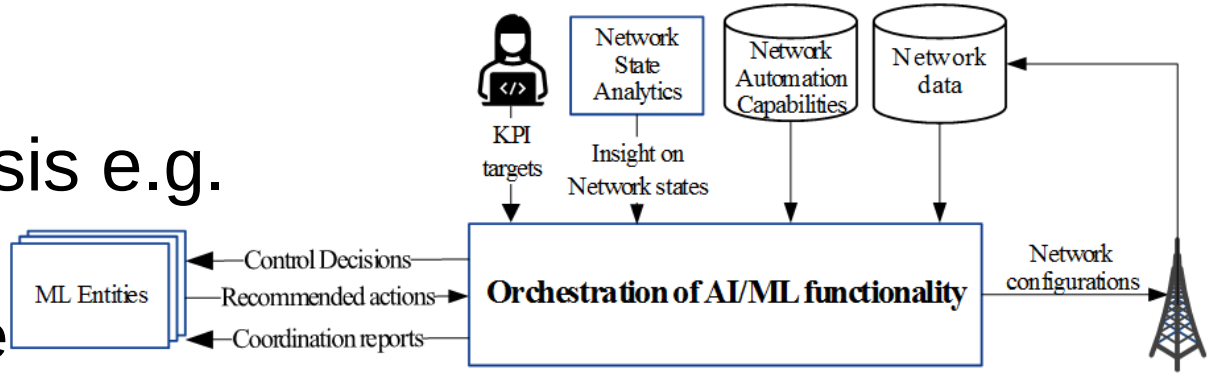
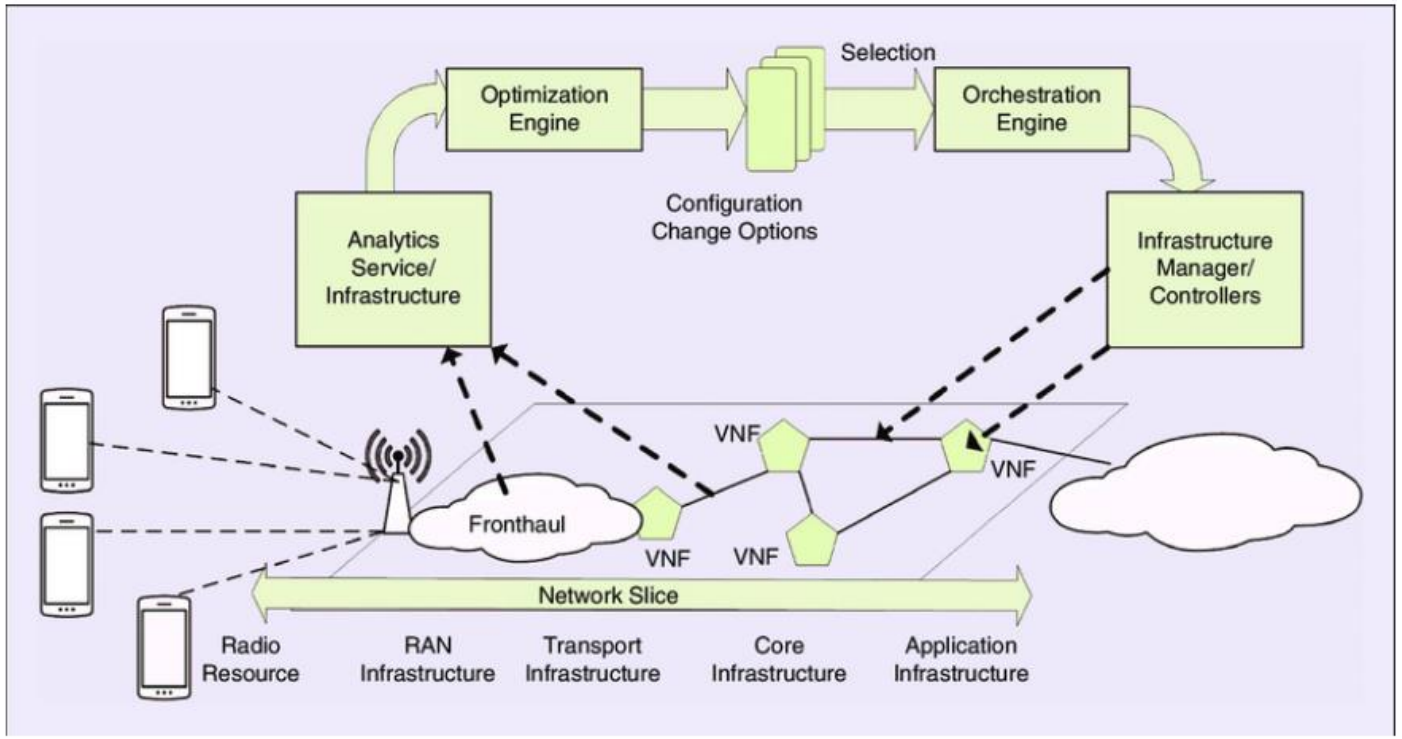


