Network Monitoring for Security Checking

Wissam Mallouli – Montimage
RCIS industrial day – May 31st 2013
wissam.mallouli@montimage.com

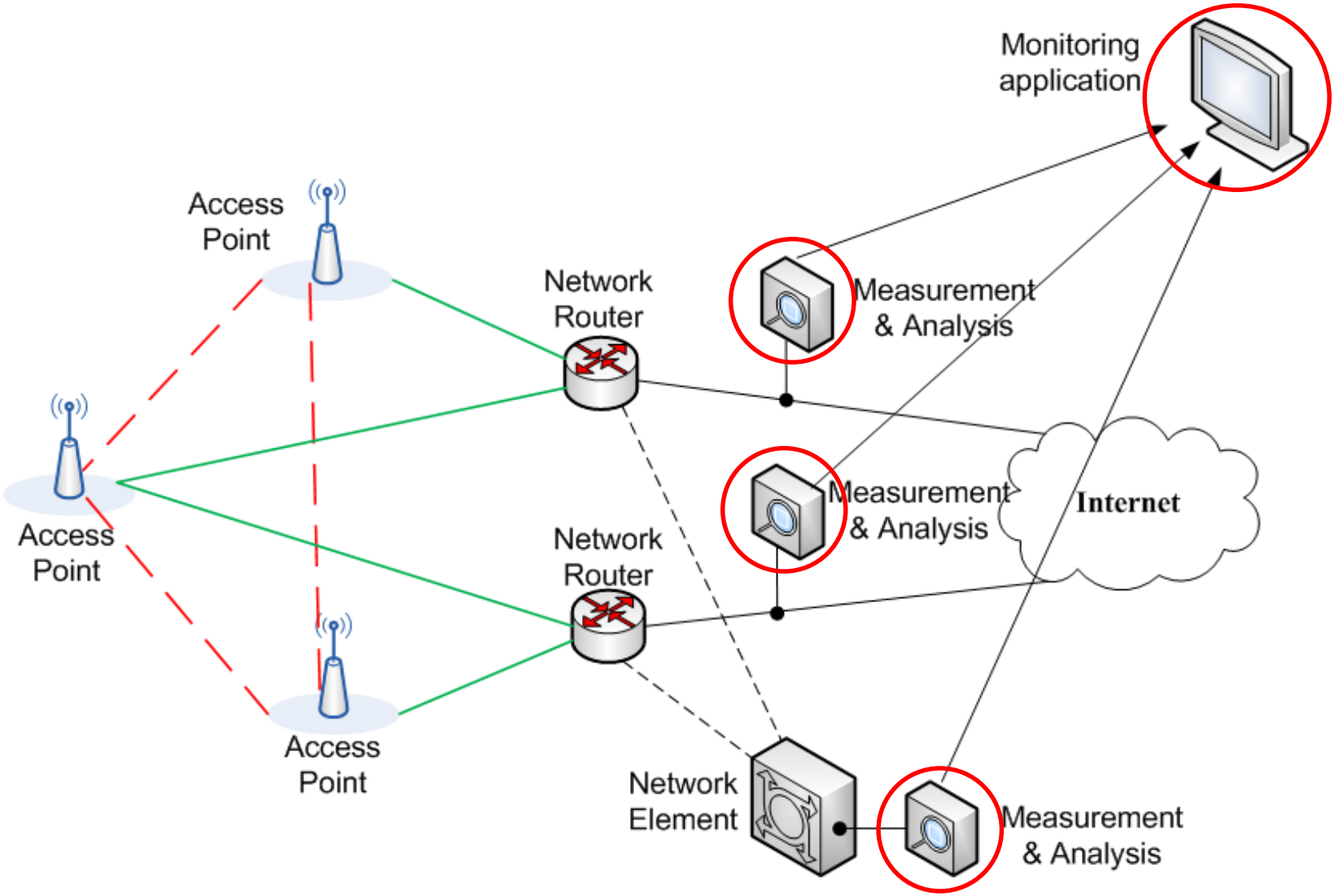
montimage monitoring tool

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

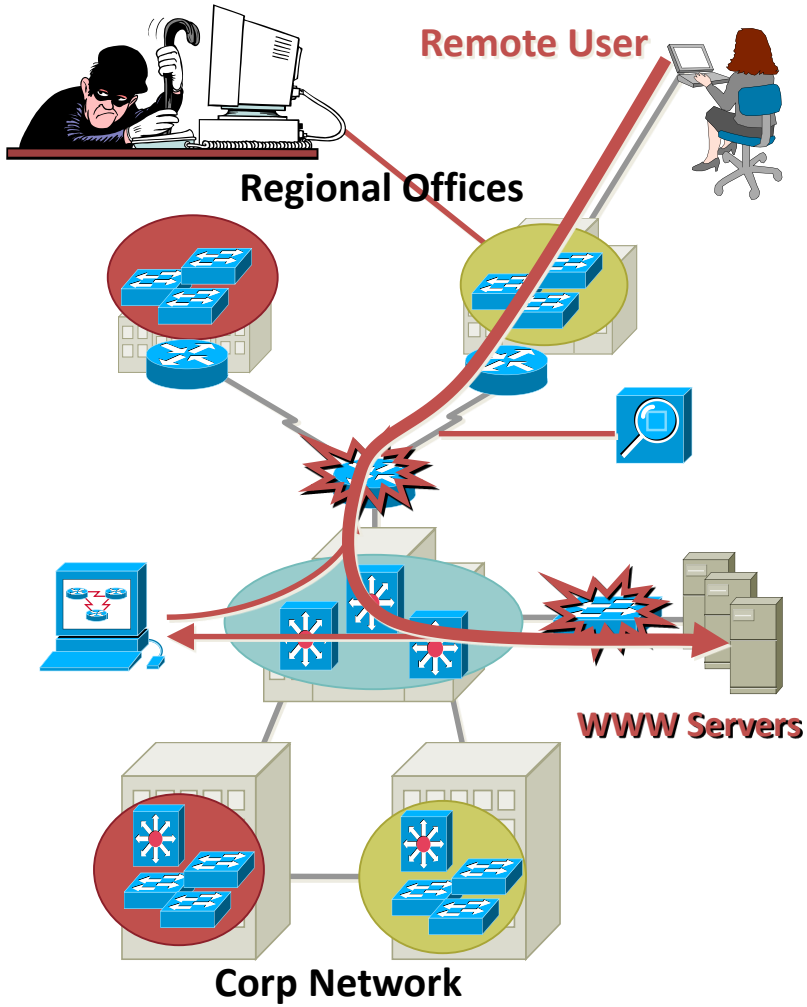
- Can be used to
  - Understand the behavior of the network
  - Network planning & resource optimization
  - Detect faults and abnormal operation
  - Network security (Intrusion & Attack Detection)
  - Performance, quality & SLA monitoring
  - CRM, Marketing
