



Security Testing & Monitoring of 5G Networks

Vinh La, Ana Cavalli, Edgardo Montes, Wissam Mallouli, Zujany Salazar, HUU-Nghia Nguyen

TAROT-2022 Ávila
08 July 2022

Plan

- **Introduction**
- How do we see Network Monitoring?
- Security Testing & Monitoring of 5G Networks

Montimage



Key information of the company :

Type: SME

Creation date : 2004

Location: Paris, France

Employees : 12

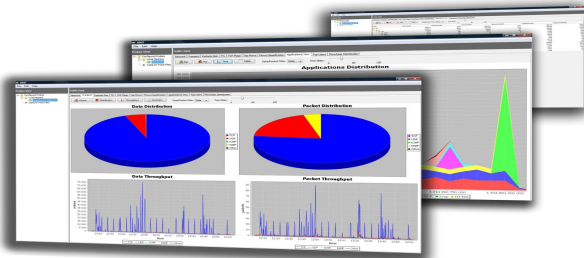
Expertise

- Network Monitoring and analysis
 - Classification of network traffic, Statistics, QoS/QoE
 - Incidents detection: behaviour, security and performance
- Research and innovation in different fields related to future networks, cloud computing, IoT, 5G, cybersecurity and quality assurance etc.
- Flagship tool: Montimage Monitoring Tool (MMT)



Activity :

Analysis of network traffic – supervision, detection, decision making, reactions



Personal Background

- PhD researcher / Project Manager
- Expertise in Cybersecurity
 - IoT/ WSN/ 5G
 - Evasions
 - Honeypots
 - Anomaly Detection
 - Root-cause Analysis
- 6 years in Montimage:
 - H2020 European research projects (SISSDEN, FED4FIRE, ENACT, INSPIRE-5G+, SANCUS, SPATIAL, PRECINCT)
 - French R&D projects (SODIUM, TDS, MOSAICO)

Montimage's 5G-related projects

- [H2020-INSPIRE-5G+](#)
- [H2020-SANCUS](#)
- [ANR-MOSAICO](#)
- [H2020-SPATIAL](#)
- ANR-5GOpenRoad



INSPIRE-5Gplus

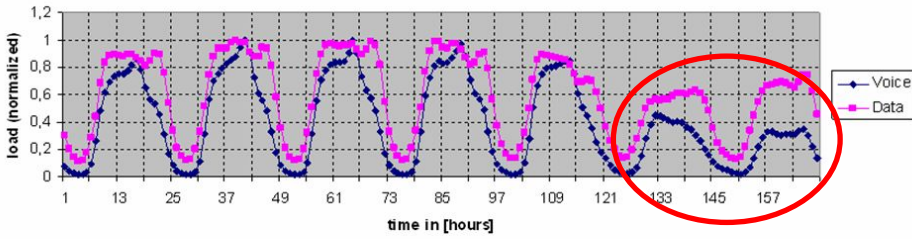


Plan

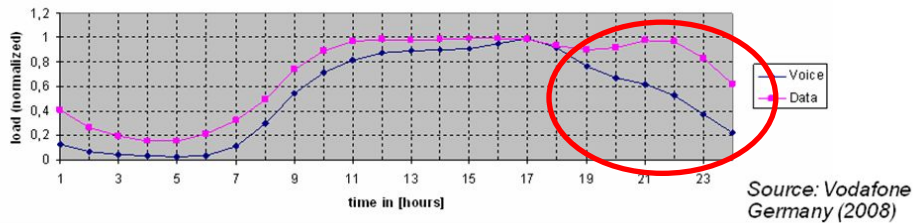
- Introduction
- **How do we see Network Monitoring?**
- Security Testing & Monitoring of 5G Networks

Need for Network Monitoring Understand / Plan

One Week

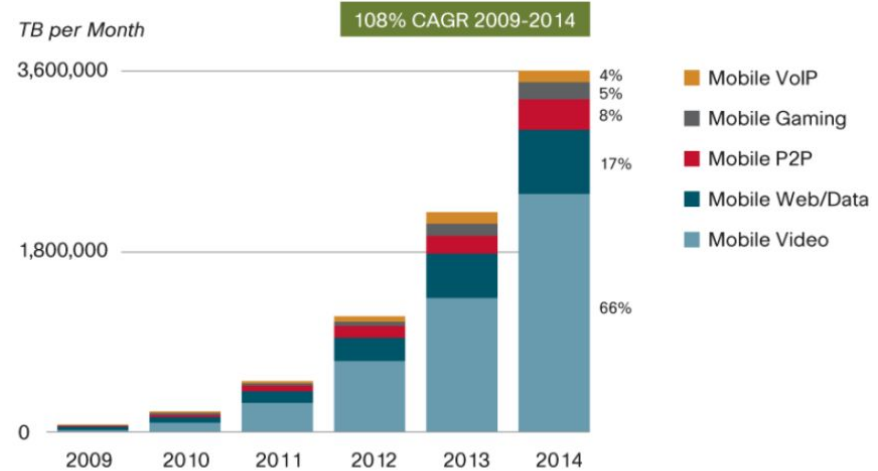


One Day



- Need to have a clear visibility over the network
- Status, traffic trends, peak time, evolution, etc.

TB per Month



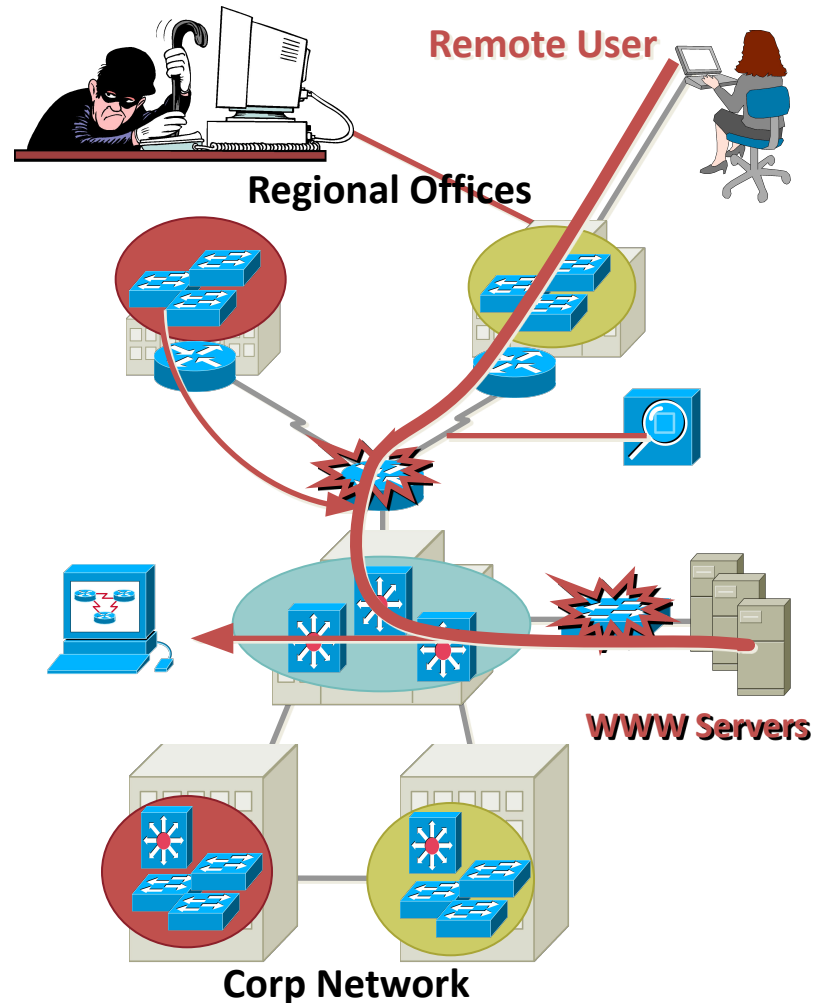
Source: Cisco VNI Mobile, 2010

- 3.5 billion mobile broadband users by 2015
- Traffic increase 30 times (wrt 2010)
- Understanding
 - the drivers of this growth
 - applications/usages
 - contribute for a successful network planning

Need for Network Monitoring

Diagnose & react

- Typical problem
 - Remote user arrives at regional office and experiences slow or no response from corporate web server
- Where to begin?
 - Where is the problem?
 - What is the problem?
 - What is the solution?
- Without proper network monitoring, these questions are difficult to answer

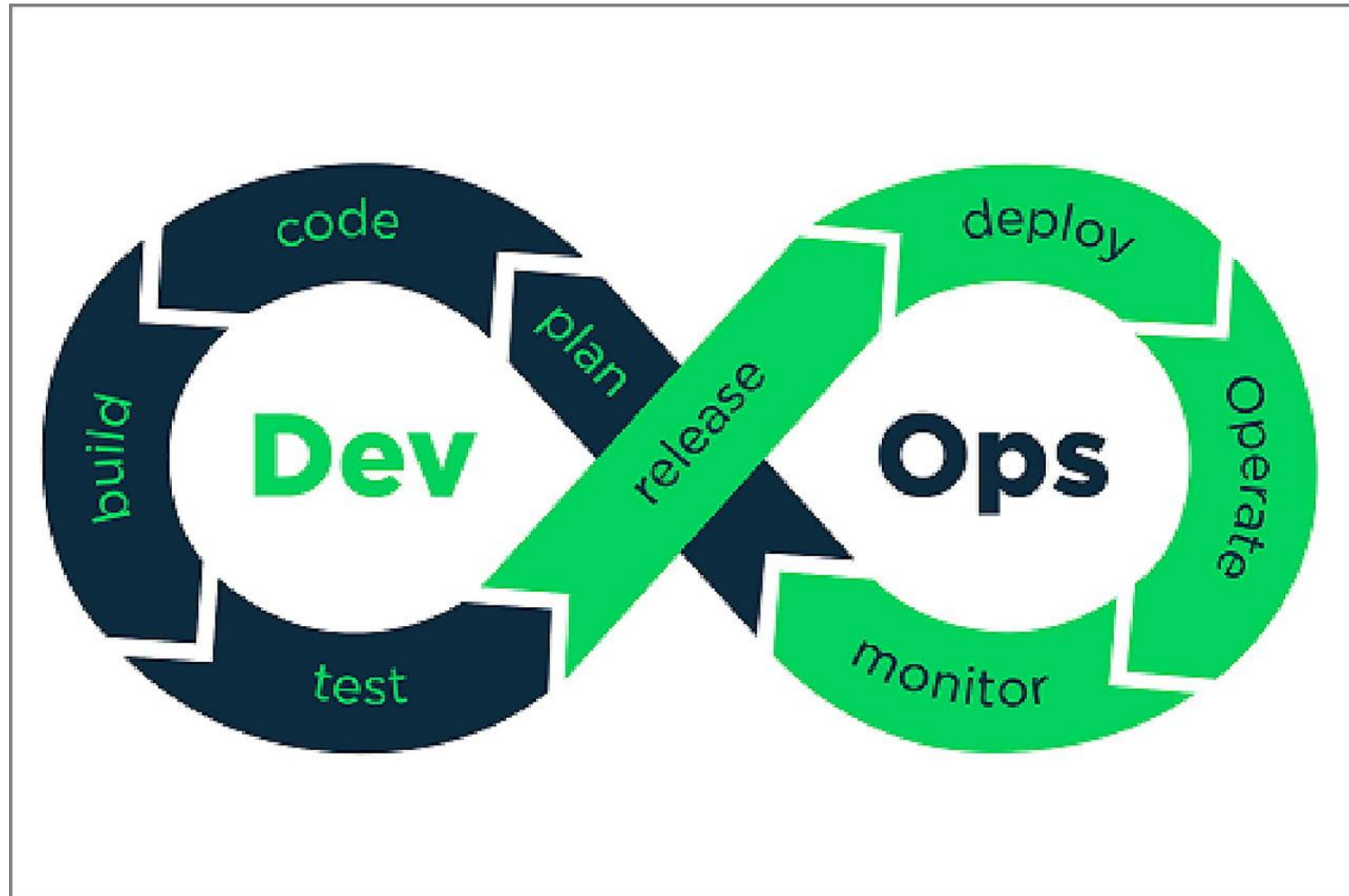


What is Network Monitoring?

- Process of observing or inspecting the network at different points
- With the objective of
 - Drawing operation baselines
 - Produce reports
 - Notify on abnormal operation
 - Provide input to network management
- Can be used to
 - Understand the behavior of the network
 - Detect faults and abnormal operation
 - Network planning & resource optimization
 - Network security (Intrusion & Attack Detection)
 - Performance, quality & SLA monitoring



DevOps model



Network Monitoring: Basics

Monitoring application

- Interface for real-time monitoring.
- Store collected data in a database for post analysis (trends, history, reporting ...).