Figure 5.2.2.2.5-1: Orchestrating AI/ML

3GPP TR 28.908 V1.2.0 (2023-04)

Summary

- Network Slice resiliency
- What actions will an operator want to take automatically?
  - Contain, mitigate, isolate, etc.
- Closed Loop



https://www.researchgate.net/figure/an-Son-in-a-5g-network-including-orchestration-of-the-ran_fig2_322879450

LF NETWORKING

LFN Developer & Testing Forum

5G Cyber Using ONAP's DCAE

Yatis K. Dodia

LFN Developer & Testing Forum

Background
Problem Motivation
Slice Threat Modeling
SD-Core and Data Generation
DCAE
Closing the Loop

Yatis K. Dodia

5G Cybersecurity

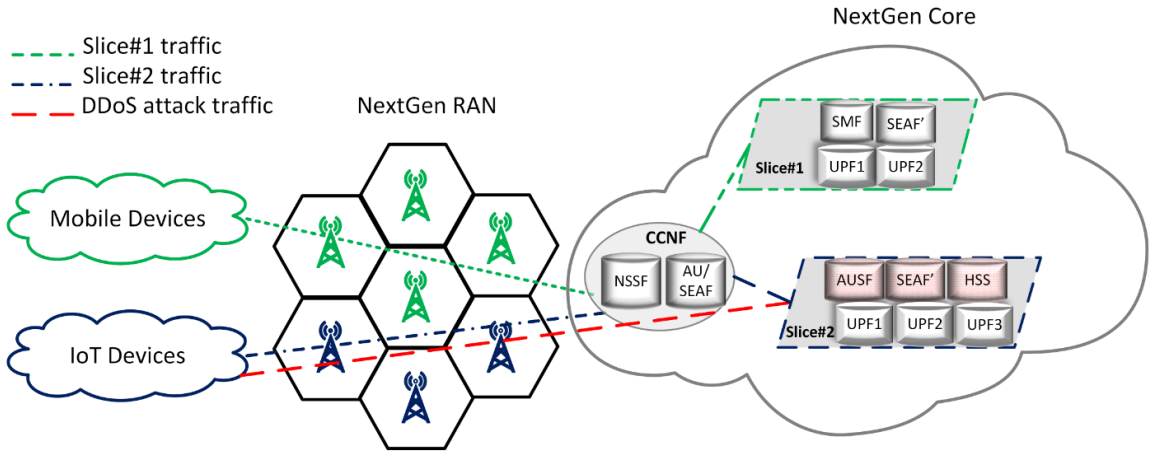
LFN Developer & Testing Forum

Cyber Threats

- Privacy
  - User targeting and presence detection
- Accessibility and/or Service Degradation
  - RAN jamming attacks, low-power
- Slicing
  - DoS
  - Economic costs to MNO

- **Goal**: Leverage smart algos & AI/ML to detect and mitigate threats at machine speed

Adversary covertly injects messages to the target, reveal presence of target in a given cell.



