Monitoring techniques in practice:

Experiences and lessons learned

Ana Cavalli – Institut Mines-Telecom/Telecom Sudparis
Wissam Mallouli- Montimage

SAM, Saint Malo 2016

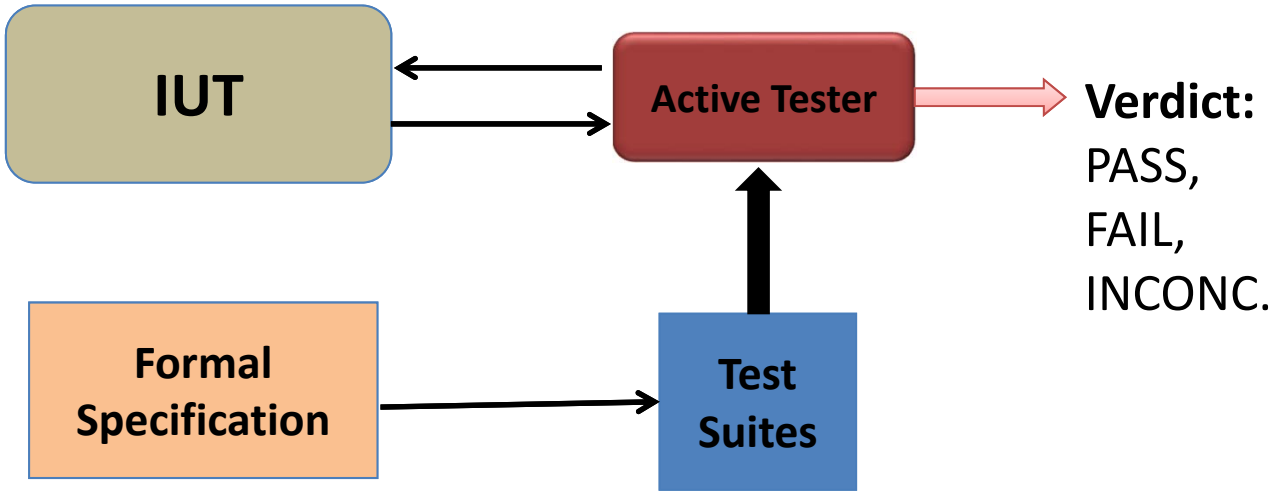
Motivation

- Show the evolution of active testing to monitoring (passive testing) techniques
- Explain the differences and complementarity of these techniques
- Show monitoring in practice
- Present an industrial monitoring tool: MMT

Testing

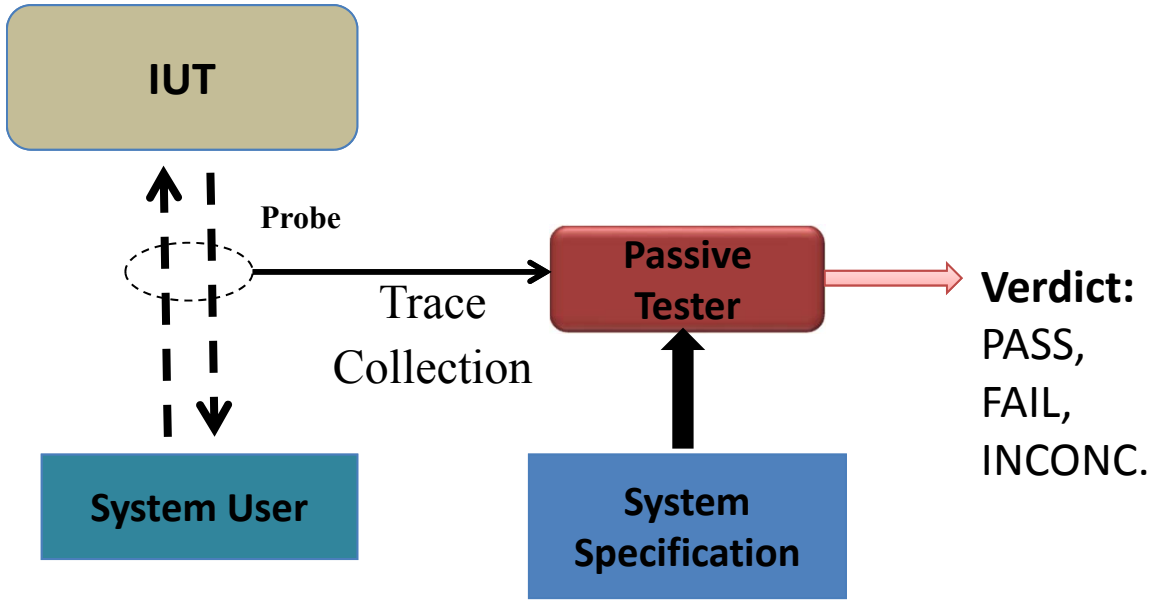
- Testing: The process of executing software with the intent of finding and correcting faults
- Conformance testing: The process of checking if the implementation under test conforms the specification
  - Two techniques: active and passive testing (monitoring)
  - This presentation will focus mostly on monitoring, but there are many common objectives and challenges with active testing

What is active testing ?



- Usually called Model Based Testing (MBT)
- It is assumed that the tester controls the implementation
  - Control means: after sending an input and after receiving an output, the tester knows what is the next input to be send
- The tester can guide the implementation towards specific states
- Automatic test generation methods can be defined
- Usually a test case is a set of input sequences

What is monitoring (passive testing) ?



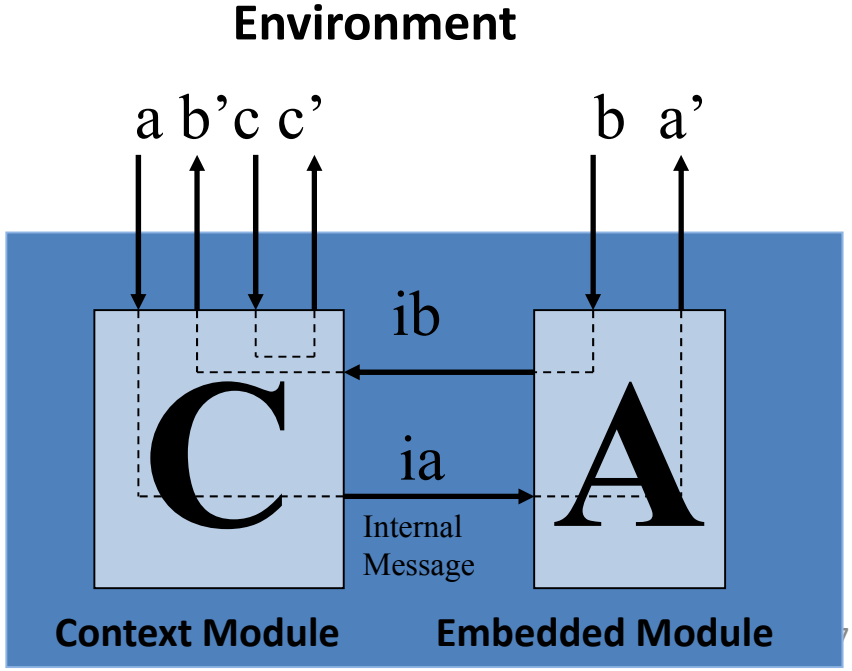
- Monitoring consists in analysing the traces recorded from the IUT and trying to find a fault by comparing these traces with either the complete specification or by verifying some specifics requirements (or properties) during normal runtime
- No interferences with the IUT

Limitations of active testing

- Non applicable when no direct access to the implementation under test
- Semi- controllable interfaces (component testing)
- Interferences on the behaviour of the implementation

Limitations for components testing

- Test in context, embedded testing:
  - Tests focused on some components of the system, to avoid redundant tests
  - Interfaces semi-controllables
  - In some cases it is not possible to apply active testing



Why monitoring?