Performance analysis unit

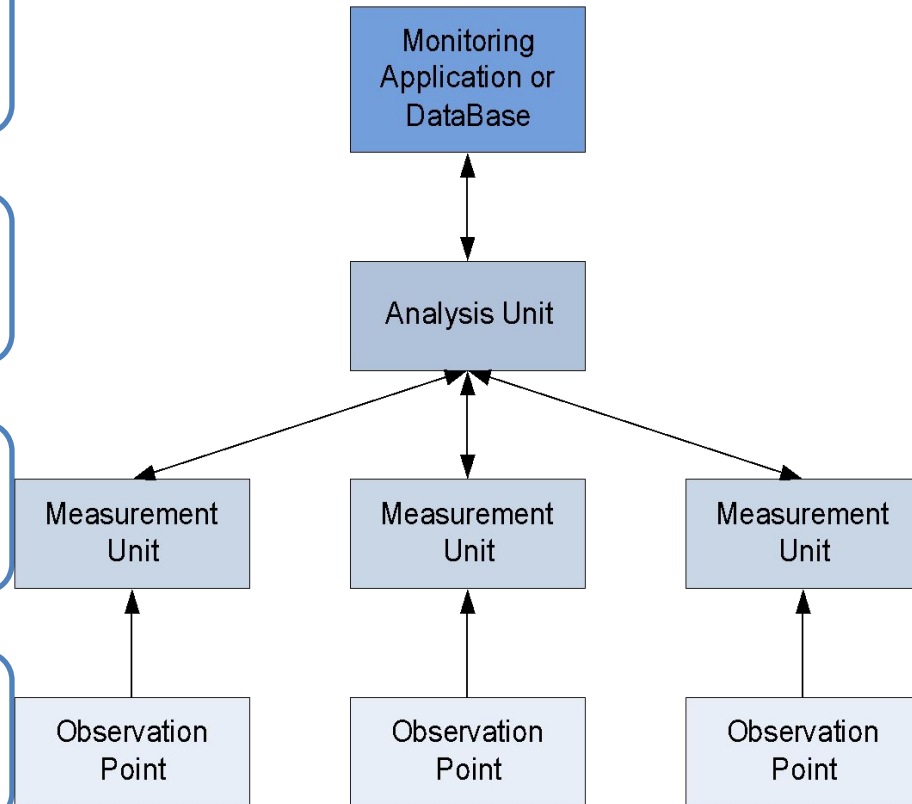
- Gathers, aggregates and correlates collected measures
- Calculate indicators (QoS parameters, KPIs).

Measurement unit

- This performs the measurements
- Collects the required information for analysis.

Observation points

- This is where the measurements will be performed.
- The more observation points we have, the more accurate data we get.



Determining *What* to Measure

- Before any measurements can take place one must determine what to measure
- Definition of metrics is closely related to the monitoring objective
- There are many commonly used network performance metrics
 - CAIDA Metrics Working Group (www.caida.org)
 - IETF's IP Performance Metrics (IPPM) Working Group

Determining *What* to Measure

- Example: Performance metrics can be classified into
 - Network metrics
 - Latency
 - Throughput
 - Arrival rate
 - Link utilization, bandwidth
 - Loss rate
 - Application metrics
 - Response time
 - Connection setup time
 - Availability
 - User quality metrics (depends on the application)
 - Mean opinion score (VoIP)
 - Quality of experience (Video)

Determining *How* to Measure

- Active measurements



- Passive measurements



Determining *How* to Measure

- Active measurements

- Send test traffic into the network

- Generate test packets periodically or on-demand
 - Measure performance of test packets or responses

- Popular tools

- Ping: RTT and loss
 - Traceroute: path and RTT

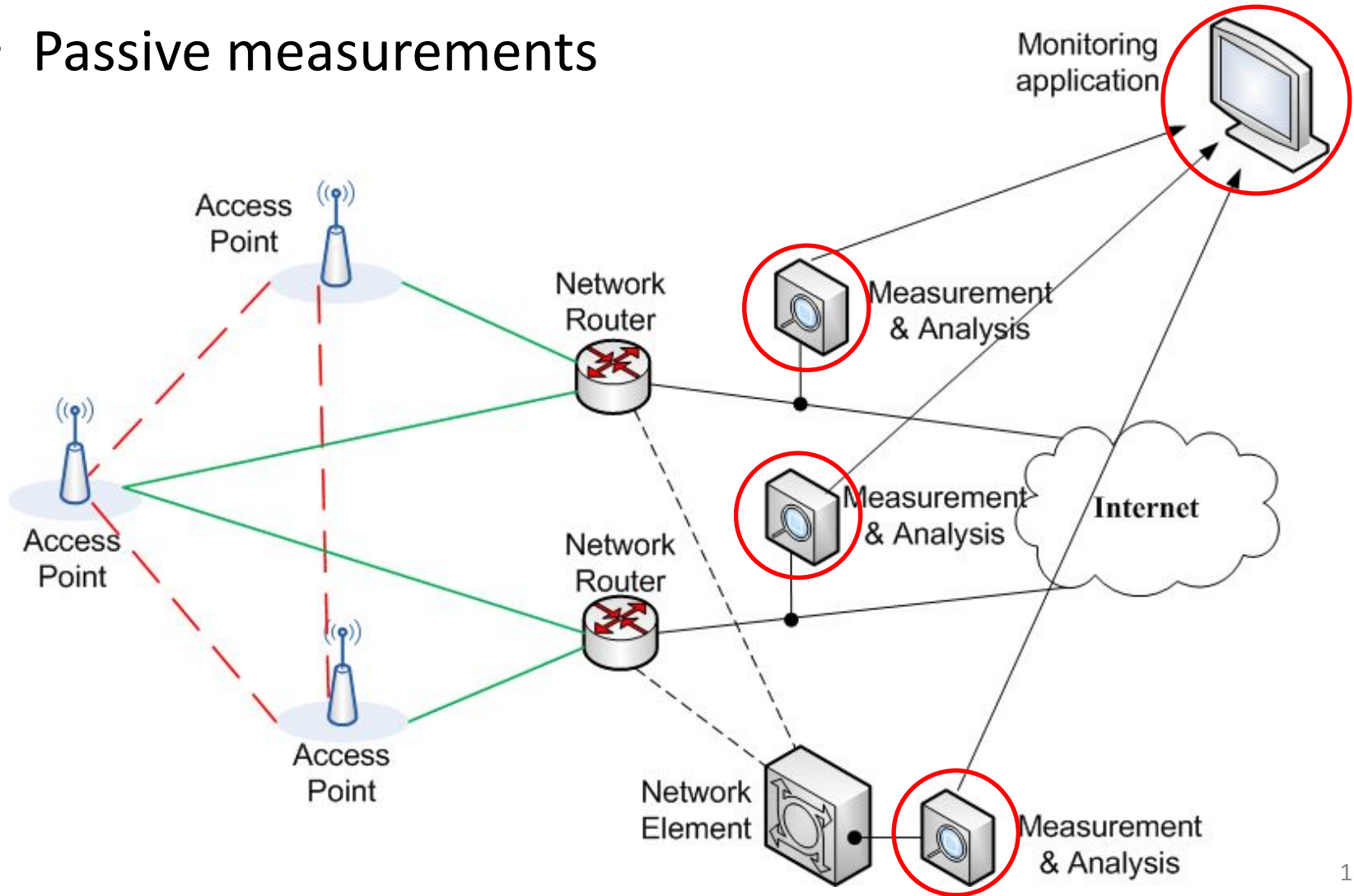
- Problems:

- Impose extra traffic on network and distort its behavior in the process
 - May impact the behavior of the network (self interfering)



Determining *How* to Measure

- Passive measurements

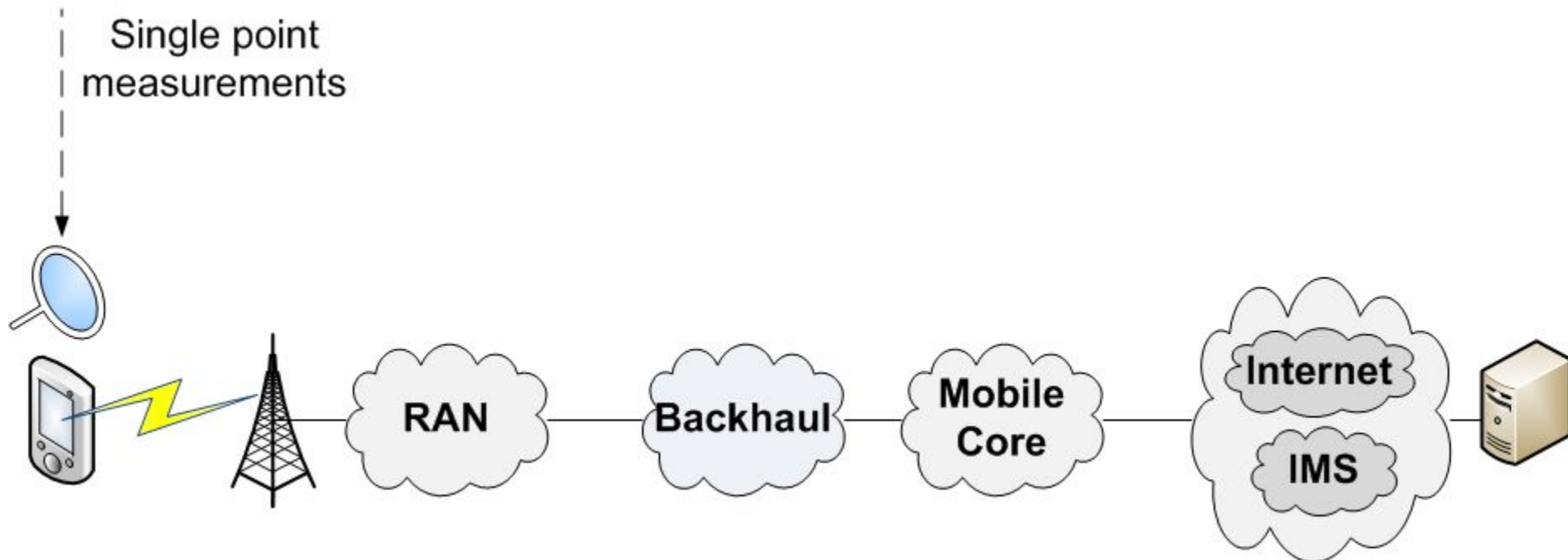


Comparison of active/passive measurements

	Active measurements	Passive measurements
Configuration	Multi-point	Single or multi-point
Data size	Small	Large
Network overhead	Additional traffic	No additional traffic
Purpose	Delay, packet loss, availability	Throughput, traffic patterns, trends & detection
CPU Requirement	Low to Moderate	High