Example DDoS scenario

LF NETWORKING

LFN Developer & Testing Forum

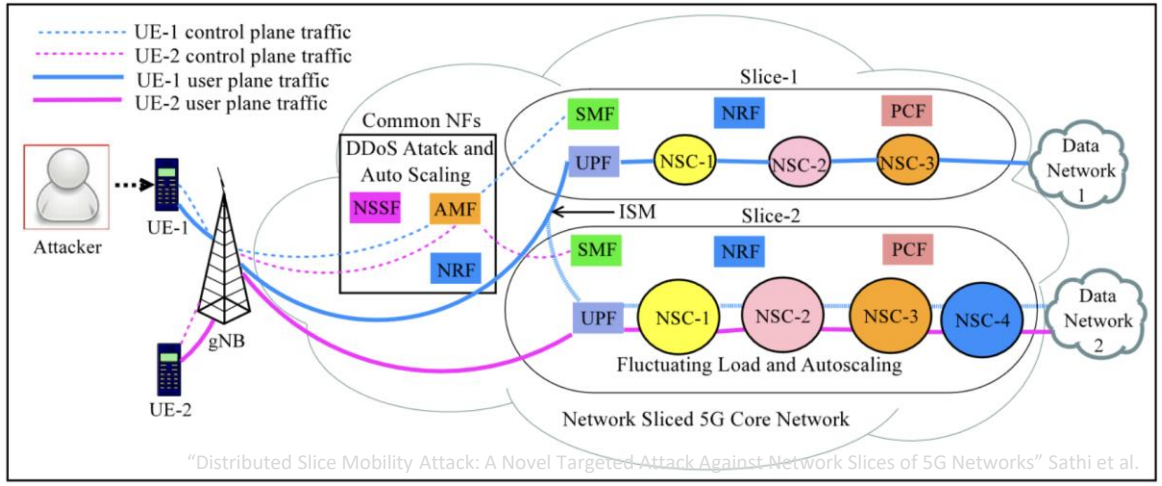
Background
Problem Motivation
Slice Threat Modeling
SD-Core and Data Generation
DCAE
Closing the Loop

Yatis K. Dodia

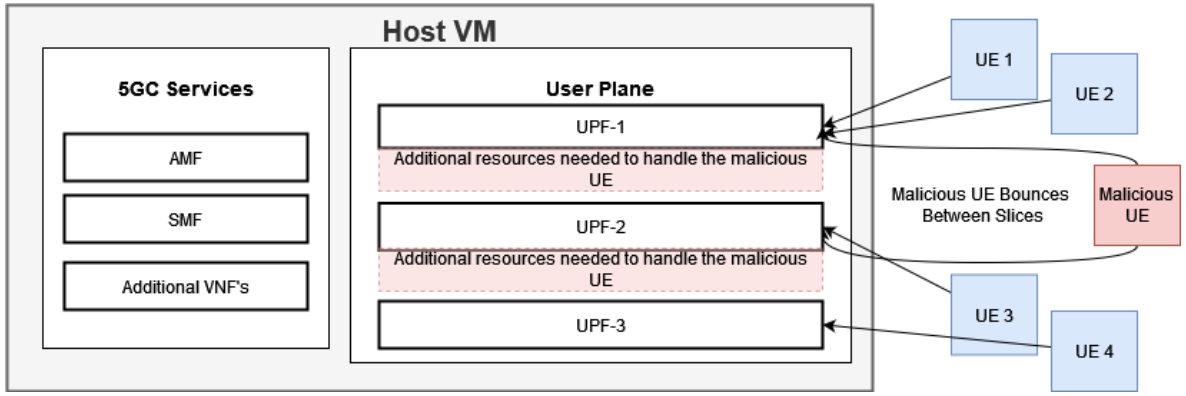
Slice Threat Modeling

- Dynamic slice mobility threat
  - Resource exhaustion
  - Trigger auto-scaling of virtual resources
  - Spin up unnecessary resources
    - MNO incurs costs
    - Degrades customer experience
    - Rinse and repeat
  - Primarily an economic attack but also service degradation