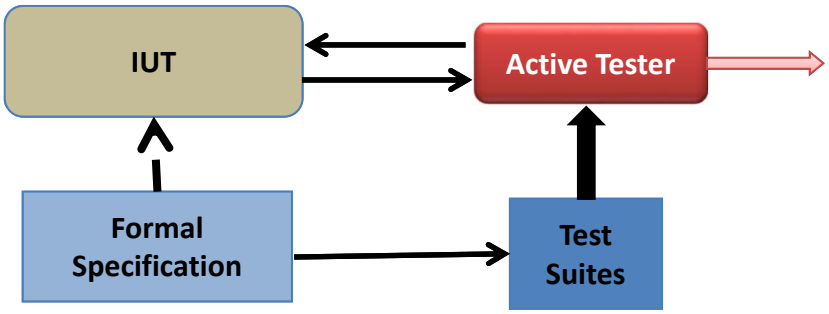
- Conformance testing is essentially focused on verifying the conformity of a given implementation to its specification
  - It is based on the ability of a tester that stimulates the implementation under test and checks the correction of the answers provided by the implementation

- Closely related to the controllability of the IUT
  - In some cases this activity becomes difficult, in particular:
    - If the tester has not a direct interface with the implementation
    - Or when the implementation is built from components that have to run in their environment and cannot be shutdown or interrupted (for long time) in order to test them

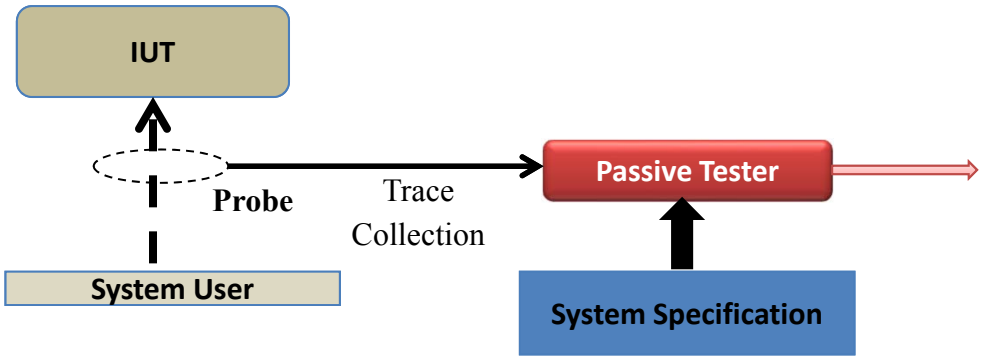
Controllability and observability issues in monitoring

- **Controllability**
  - No **controllability** issue because no interaction with the implementation under test
- **Observability**
  - It is assumed that to perform monitoring it is necessary to observe the messages exchanges between modules.
  - Monitoring is a Grey Box testing technique
- **Fault detection using monitoring**
  - It is possible to detect output faults
  - It is possible to detect transfer faults under some hypothesis: to initialise the IUT in order to be sure that the implementation is in the initial state and then perform monitoring

Monitoring vs Active Testing



☺ Full test generation automation
☹ Needs a model
☹ May modify (crash) the IUT behavior



☺ No interferences with the IUT
☺ No models needed
☺ Full monitoring automation
☹ Grey box testing

Monitoring techniques

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 (QoS, QoE) & SLA monitoring
- Based on traffic measurements
  - Gather traffic measures (e.g., performance indicators)
  - Analyze and correlate the measures in order to make a diagnosis

Complexity of network measurements

- Size, complexity and diversity of the networks
  - Understanding cause-effect relationships is difficult

- Measurement is not an objective!
  - Meaningless without careful analysis
  - Analysis depends on the monitoring objective
  - Need to define :
    - What, where, how to measure?

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 – through estimation)

Determining *How* to Measure

- Active measurements

  - Send test traffic into the network
    - Generate test packets periodically or on-demand
    - Assess the responses and provide a verdict
  - Popular tools for performance
    - Ping: RTT and loss
    - Traceroute: path and RTT
  - Issues :
    - Impose extra traffic on network and distort its behavior in the process
    - May impact the behavior of the network (self interfering)

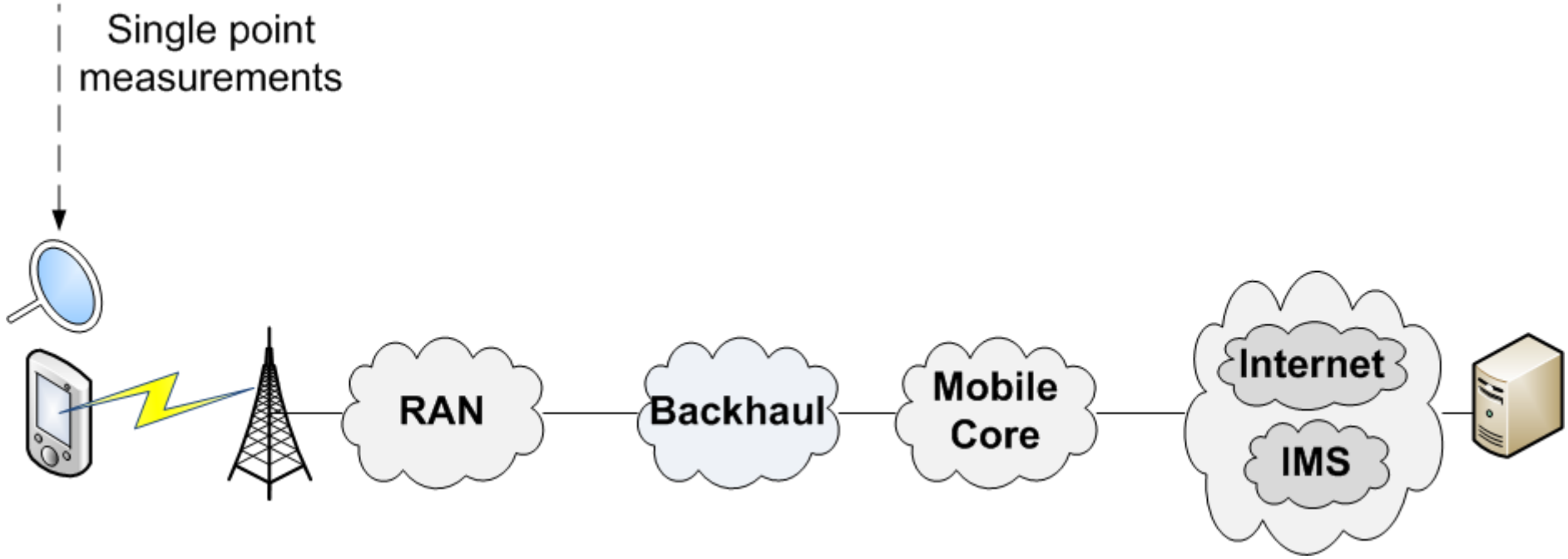
Determining *How* to Measure

- Passive measurements
  - Observing network traffic at the measurement point(s)
    - Packet capture (wireshark)
    - Flow-based measurement tools (routers)
    - SNMP tools (mostly used)
  - Perform analysis for various purposes

- Used to perform various traffic usage/characterization analysis/intrusion detection
- Problems
  - LOTS of data!
  - Privacy issues
  - Performance issues (wire speed packet capture and analysis)