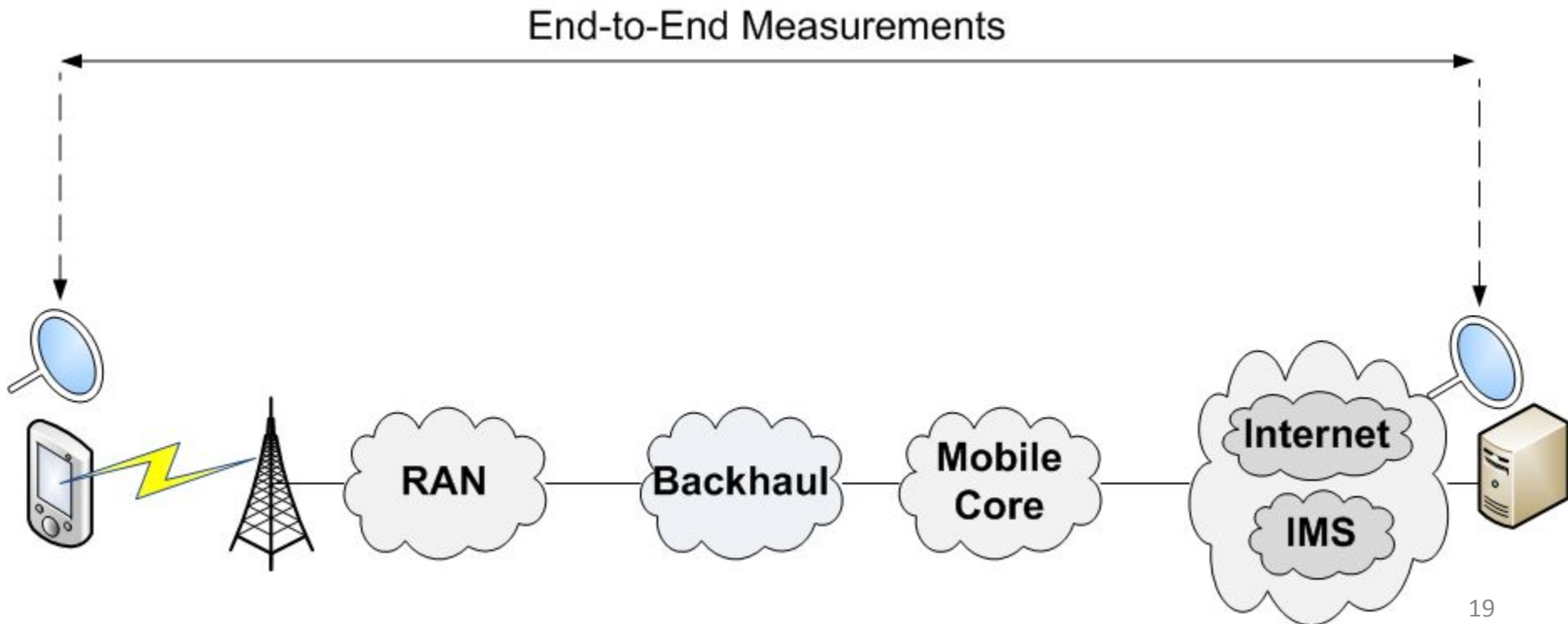
Determining *Where* to Measure

- Single point measurements
 - Provide partial view of the network



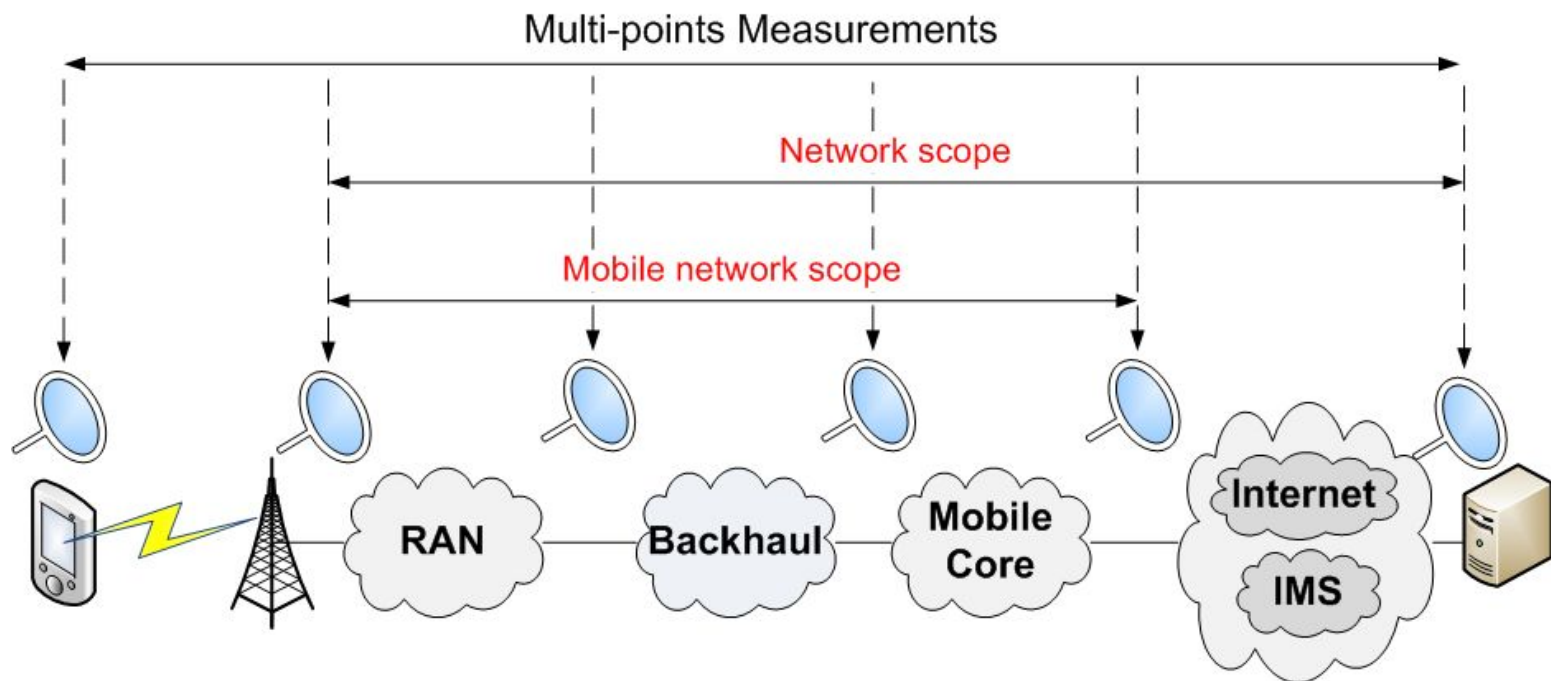
Determining *Where* to Measure

- End-to-end measurements
 - Provide a view on the performance between the the end points



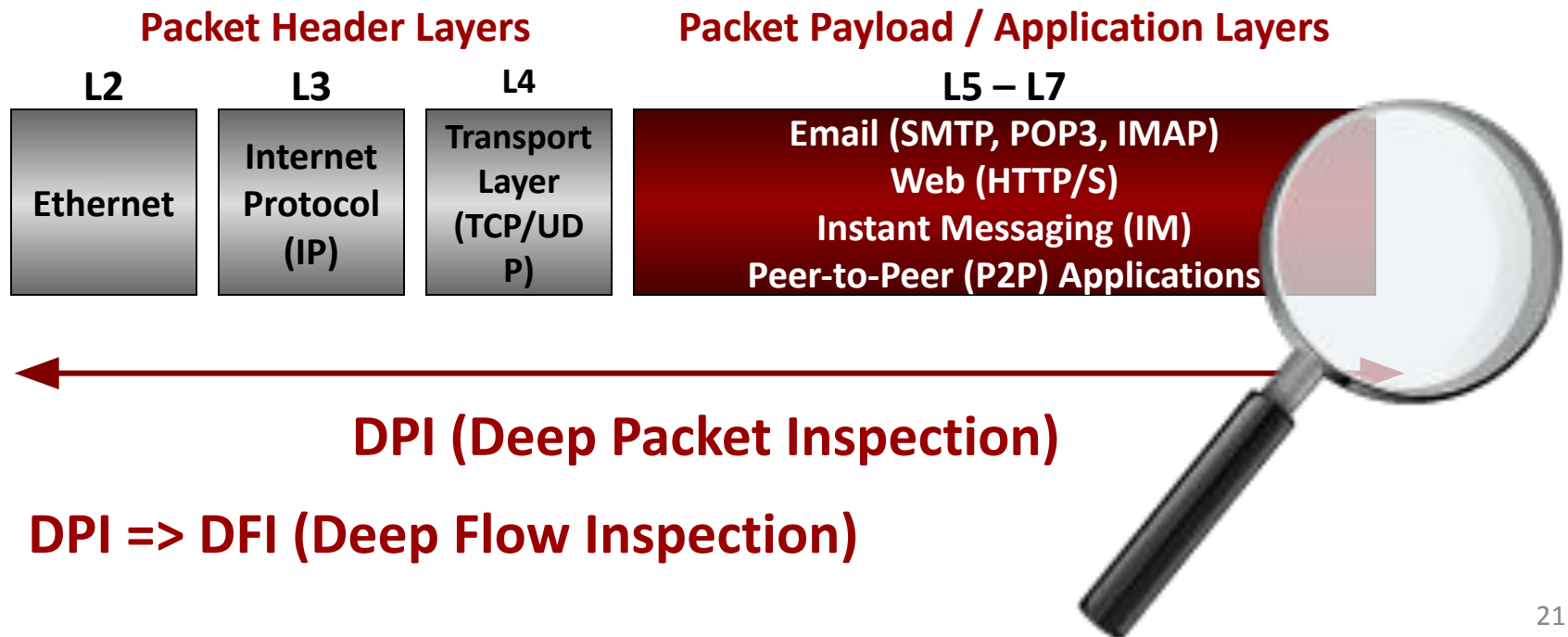
Determining *Where* to Measure

- Multi point measurements
 - Provide a view on the performance in the different “monitored” segments of the network

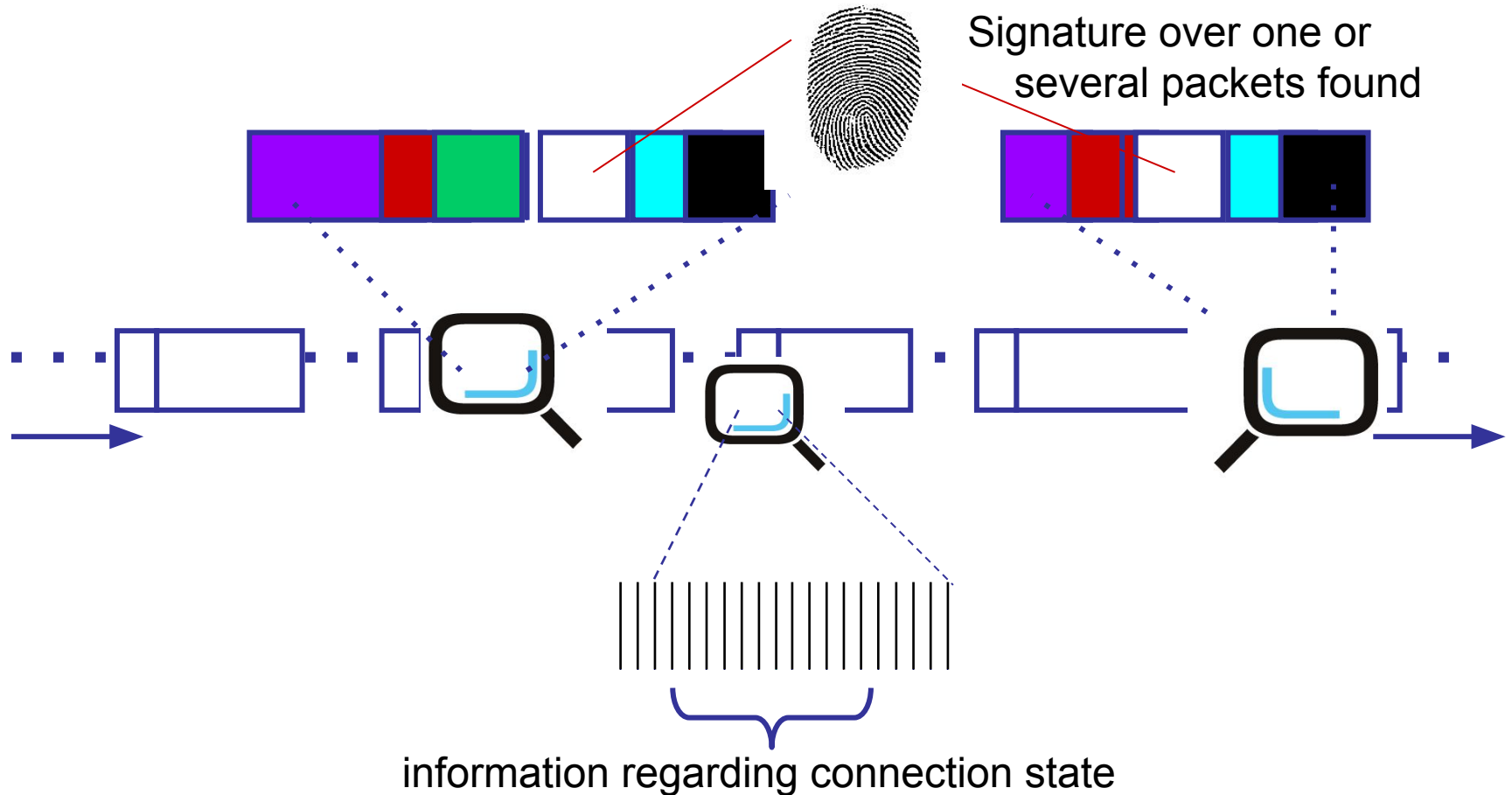


DPI/ DFI

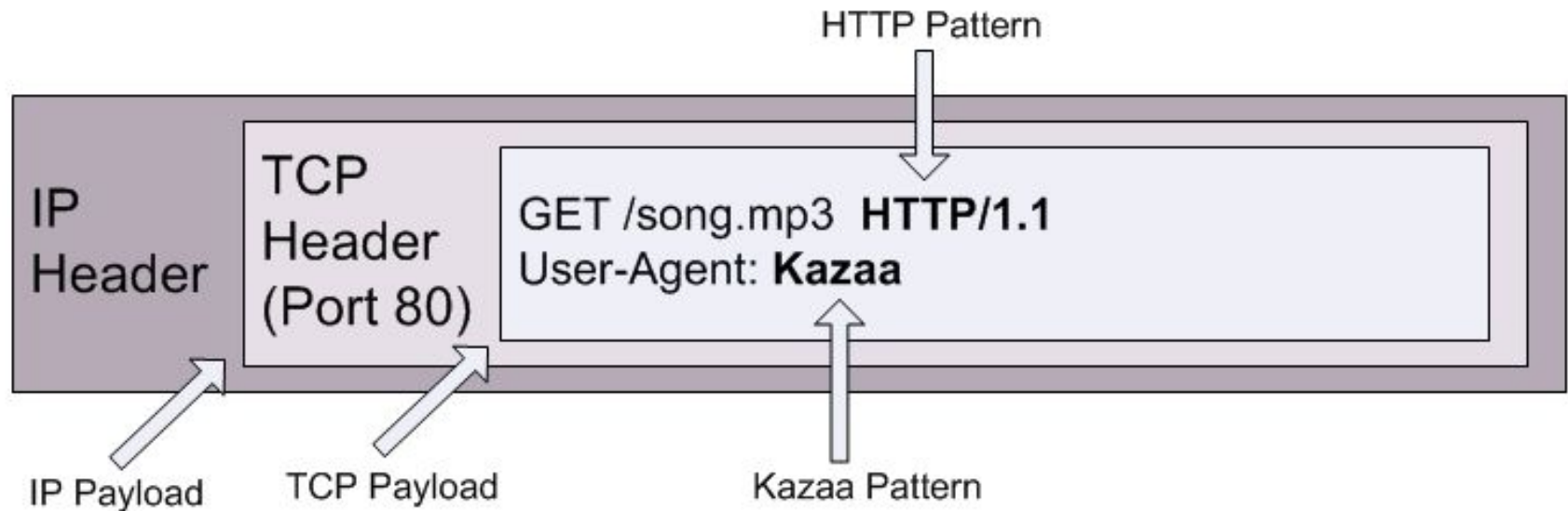
- Technology consisting of digging deep into the packet header and payload to “inspect” encapsulated content
 - Content may be spread over many packets



DPI/ DFI & Pattern Matching



Analysis by Pattern Matching



- Problems:

- Signatures need to be updated frequently
- Evasion techniques
- Encrypted traffic

Behavior and statistical analysis

- Many protocols have statistical and behavioral “signatures” that are not related to the data contents:
 - Packet size
 - Inter-arrival delay
 - Specific exchange that can be assimilated to a state machine
- Example
 - Very close inter-arrival delays with low deviation from the average (VoIP)
- Effective when application uses **encryption or obfuscation**
 - Access to the payload is not possible
 - Classification in the dark

ML and AI

- Needed for encrypted traffic
- Relies on packets and flows metadata
- Clustering algorithms, Bayesian Networks, Neural Networks and many others
 - For classification
 - Legitimate vs malicious
 - Human vs machine generated
 - User profiling
 - Etc.