- Simulated and demonstrated using SD-Core



Overview of DoS attack exploiting auto-scaling



Attack exploiting dynamic slice mobility

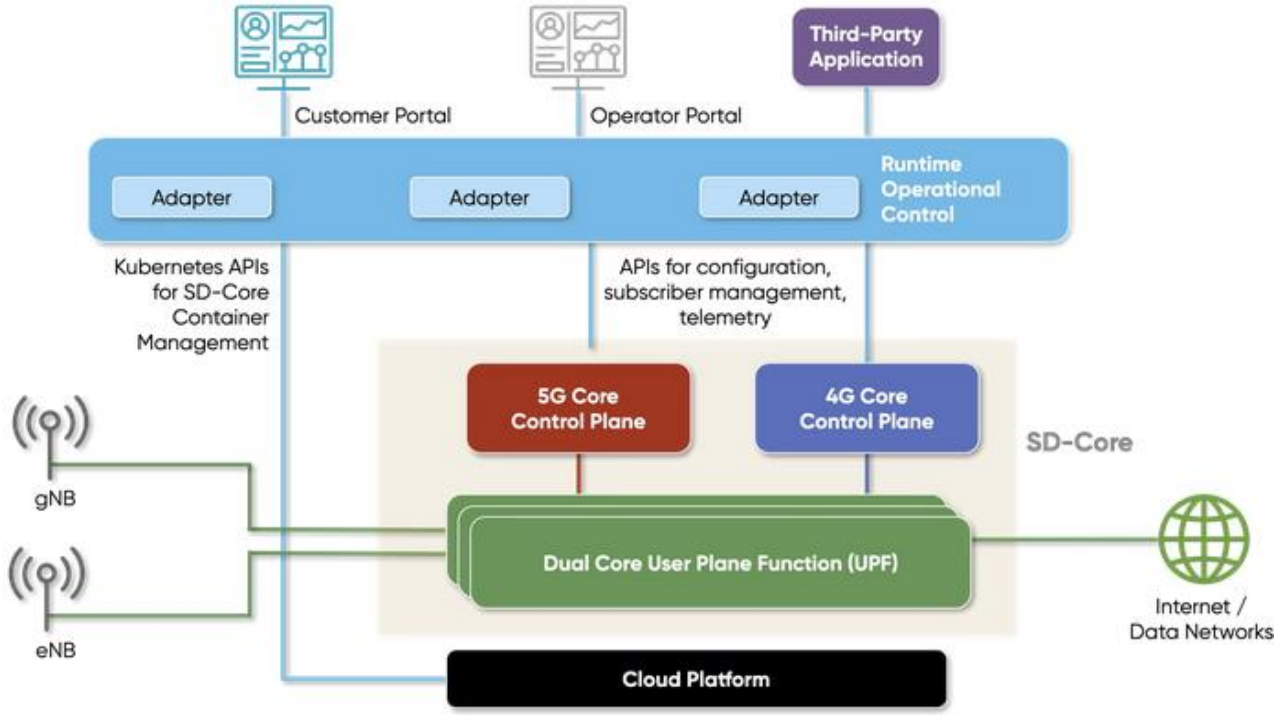
LFN Developer & Testing Forum

Background
Problem Motivation
Slice Threat Modeling
SD-Core and Data Generation
DCAE
Closing the Loop

Yatis K. Dodia

SD-Core | Overview

- Flexible and scalable 4G/5G Core
- Based on Free5GC
- 3GPP standards compliance
- APIs for runtime operational control (ROC)
- Good sandbox for 5G threat emulation



SD-Core | Data | 5G Core

- Using the slicing threat scenario, we collect data from various VNFs:
  - AMF
  - SMF
  - NSSF (TBD)
- Monitor metrics to gauge health and proper functioning of slicing mechanics
- Data is captured and packaged into VES Events and sent upstream to ONAP's DCAE

SMF

Metric	Use
n11_messages_total	Add, modify, del PDU sessions
nrf_messages_total	Session transfers
process_cpu_seconds_total	Implementation and instance resource utilization

AMF

ngap_messages_total	PDU Session Resource and UE Context management

metricfunc

nf_status	Status
smf_pdu_sessions	Count of sessions
smf_svc_stats	Various service stats

SD-Core | Data | Virtual Resources

- Compute infrastructure metrics
  - Memory
  - CPU utilization
  - Disk read/write ops and bytes
- Implementation specific metrics
  - Core VNF process info
  - SD-Core provides and open-source allows potential for extending data collection
- Finite resources are allocated to VMs, k8s pods, etc.
- If threat triggers auto-scaling, what does that look like to operator and the detection model?