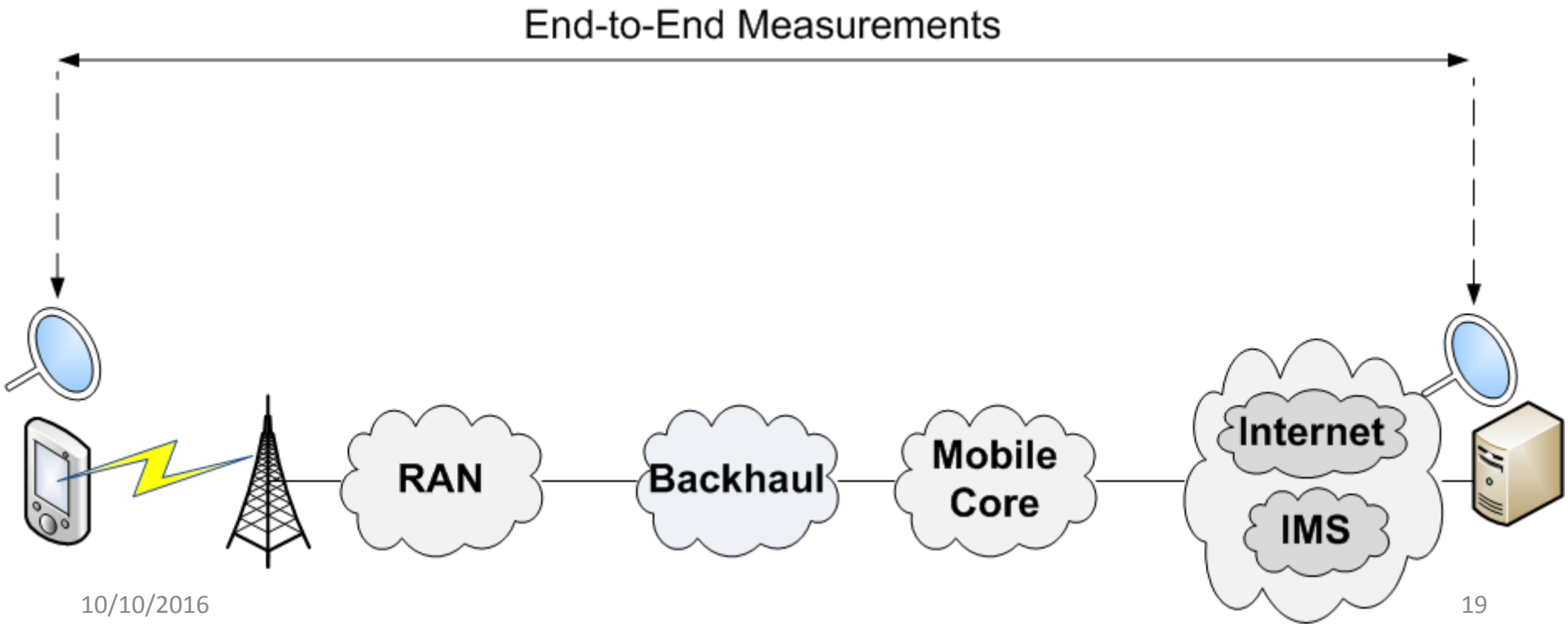
Determining *Where* to Measure

- Single point measurements
  - Provide partial view of the network



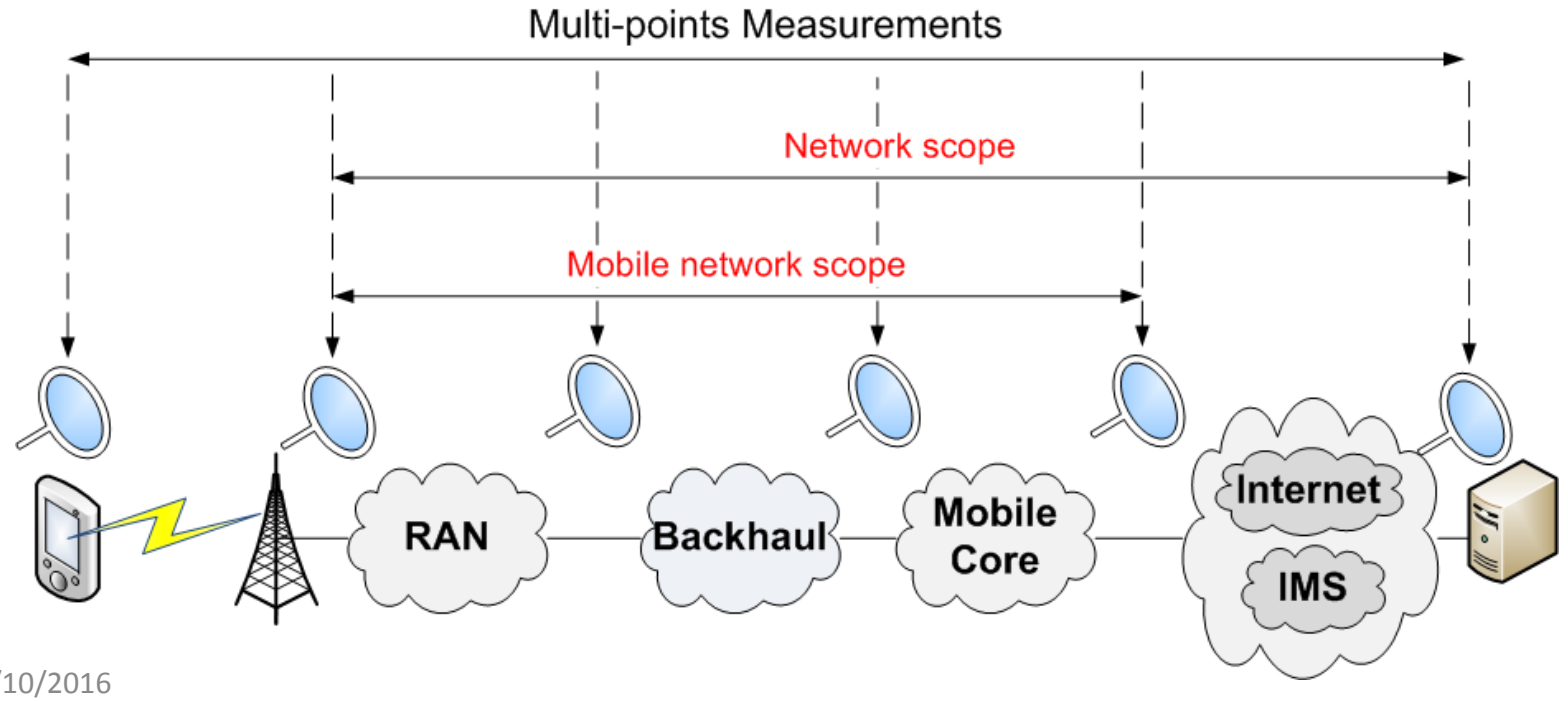
Determining *Where* to Measure

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



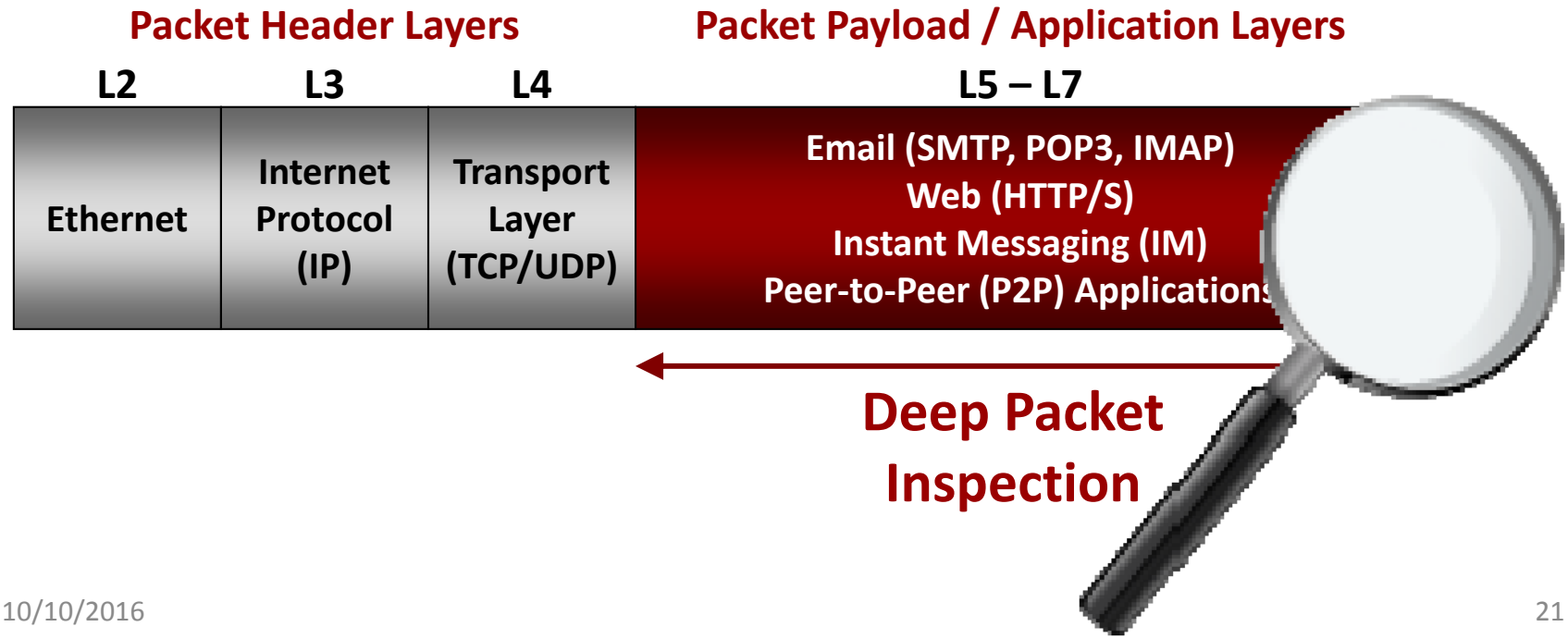
Determining *Where* to Measure

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



What is DPI?