Montimage Monitoring Tool

- Modular monitoring solution that allows to detect behavior, security, performance incidents based on a set of properties
- Easy to extend
 - Developer & User documentation
 - Plug-in architecture (TCP/IP protocols and apps, IoT-6LoWPAN, 5G, etc,)
- Advantageous support to Research/ Academic institutions



More info: <https://www.montimage.com/products>

Plan

- Introduction
- How do we see Network Monitoring?
- **Security Testing & Monitoring of 5G Networks**
 - **5G Principles**
 - MMT solutions
 - Practical 5G use cases

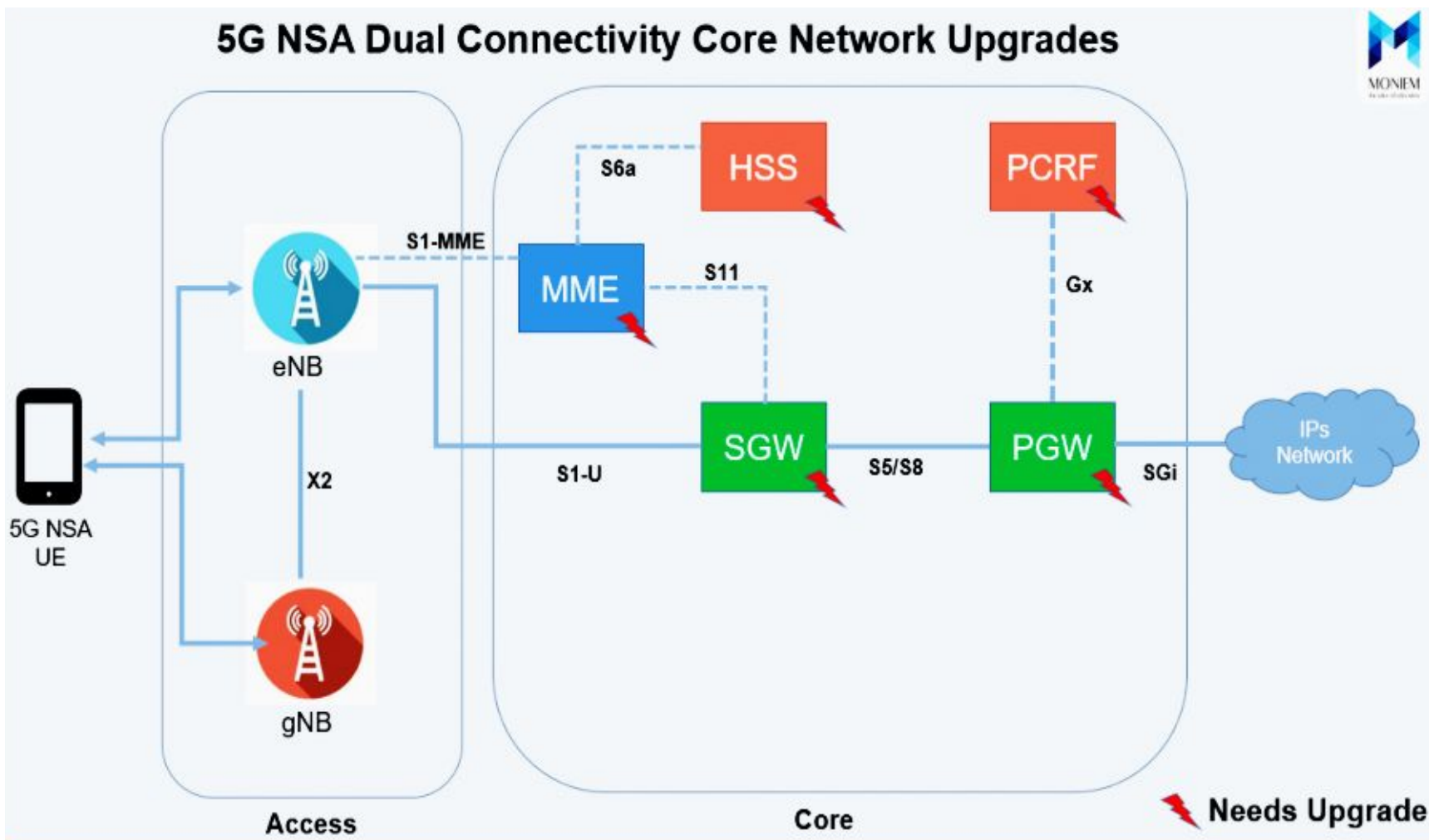
5G

- Massive growth in data and connectivity
- Ultra-reliable low latency
- Enhanced mobile broadband



Source: <http://www.emfexplained.info/?ID=25916>

5G NSA and SA

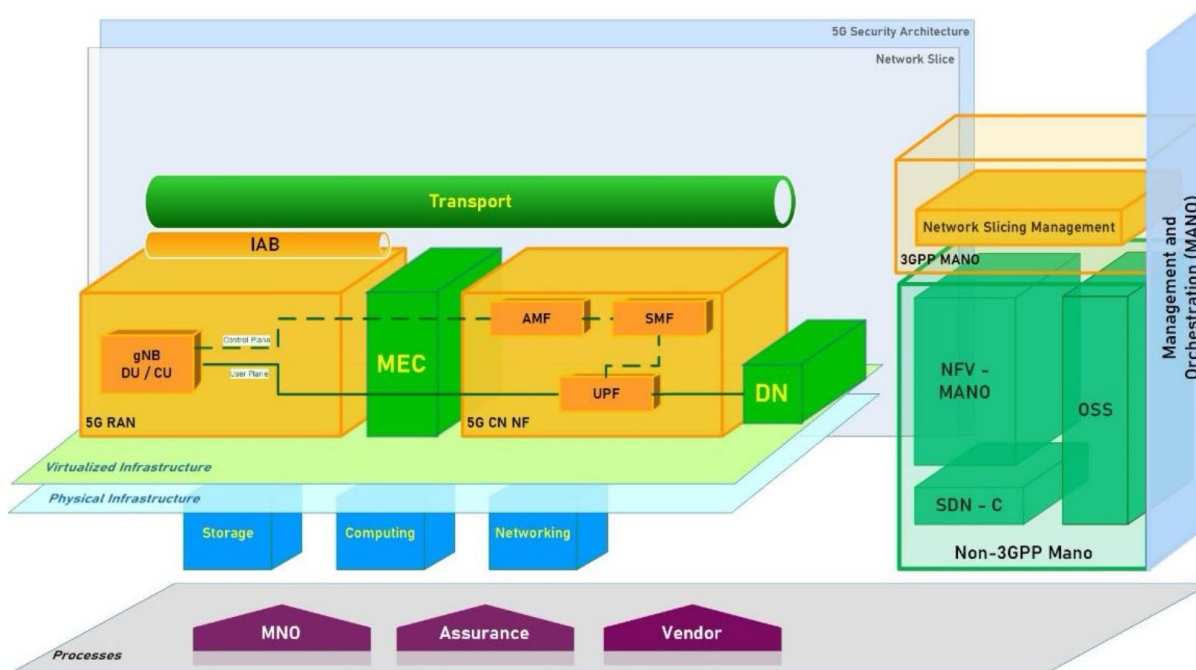


Overview: 5G implementation

- 5G Commercial:
 - First 5G launched in April, 2019: South Korea (first 5G mobile), USA (first 5G network)
 - France: 1st release in December 2020
 - June 2020: 8867 cities + 124 operators
(<https://www.speedtest.net/ookla-5g-map>)
 - Mostly Non-Standalone Architecture (NSA-5G)
 - Several Standalone Architecture (SA-5G)

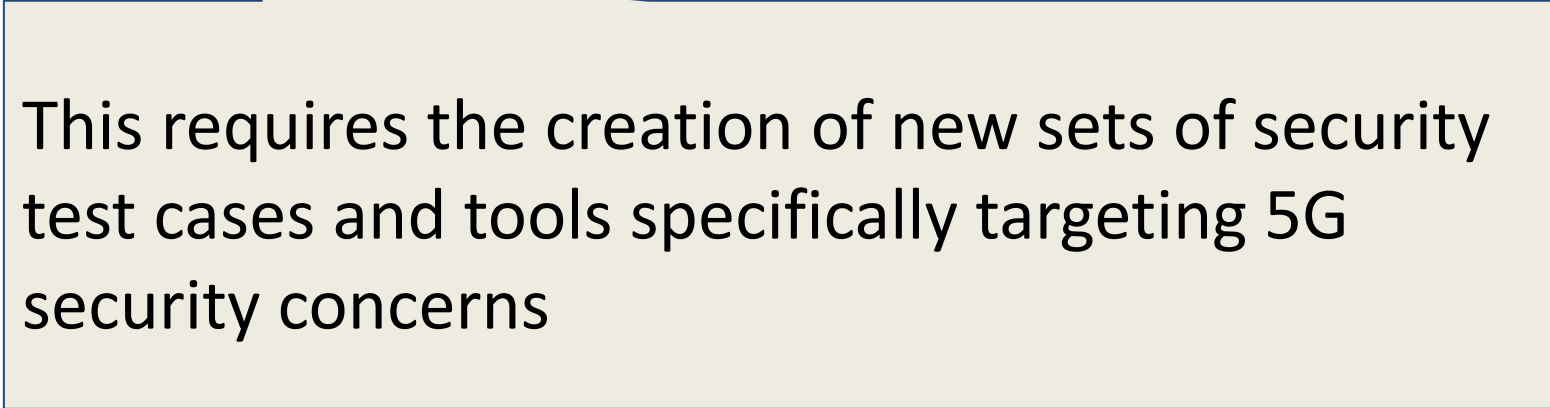
5G enabling technologies

- Software Defined Networks (SDN)
- Network Functions Virtualization (NFV)
- Mobile Edge Computing (MEC)
- Network Slicing (NS)



5G security challenges

- 5G new technologies require to be tested (functional and non-functional)
- New 5G protocol = New traffic to be decoded
- New cybersecurity threats
- Previously adopted security and privacy mechanisms become ineffective



This requires the creation of new sets of security test cases and tools specifically targeting 5G security concerns

Plan

- Introduction
- How do we see Network Monitoring?
- **Security Testing & Monitoring of 5G Networks**
 - 5G Principles
 - **MMT solutions**
 - 5Greplay: 5G (Security) Testing
 - MMT-5G: 5G traffic decoding
 - MMT-TaS: Simulation and Test
 - MMT-RCA: ML-based Anomaly Detection and Root-cause Analysis
 - Practical testbeds and use cases

5Greplay

Documentation and tutorials: <http://5greplay.org>

Page 18 of 29

Scenario 2: NAS-5G SMC Replay attack

Objective

Perform **security tests** by modifying and injecting network traffic into a specif target. Test proposed in the **3GPP TS33.512** [2].