Implementation Metrics

Metric	Use
info	Various info about the VNF process
VM additions and scaling Count of threshold triggers	Physical layer resource saturation and “yoyo-ing”
Stack and heap memory CPU utilization	Metrics exist for mem and call stack instrumentation
threads	Thread count of VNF processes

LF NETWORKING

LFN Developer & Testing Forum

Background
Problem Motivation
Slice Threat Modeling
SD-Core and Data Generation
DCAE
Closing the Loop

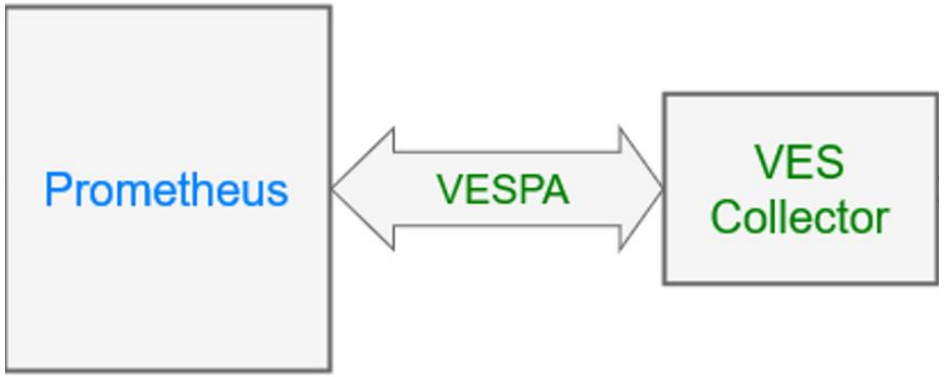
Yatis K. Dodia

DCAE Integration | VESPA

- VESPA converts the metrics captured by Prometheus into VES events
- A known metric can be formatted as a JSON object and marked for collection

```
metrics:
  - target: AdditionalObjects
    expr: ngap_messages_total
    object_name: ngapMessages
    object_instance: totalMessages
    object_keys:
      - name: msgType
        expr: "{{.labels.msg_type}}"
```

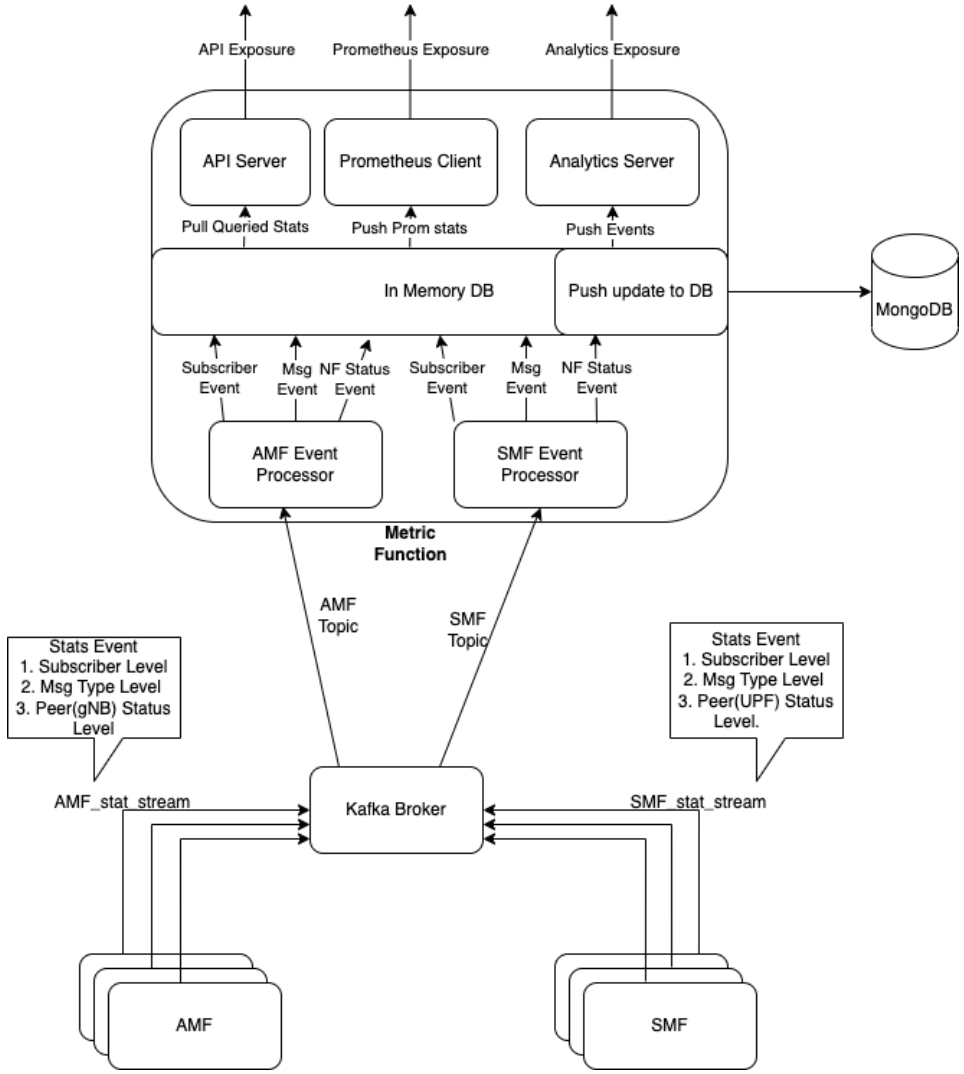
Example Prometheus to VES Event Definition