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



Why DPI?

- Network Visibility
  - Understand how bandwidth is utilized
    - What is the application mix
    - Who is using what, where and when?
- Traffic Management (Application Control)
  - Block undesired traffic (spam, worms, etc.)
  - Prioritize and shape traffic (limit P2P, QoS, QoE)
  - Advanced policy enforcement
  - Zero Facebook, OTT services, per application policy rules
- Network management
  - Advanced billing (abandoning the unlimited data plans)
  - New pricing may appear soon (user defined preferred applications for free, fees applies for the rest of applications)
- Security
  - Understand network attacks
  - Core component in next generation firewalls

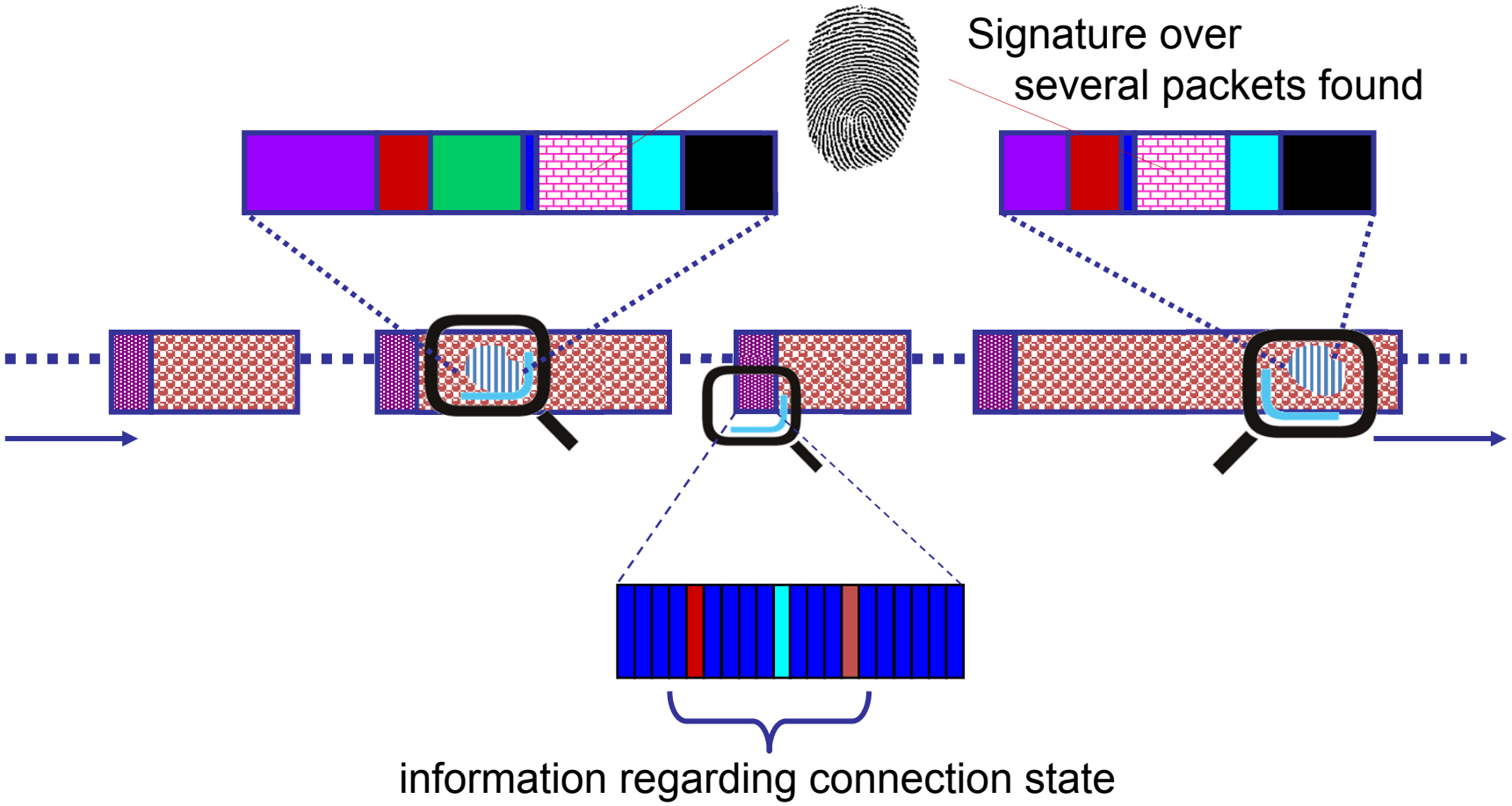
Classification Techniques: The challenge

- High number of applications and protocols
  - Same Application – Different Implementations/versions
    - Bittorrent has more than 30 different client implementations
    - IM or VoIP don't use similar protocols
  - Evolving Architectures
    - Client/server, Cashes, P2P, Client's network surroundings: Firewall/NAT, Proxy
  - Various Clients: PC, Smartphone, Gaming Console
- Frequent Updates
  - Can vary from every year to every month
  - Typically will affect protocol format
- Use of Encryption (Obfuscation)
  - Primarily designed for counter measuring operator's throttling and monitoring efforts (eMule, Bittorrent)
  - In some cases protect proprietary implementation (Skype)
- Need to differentiate use
  - "Good" (legit streaming, SW updates) vs. "Bad" (pirated file sharing) P2P
- Need to recognize application subtleties for proper actions
  - Example: MSN IM – block VoIP & Streaming, allow Chat

Classification Techniques

- Port based
- Pattern matching
- Statistical

Analysis by Pattern Matching



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
- The detection requires a number of packets
- Example
  - Very close inter-arrival delays with low deviation from the average (VoIP)
- Extremely effective analysis when application uses encryption or obfuscation
  - Or simply when access to the payload is not possible
  - Classification in the dark

Security monitoring with DPI: Abstract description

- The concept:
  - Detect the occurrence of **events** on the network
    - Input provided by DPI
    - Event can be: packet arrival, HTTP POST request, etc.
  - Inspect and analyze the succession of events to detect **properties**
    - Property: Succession of events that are linked with “time” and “logical” constraints
      - If we detect event “A”, then we MUST detect event “B” before 10 seconds
- The idea:
  - Monitor the network looking for the occurrence of properties.