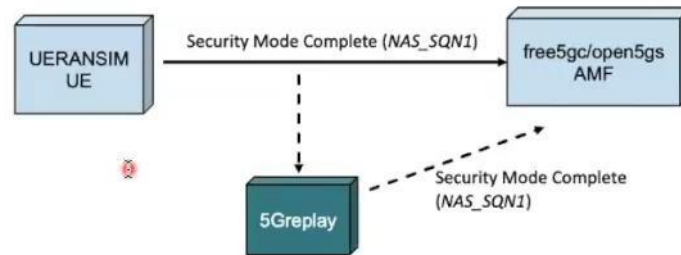


Figure 5: Sending malformed NGAP packets against free5GC

MMT-5G

- Development of new plugins to understand and to decode 5G traffic (e.g., GTPv2, NGAP, NAS-5G)
- Edition of new MMT-Security rules to detect 5G security threats.
- Example: Raise an alert if an "Authentication Request" comes after a "Registration Request" less than 1ms, e.g., the interval should be $> 1\text{ms}$ due to calculation time of 5G core.

```
1 <beginning>
2 <property value="THEN" delay_units="ms" delay_min="0" delay_max="1" property_id="101" type_property="ATTACK"
3   description="5G testing">
4   <event value="COMPUTE" event_id="1"
5     description="registration request"
6     boolean_expression="((ngap.procedure_code == 15) &&& (nas_5g.message_type == 65))"/>
7   <event value="COMPUTE" event_id="2"
8     description="Authentication request"
9     boolean_expression="(((ngap.procedure_code == 4) &&&(nas_5g.message_type == 86)) &&&(ngap.ran_ue_id == ngap.ran_ue_id.1))"/>
10 </property>
11 </beginning>
```

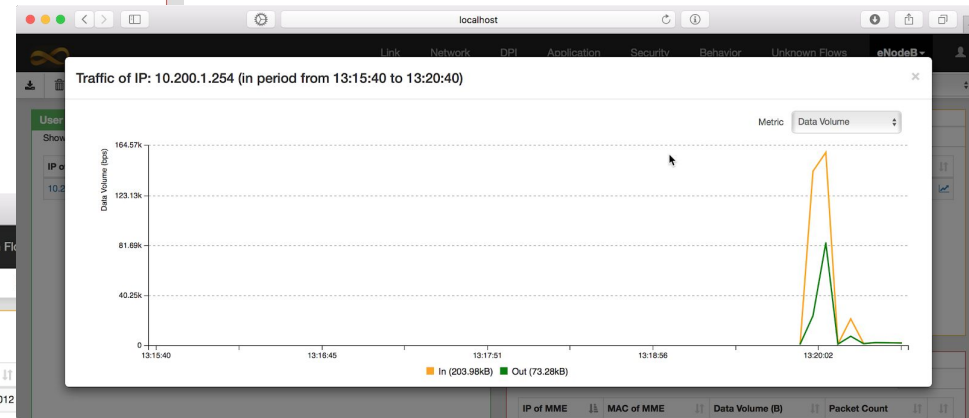
MMT-5G

The screenshot displays the MMT-5G dashboard interface. At the top, there are navigation tabs: Link, Network, DPI, Application, Security, Behavior, and Unknown Flows. The 'Security' tab is active, and the 'Auto reload' toggle is set to 'ON'. A dropdown menu shows 'Network Topology' and 'Traffic Monitoring'. The main area features a network topology diagram with nodes labeled 1 through 10. Below the topology, there are three data tables: 'User Plane', 'Control Plane: eNodeB', and 'Control Plane: MME'. The 'User Plane' table shows traffic for IP 10.200.1.254. The 'Control Plane: eNodeB' table shows traffic for IP 172.16.0.2. The 'Control Plane: MME' table shows traffic for IP 172.16.0.1.

IP of UE	Data Volume (B)	Packet Count	TEID Count
10.200.1.254	277252	518	3

IP of eNodeB	MAC of eNodeB	Data Volume (B)
172.16.0.2	00:0f:bb:ef:81:06	7012

IP of MME	MAC of MME	Data Volume (B)	Packet Count
172.16.0.1	00:0d:b9:43:3f:8d	7012	66



MMT-TaS

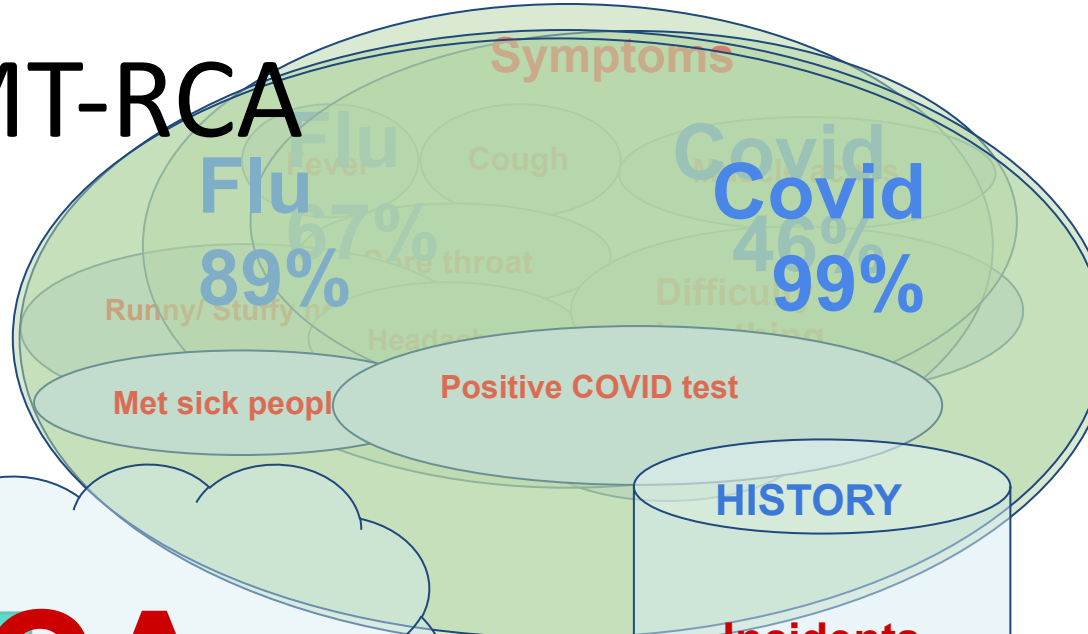
- Provide **simulated IoT/5G devices** for testing IoT/5G applications, especially **scalability**
- **Stressing the boundaries** of the scenarios to detect potential problems, such as denial of service (DoS) or low battery

MMT-RCA



Above the surface you see the **Symptoms** of the problem

Dig deeper to find the **Root Cause** of the problem



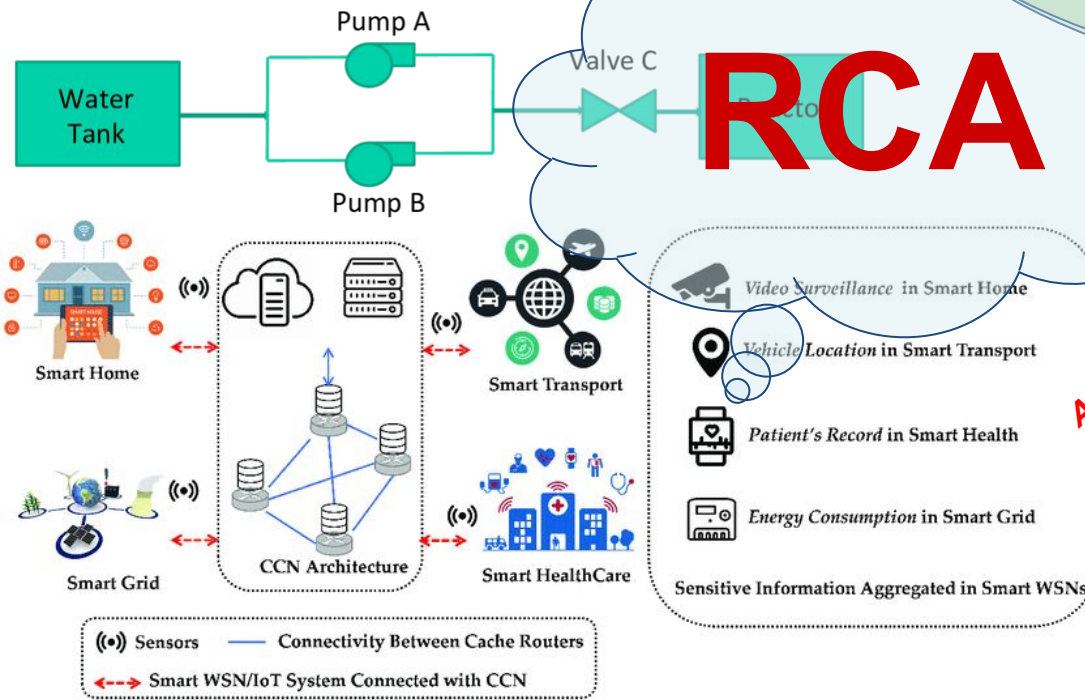
RCA

HISTORY

Incidents, Symptoms, Root-causes, Impacts, Remediations

Actively created incidents
Passively detected incidents
NEW! [Incident + Symptoms]

SIMILARITY



MMT-RCA

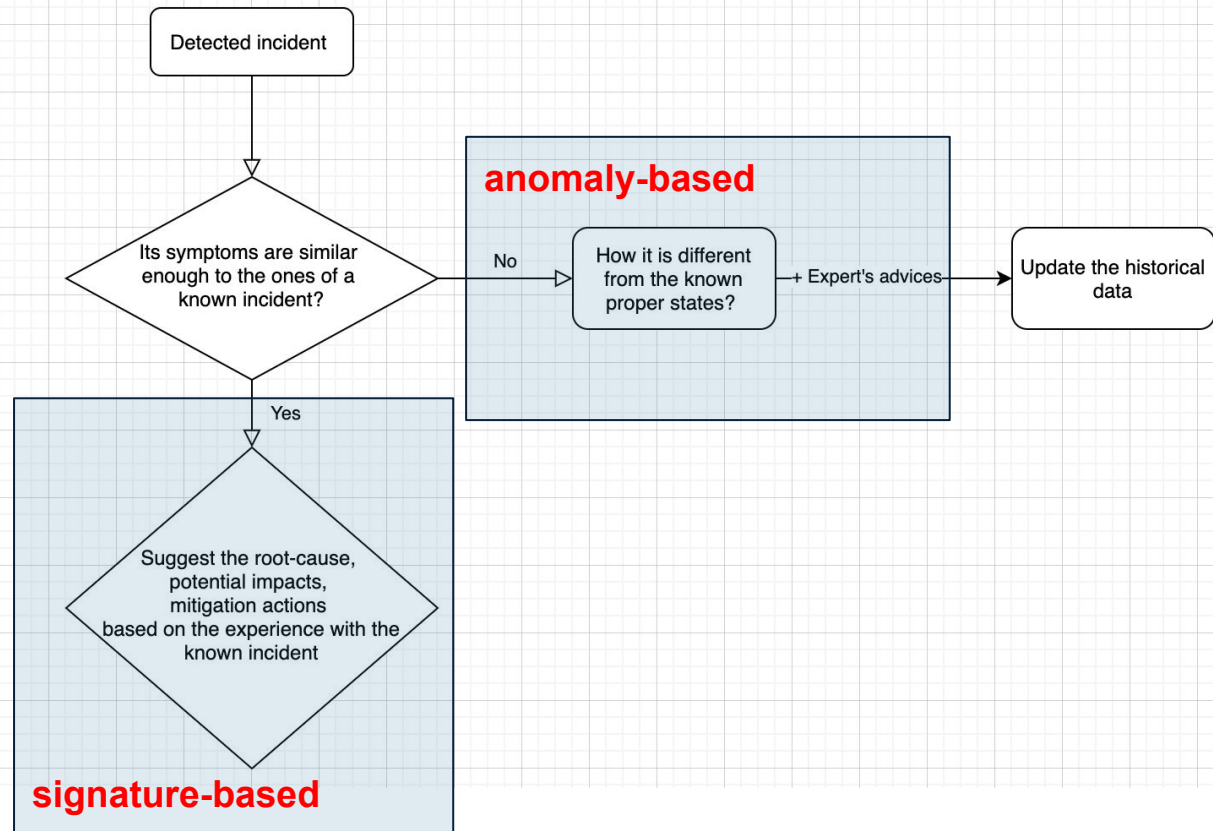
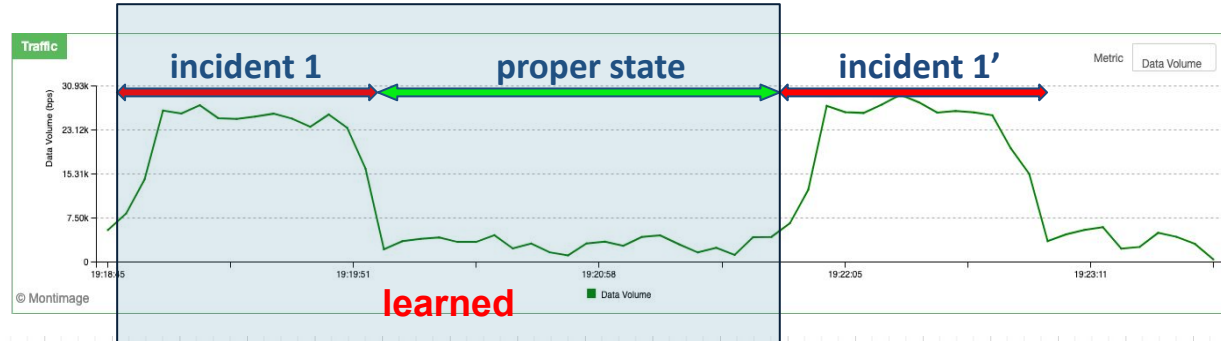
- **Signature-based:**

- Historical data of known incidents and their symptoms (observed in monitoring data)
+ known root causes
(~ **labelled** data)

- Similarity?