VESPA Connection Between Prometheus and VES Collector

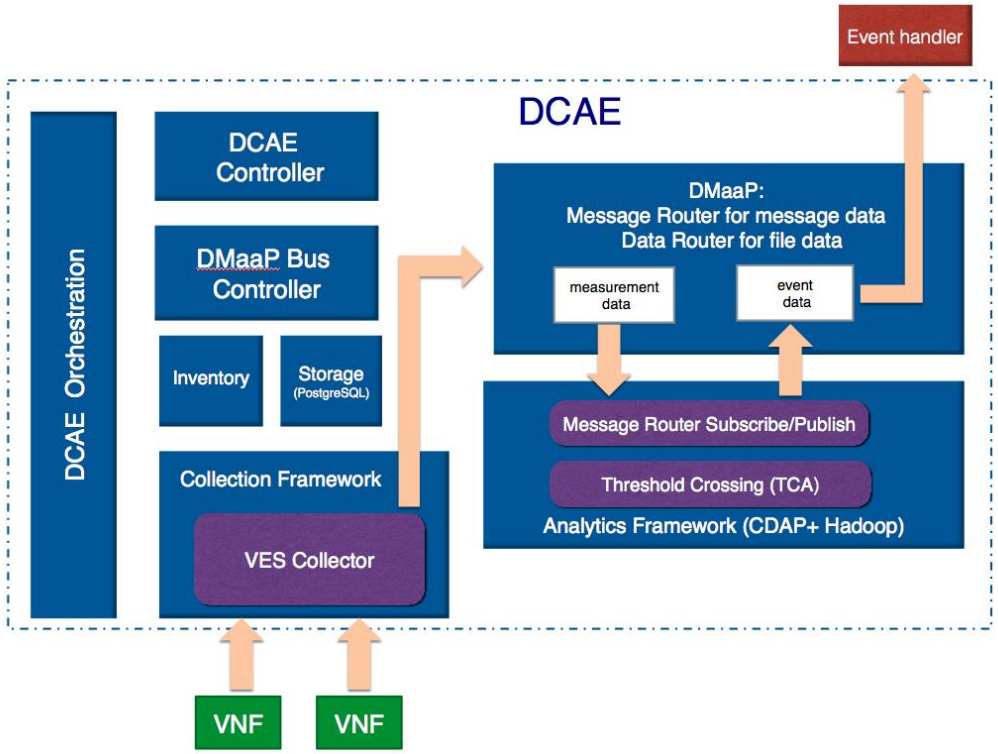
DCAE Integration | metric function

- SD-Core has a built-in metricfunc which upstreams data into Kafka
- Send data from VNFs to Kafka, upstream consumer subscribes to specific topics
- Database or stream