Properties Expressivity

- Considering security monitoring, properties can be used to express:
  - A Security rule describes the expected behavior of the application or protocol under-test.
    - The non-respect of the Security property indicates an abnormal behavior.
    - Set of properties specifying constraints on the message exchange
      - i.e. the access to a specific service must always be preceded by an authentication phase
  - An Attack describes a malicious behavior whether it is an attack model, a vulnerability or a misbehavior.
    - The non respect of the Security property indicates the detection of an abnormal behavior that might indicate the occurrence of an attack.
    - Set of properties referring to a vulnerability or to an attack
      - A big number of requests from the same user in a limited period can be considered as a behavioral attack

MONTIMAGE Monitoring Tool (MMT)

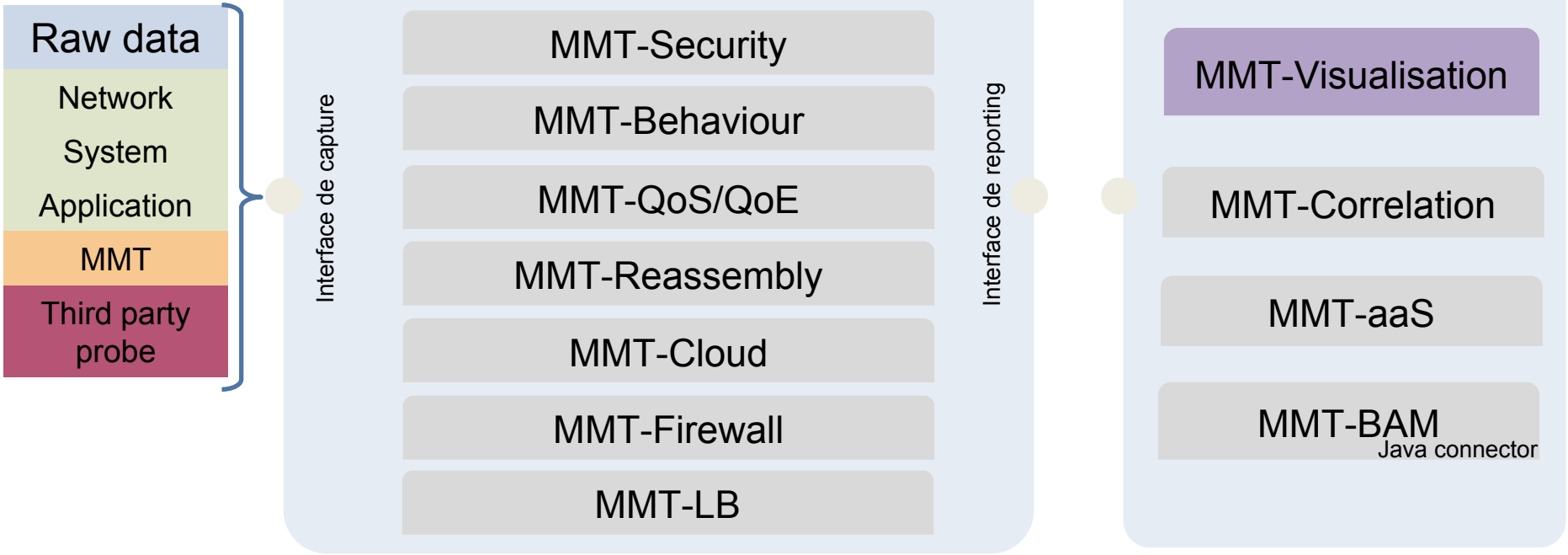
Montimage Monitoring Tool

- Modular monitoring solution that allows to detect behavior, security, performance incidents based on a set of properties (written in XML)
  - License for academia (for research)
  - Easy to extend – Provide documentation + support
  - Brochure

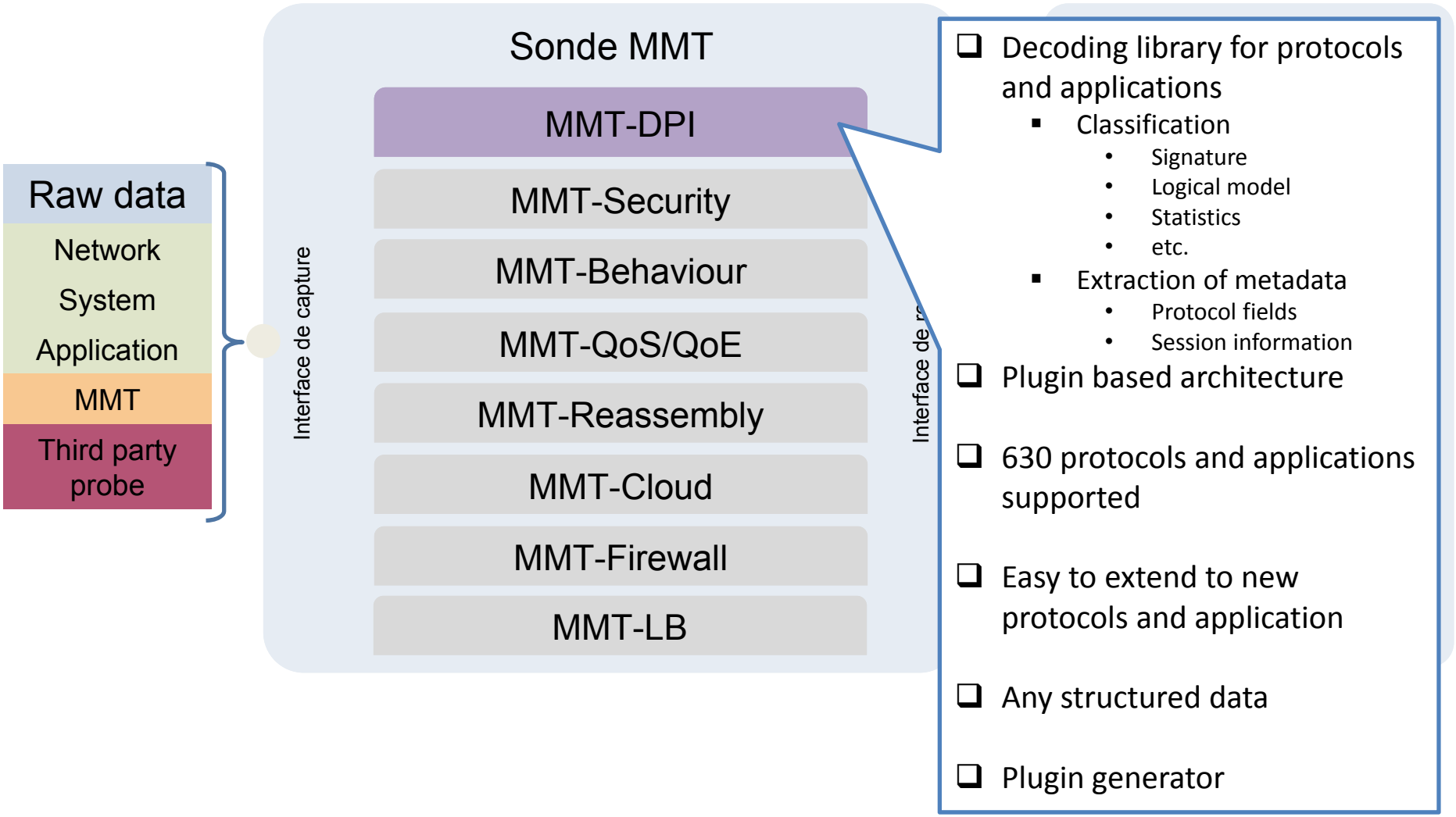
How MMT sees monitoring ?

- Events based Monitoring
  - Online or offline
  - Non-obtrusive
- Different objectives
  - Understand
  - Behaviour
  - Security
  - Performance
- Help in decision making
  - Resources planning
  - Counter-measures
- When to monitor
  - During the testing phase
  - During application/system operation
- How to monitor
  - Local
  - Distributed
  - Centralized
    - Hierarchical
    - P2P