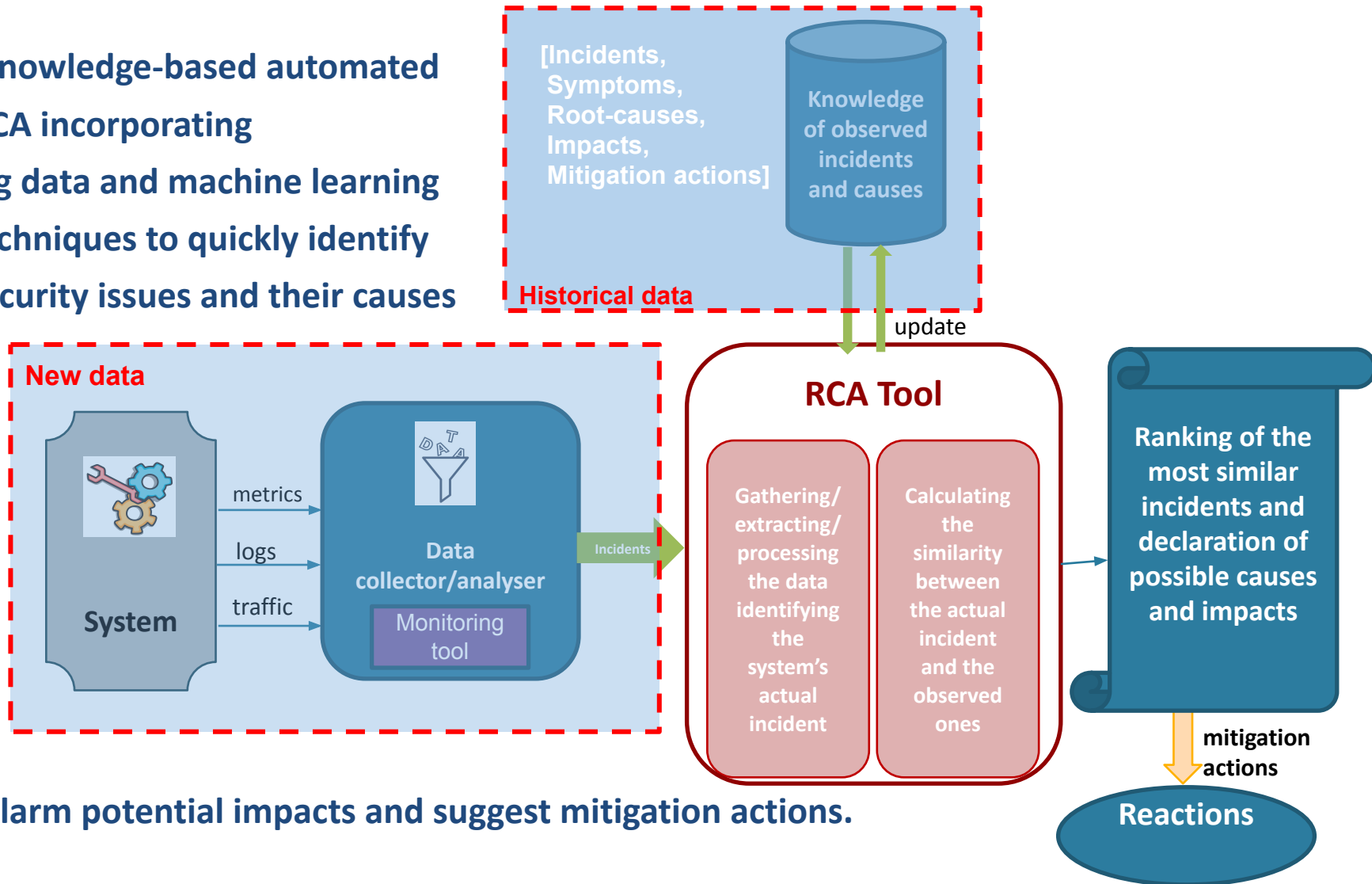
- **Anomaly-based:**

- Historical data of proper states
(~ **unlabelled** data)
- Dissimilarity? The change reflected in which metrics/ attributes?



MMT-RCA

- Knowledge-based automated RCA incorporating big data and machine learning techniques to quickly identify security issues and their causes



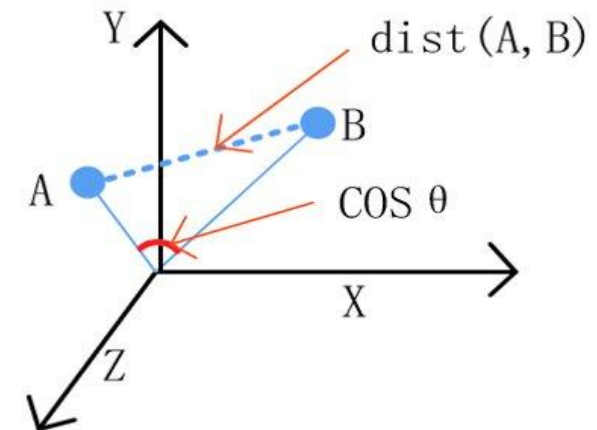
- Alarm potential impacts and suggest mitigation actions.

MMT-RCA

- **How to translate monitoring data to symptoms and vice versa?**
 - Heterogeneous data of different units / ranges:
=> Data normalization/ standardization
 - Data redundancy (noises/ too many dimensions):
=> Feature selection (5 selection models integrated)
- **How to measure similarity/dissimilarity between two sets of symptoms?**

The system's state can be characterized by a set of n attributes: $\langle a_0, a_1, \dots, a_n \rangle$, which can be represented by a vector in n -dimensional space.

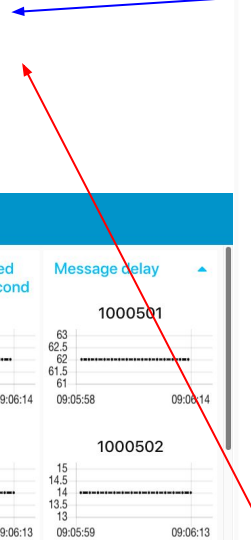
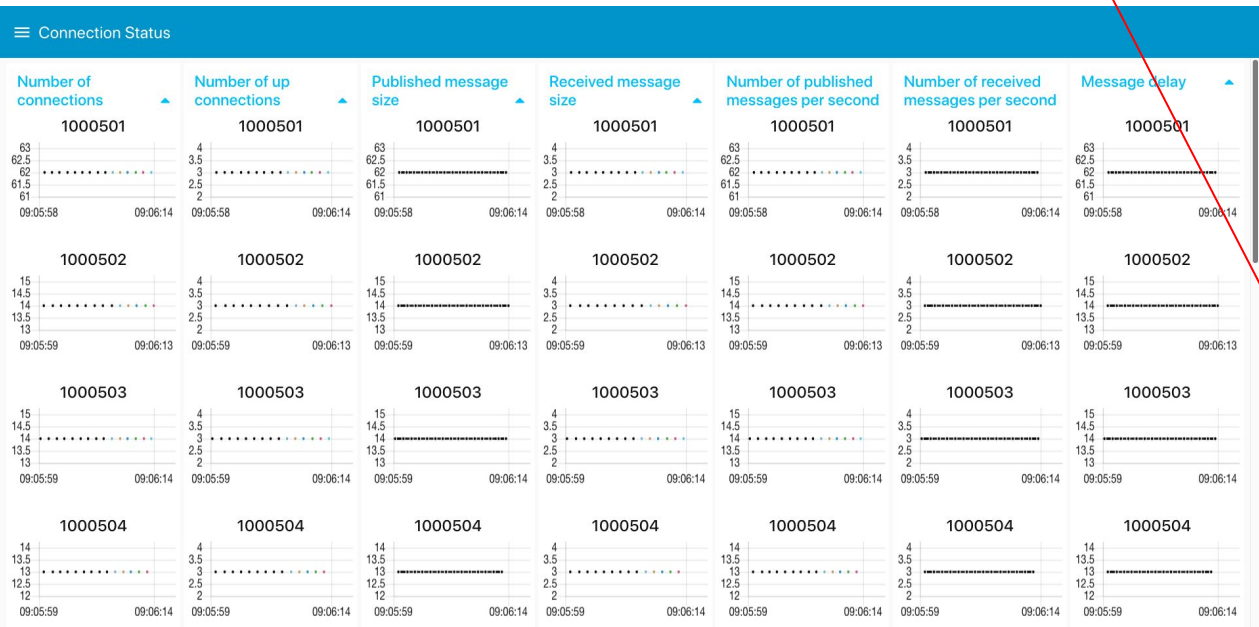
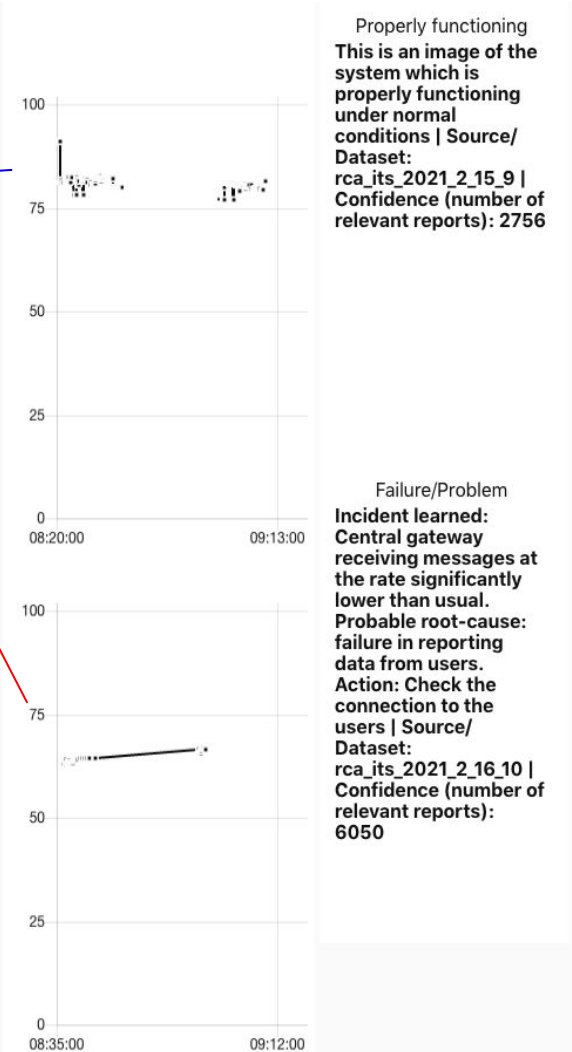
- Similarity/ Dissimilarity score calculation:
 - distance of **orientation** (the angle)
 - distance of **magnitude** (the length)



MMT-RCA

- Feature selection

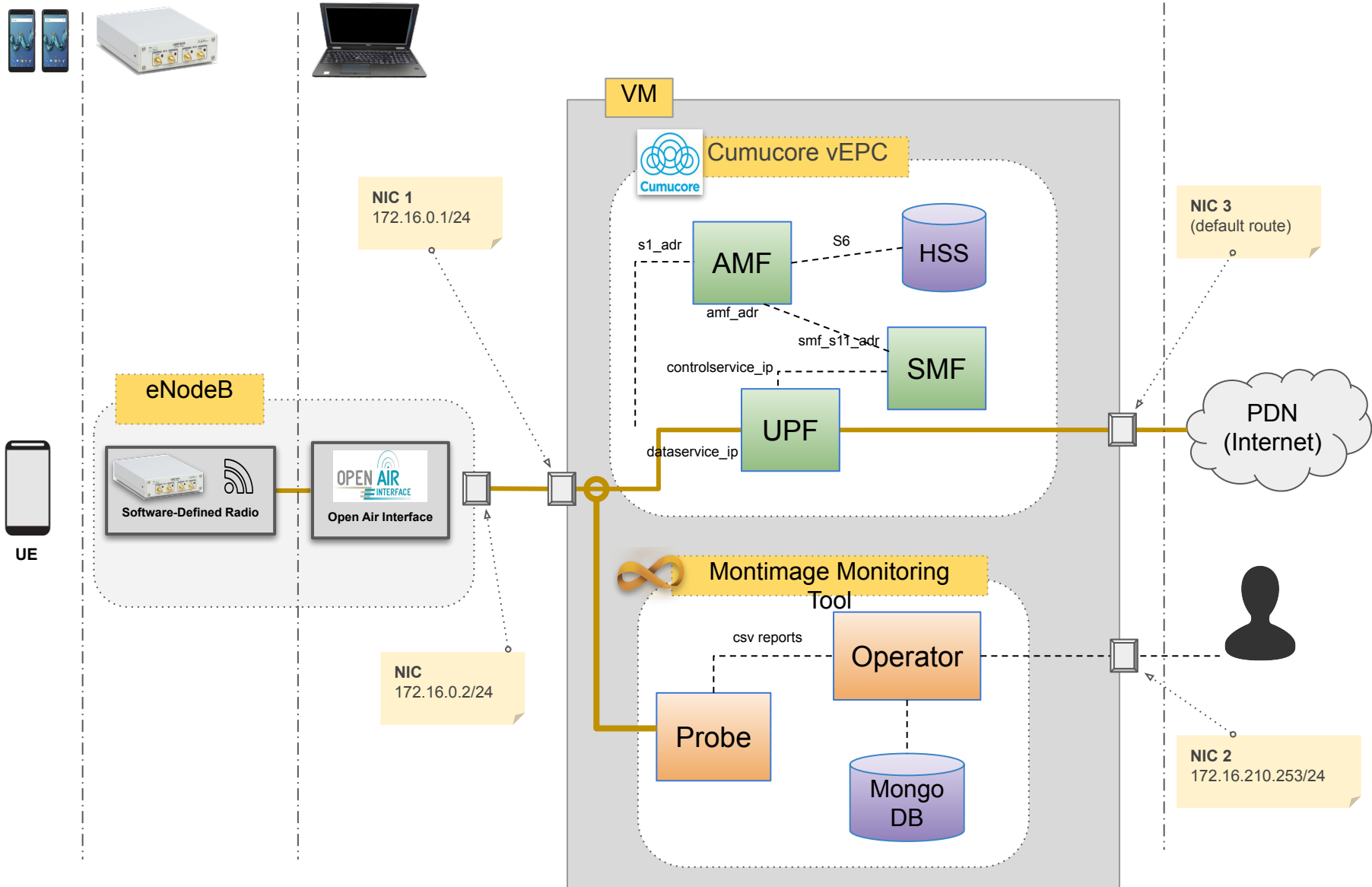
Which features are important for RCA?