DCAE Integration | Data Flow

- Data is housed and processed within DCAE
- Data persistence and routing all done within ONAP
- Any service can use/subscribe to data store



LF NETWORKING

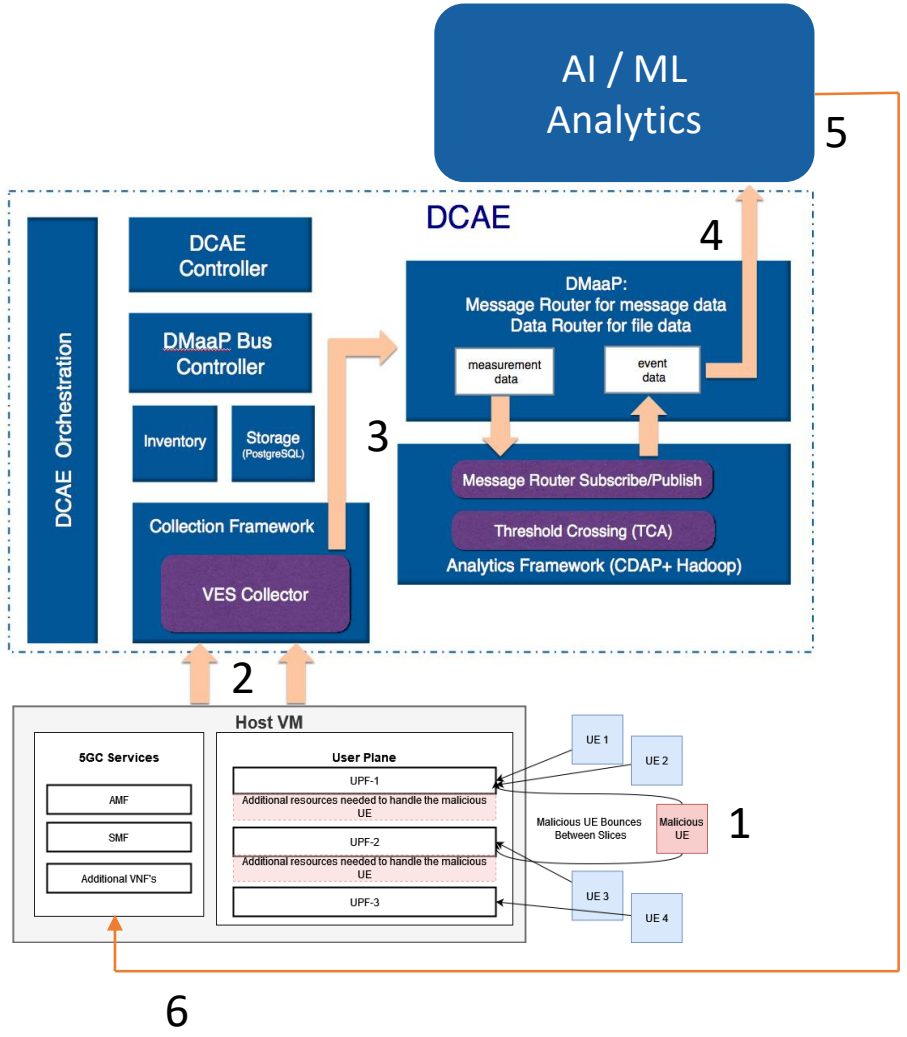
LFN Developer & Testing Forum

Background
Problem Motivation
Slice Threat Modeling
SD-Core and Data Generation
DCAE
Closing the Loop

Yatis K. Dodia

ML for 5G Cybersecurity

1. Threat actor on the network
2. Data and Event Generation
3. Data Collection
   - Scale
   - Machine speed
4. Data Packaging and Transport
5. AI/ML Analytics
6. Feedback into Network
   - Detection / Alert
   - Mitigation Actions



Community Feedback

- Cybersecurity Discussion
  - How can open-source tools, such as ONAP, increase use cases for cybersecurity research / modeling?
  - Data collection and analytics facilities are helpful
  - Support for PyTorch (also part of LF…)?

- How would you handle distributed, large-scale data?
  - Centralized AI/ML?
  - What about federated or distributed learning?