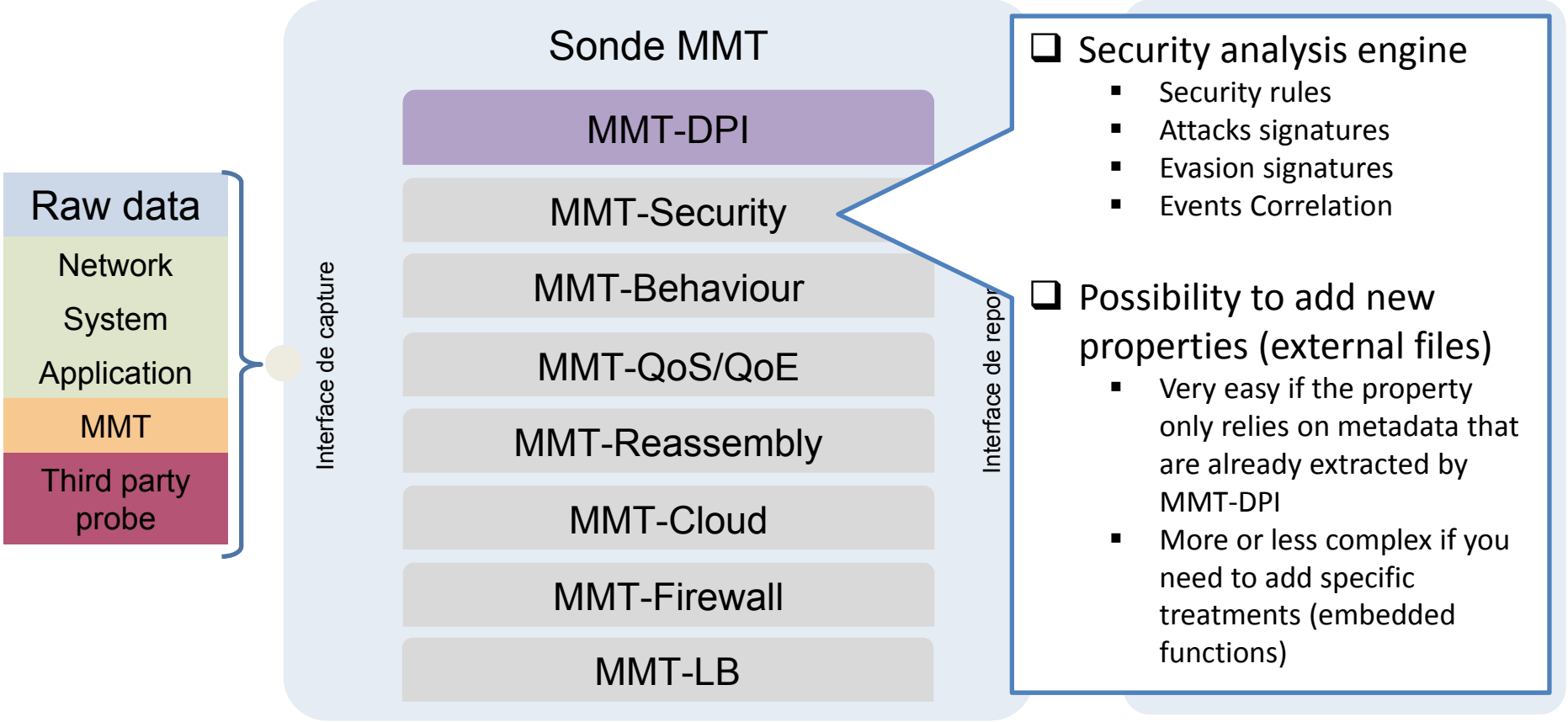
MMT DPI


Raw data
Network
System
Application
MMT
Third party probe
Interface de capture
Sonde MMT
MMT-DPI
MMT-Security
MMT-Behaviour
MMT-QoS/QoE
MMT-Reassembly
MMT-Cloud
MMT-Firewall
MMT-LB
Interface de reporting
MMT Operator
MMT-Admin
MMT-Visualisation
MMT-Correlation
MMT-aaS
MMT-BAM
Java connector

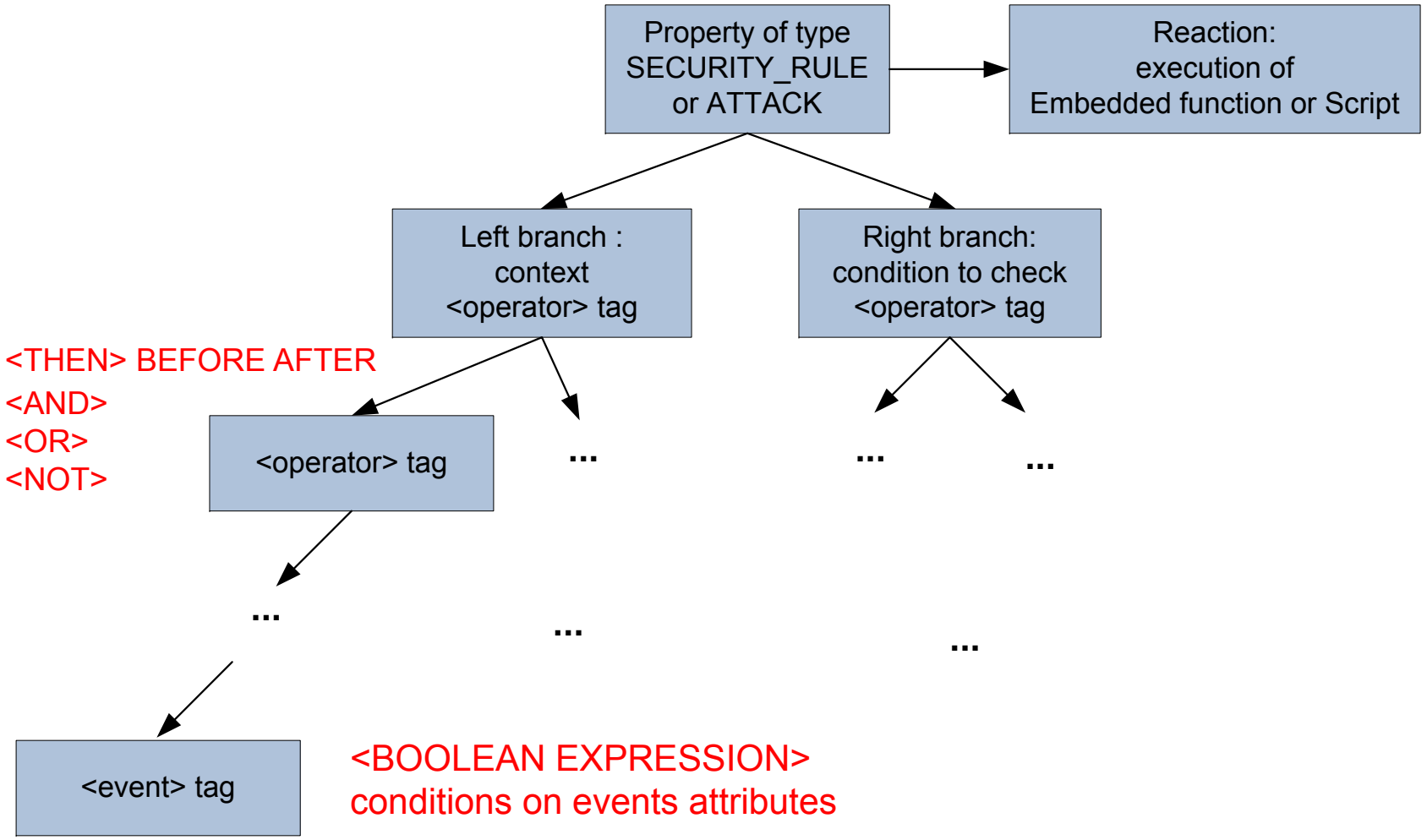
MMT DPI


Raw data
Network
System
Application
MMT
Third party probe
Interface de capture
Sonde MMT
MMT-DPI
MMT-Security
MMT-Behaviour
MMT-QoS/QoE
MMT-Reassembly
MMT-Cloud
MMT-Firewall
MMT-LB
Interface de r
❑ Decoding library for protocols and applications
▪ Classification
• Signature
• Logical model
• Statistics
• etc.
▪ Extraction of metadata
• Protocol fields
• Session information
❑ Plugin based architecture
❑ 630 protocols and applications supported
❑ Easy to extend to new protocols and application
❑ Any structured data
❑ Plugin generator