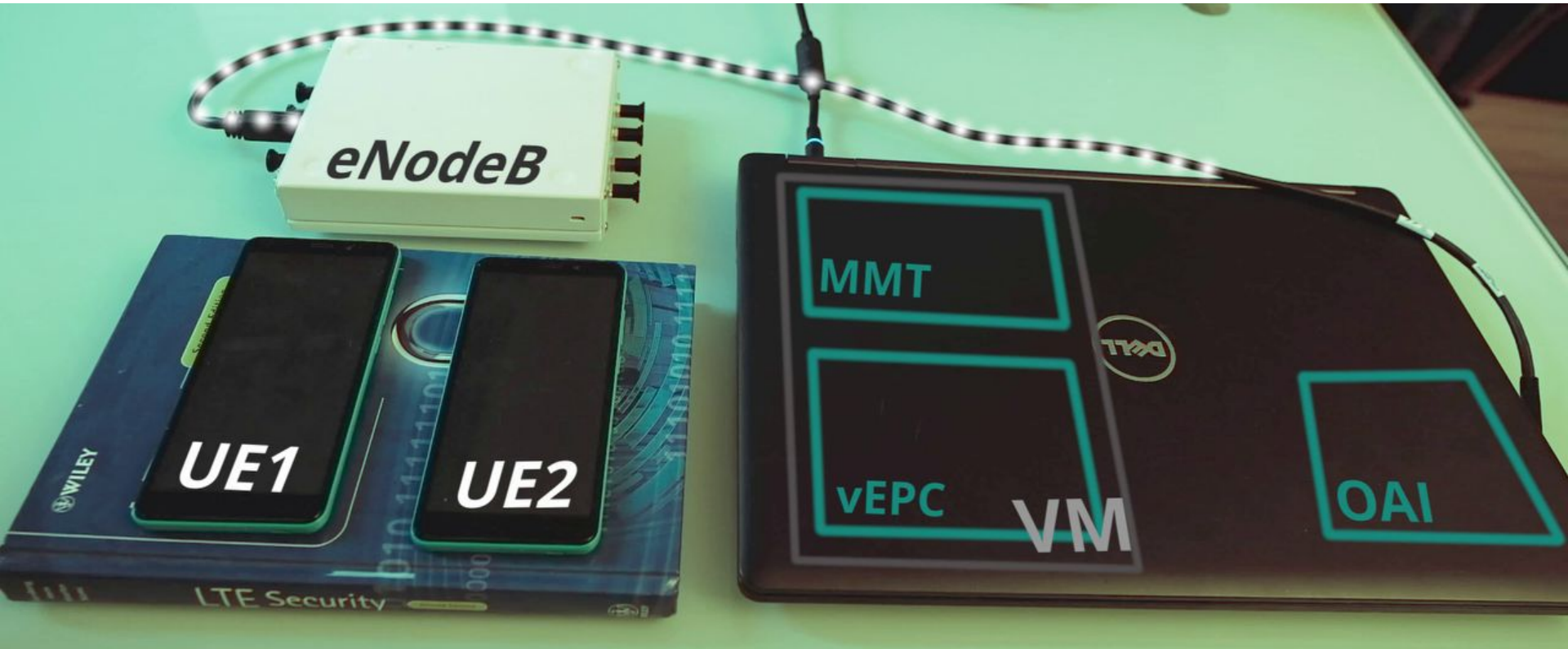
Plan

- Introduction
- How do we see Network Monitoring?
- **Security Testing & Monitoring of 5G Networks**
 - 5G Principles
 - MMT solutions
 - **Practical testbeds and use cases**

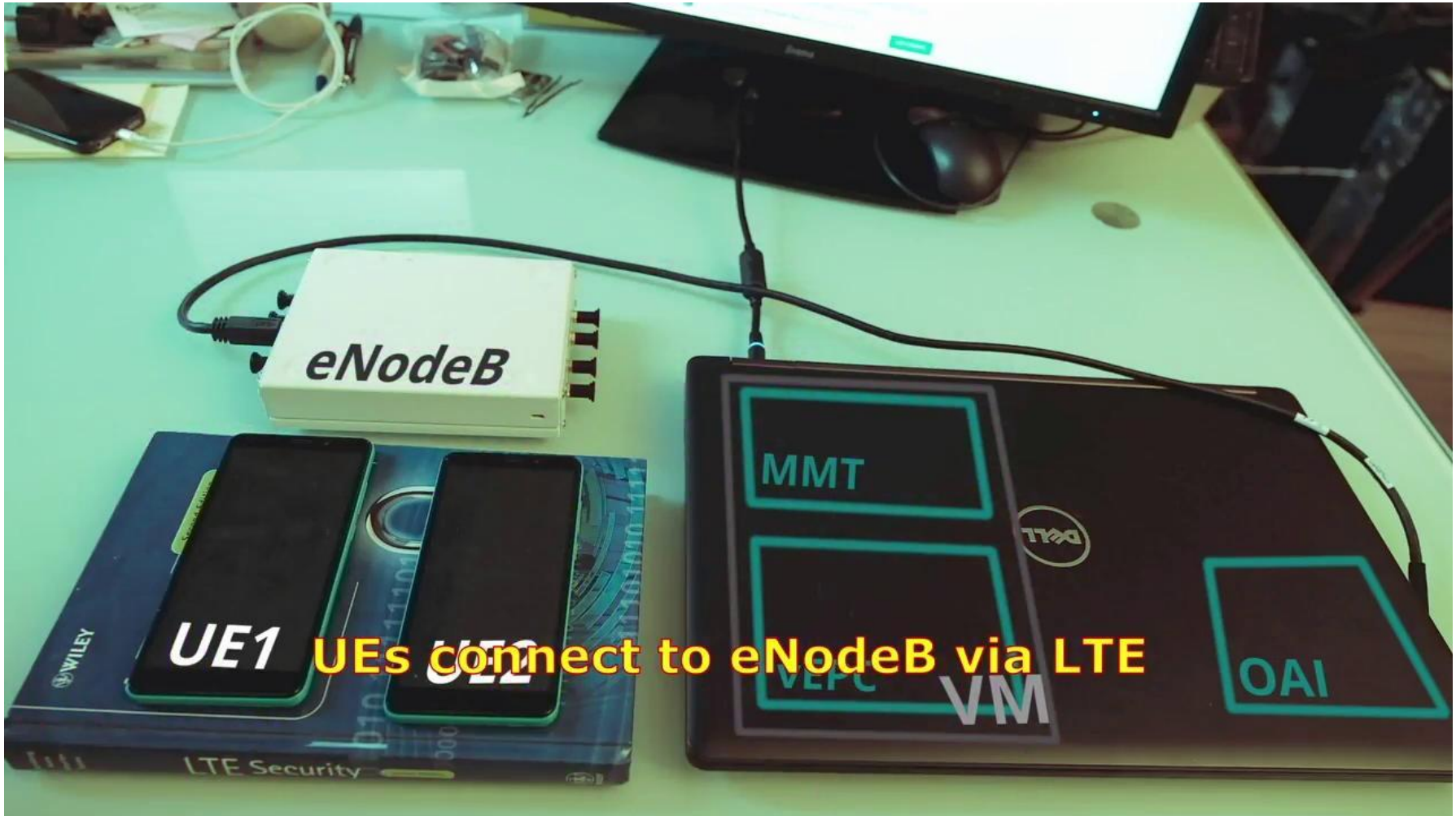
4G testbed



4G testbed

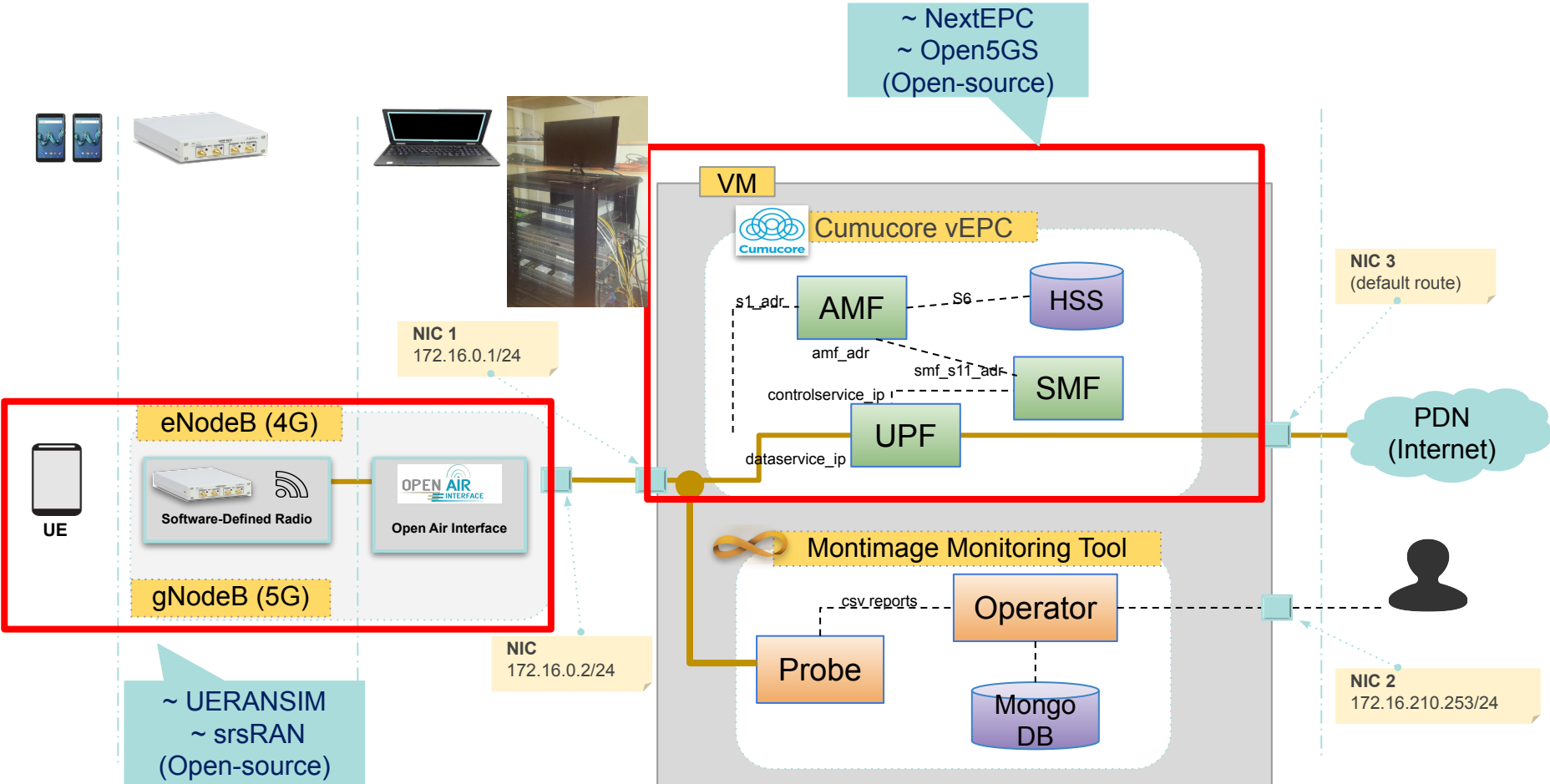


4G demo



UEs connect to eNodeB via LTE

5G testbed



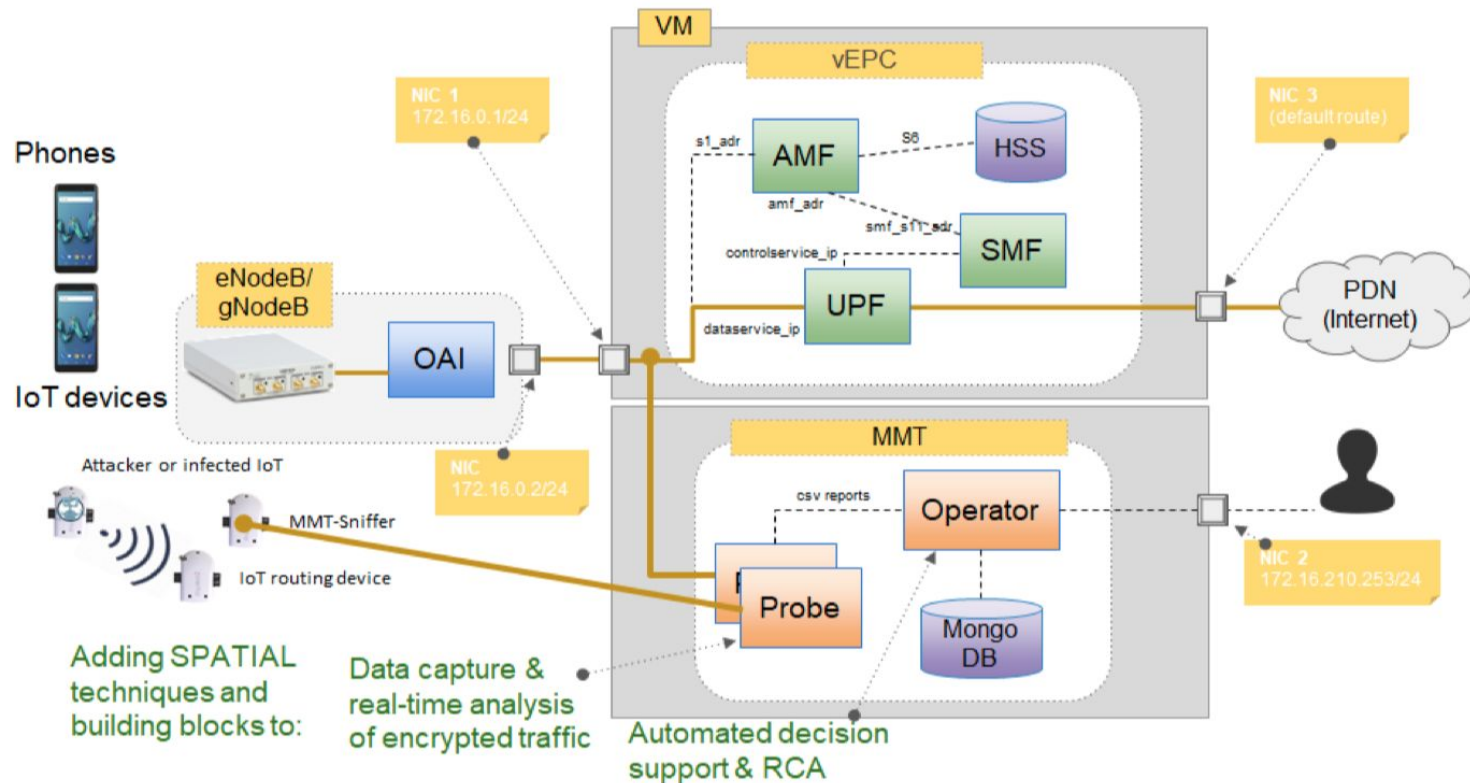
5G NSA testbed



5G demo



5G-IoT testbeds



- SPATIAL use case:

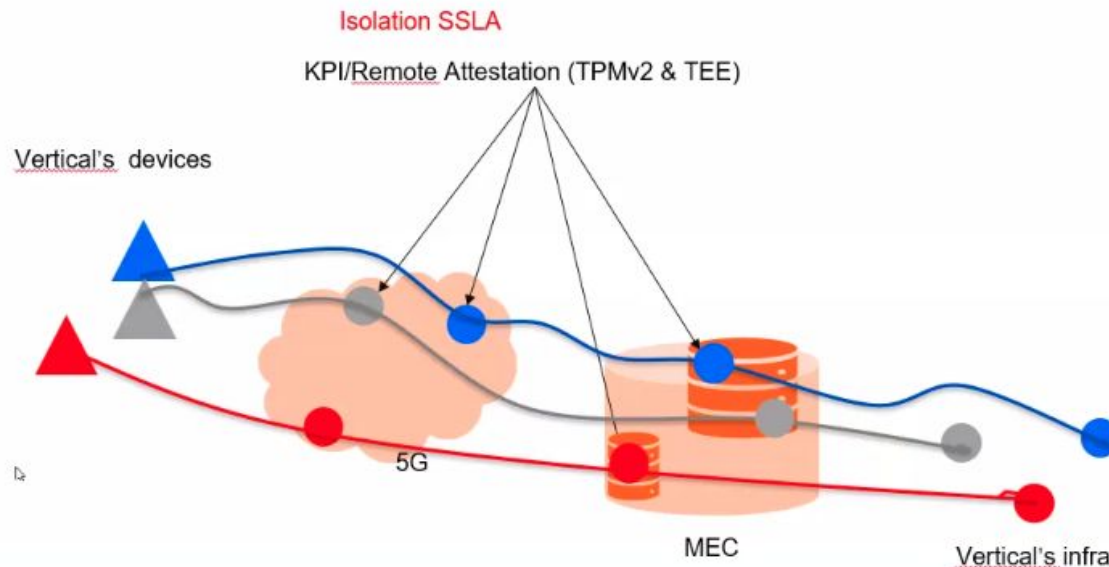
<https://spatial-h2020.eu/more-cybersecure-5g-networks/>

- FED4FIRE use case:

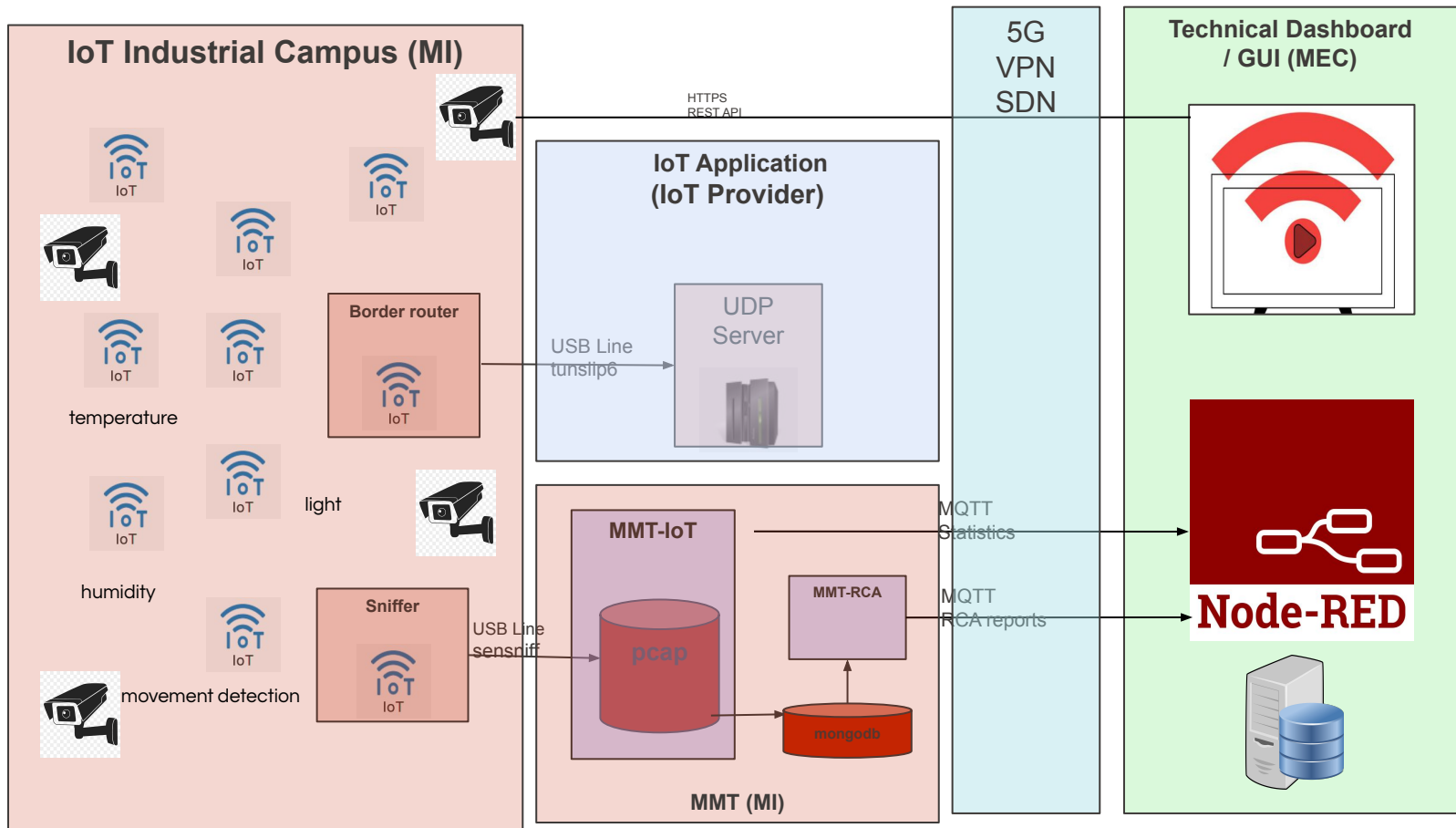
https://www.montimage.com/pubs/pdf/ICSOFT_2021_82_CR.pdf

INSPIRE-5G+ use case

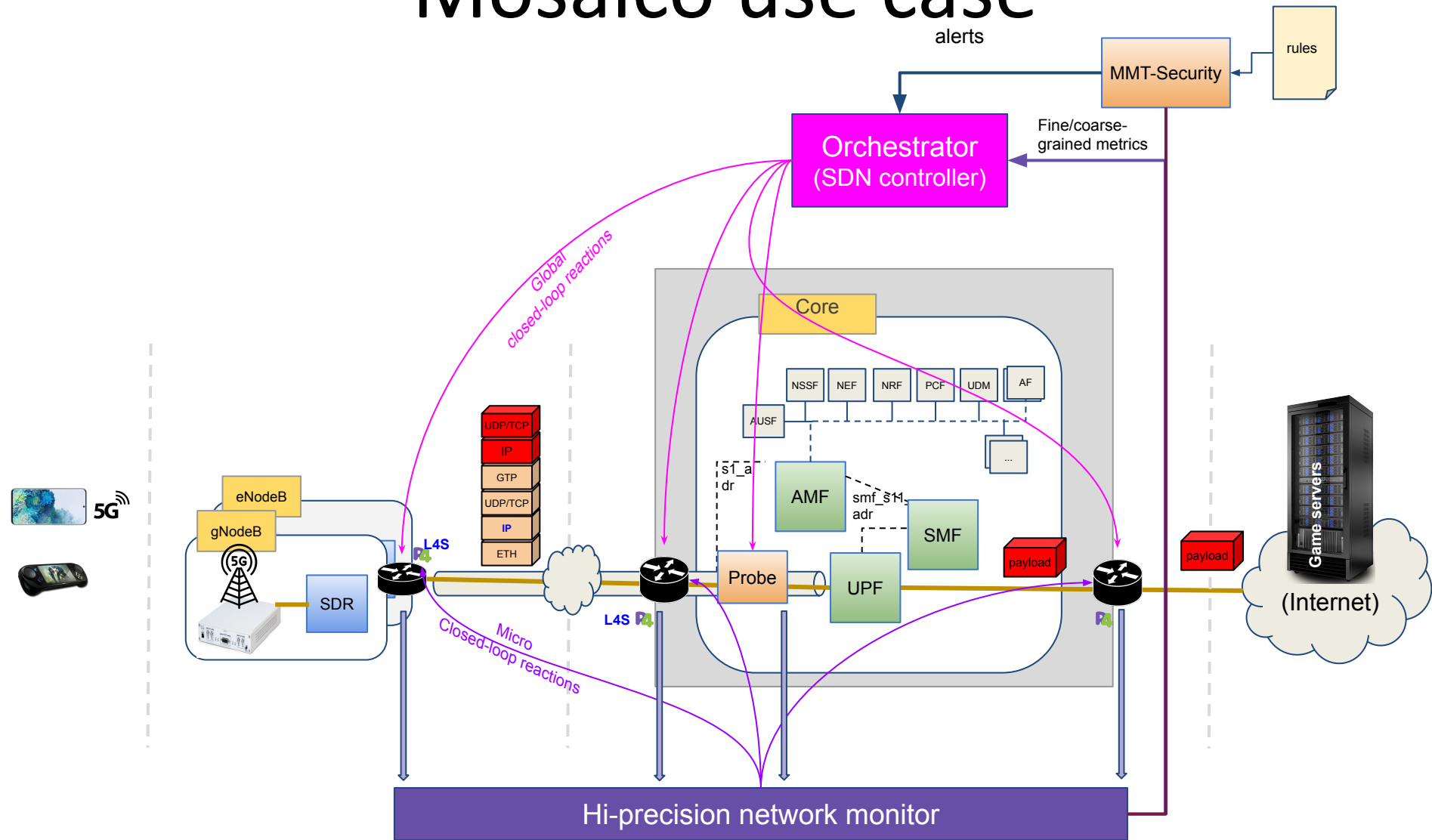
- **Blue** - E2E service under normal conditions: MMT monitors the IoT Industrial Campus (MI)
- **Red** - Additional E2E Service activated only under critical conditions: Video streaming (OLP, MI)
- Scenario:
 1. MMT detects some anomaly (e.g., some IoT nodes stop sending data, some are sending data but slowly)
 2. MMT-RCA determines and locates the possible (physical or cyber) root-cause (e.g., fire, intrusion) but does not have enough data to certify the conclusion 100%. It does this based on past experience.
 3. MMT notifies the Orchestrator.
 4. The Orchestrator (or a human) activates the **Red** line (e.g., a dedicated network slice) for video streaming. The camera is configured to point to the location indicated by MMT.



INSPIRE-5G+ use case



Mosaico use case



THANK YOU

Vinh La

vinh_hoa.la@montimage.com