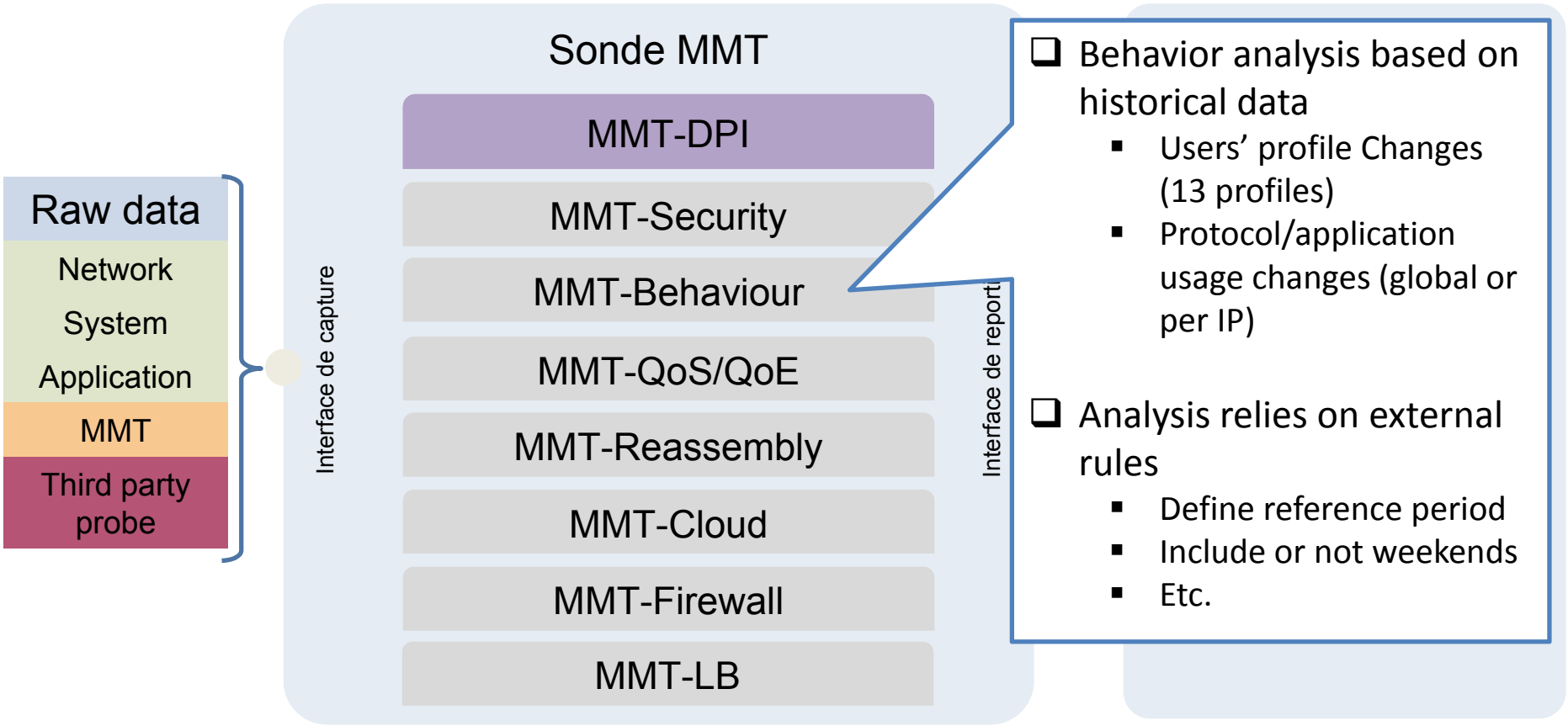
MMT-Security



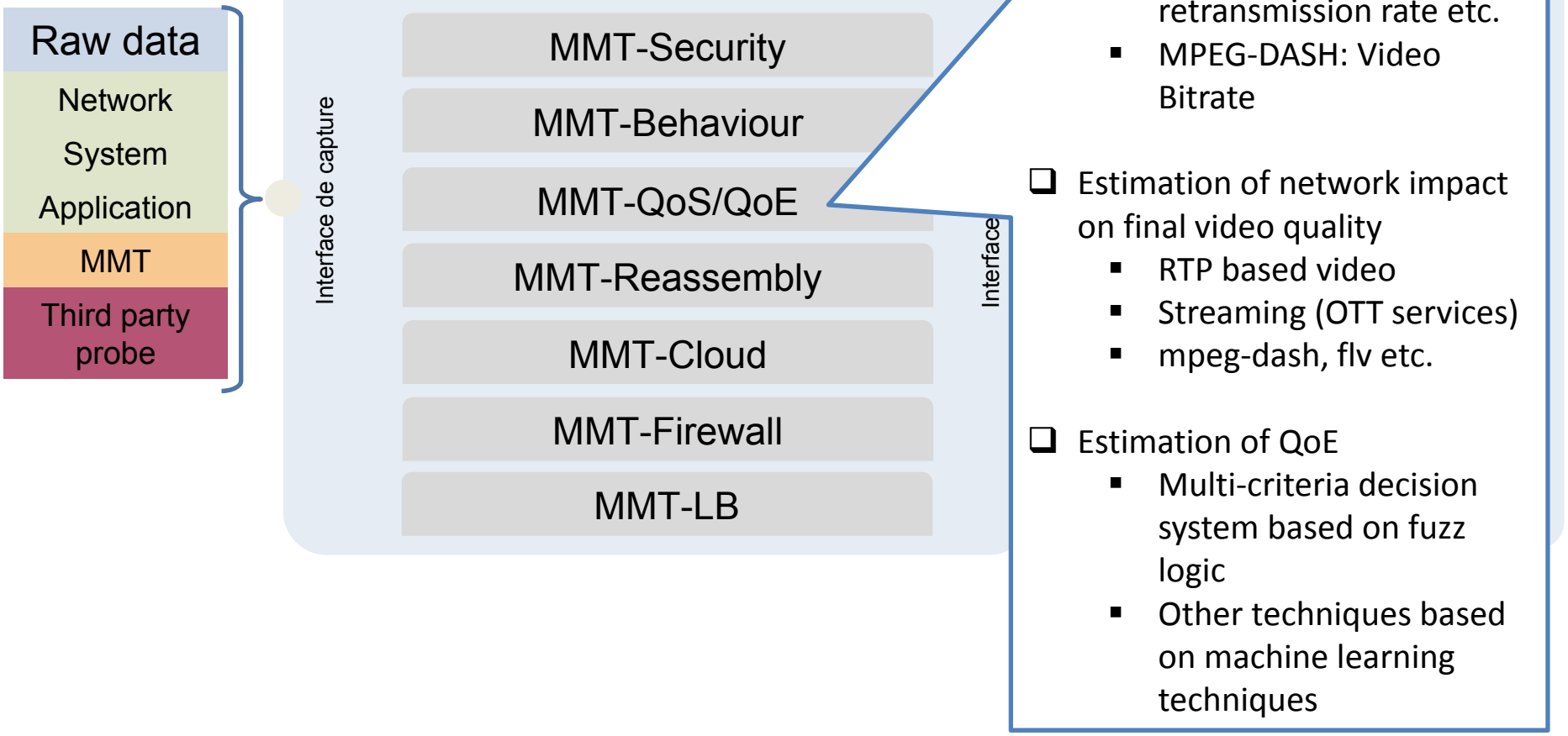
MMT-Properties



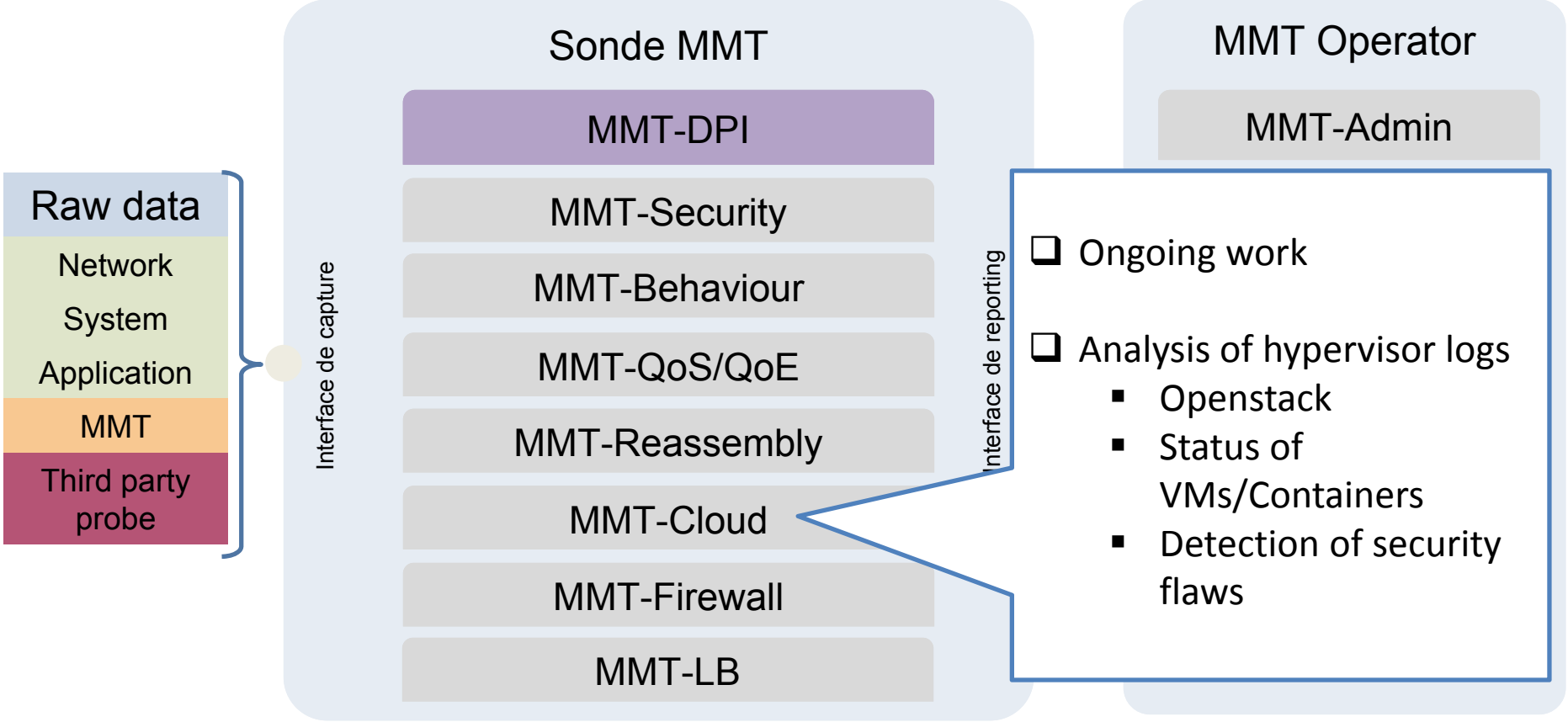
MMT-Behavior



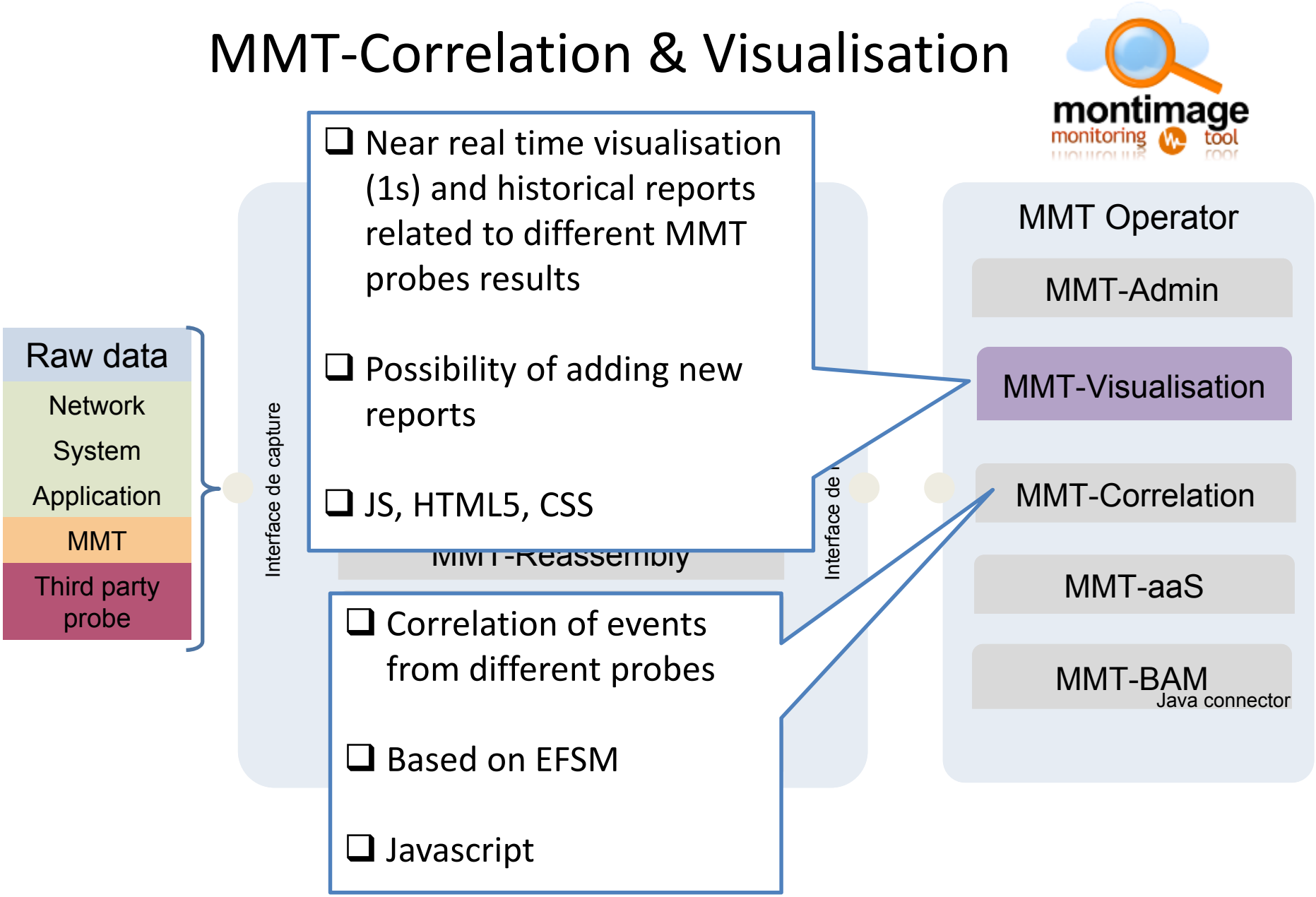
MMT-QoS/QoE


Raw data
Network
System
Application
MMT
Third party probe
Interface de capture
Sonde MMT
MMT-DPI
MMT-Security
MMT-Behaviour
MMT-QoS/QoE
MMT-Reassembly
MMT-Cloud
MMT-Firewall
MMT-LB
Interface
❑ Analysis of technical KPIs
▪ Example: packet loss rate, Jitter, retransmission rate etc.
▪ MPEG-DASH: Video Bitrate
❑ Estimation of network impact on final video quality
▪ RTP based video
▪ Streaming (OTT services)
▪ mpeg-dash, flv etc.
❑ Estimation of QoE
▪ Multi-criteria decision system based on fuzz logic
▪ Other techniques based on machine learning techniques

MMT-Cloud


Raw data
Network
System
Application
MMT
Third party probe
Interface de capture
Sonde MMT
MMT-DPI
MMT-Security
MMT-Behaviour
MMT-QoS/QoE
MMT-Reassembly
MMT-Cloud
MMT-Firewall
MMT-LB
Interface de reporting
MMT Operator
MMT-Admin
Ongoing work
Analysis of hypervisor logs
Openstack
Status of VMs/Containers
Detection of security flaws

MMT-Correlation & Visualisation



Conclusion

- MMT has been used in many European projects (H2020, ITEA, CELTIC)
- MMT has been used in many national projects
- MMT is used by industrials (Thales, Orange, Ericsson, Softeam, …)
- Universities (Telecom Paris Sud, University Paris Sud, Troyes University, …)

THANK YOU!!

- **Address**

39 rue Bobillot,
75013, Paris, France

- **Phone**

Phone: +33 (0) 1 77 19 68 99

- **Email**

contact@montimage.com

This work presented here has been financed by the H2020 CLARUS project

http://www.clarussecure.eu/

User centred privacy and security in the cloud