- Sit above traffic measurements
  - Gather traffic measures and performance/security indicators
  - Analyze and correlate the measures in order to make a diagnosis

Network monitoring: Basics



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



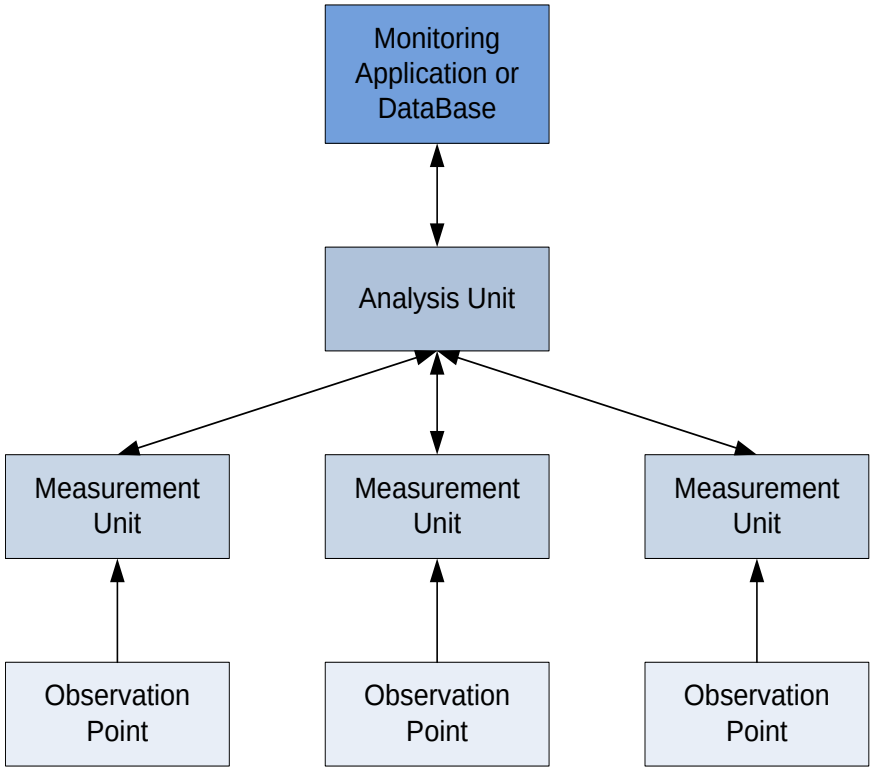
Network monitoring: Components

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

Security analysis unit
- Gathers, aggregates and correlates collected information (events)
- Notify remote events

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.



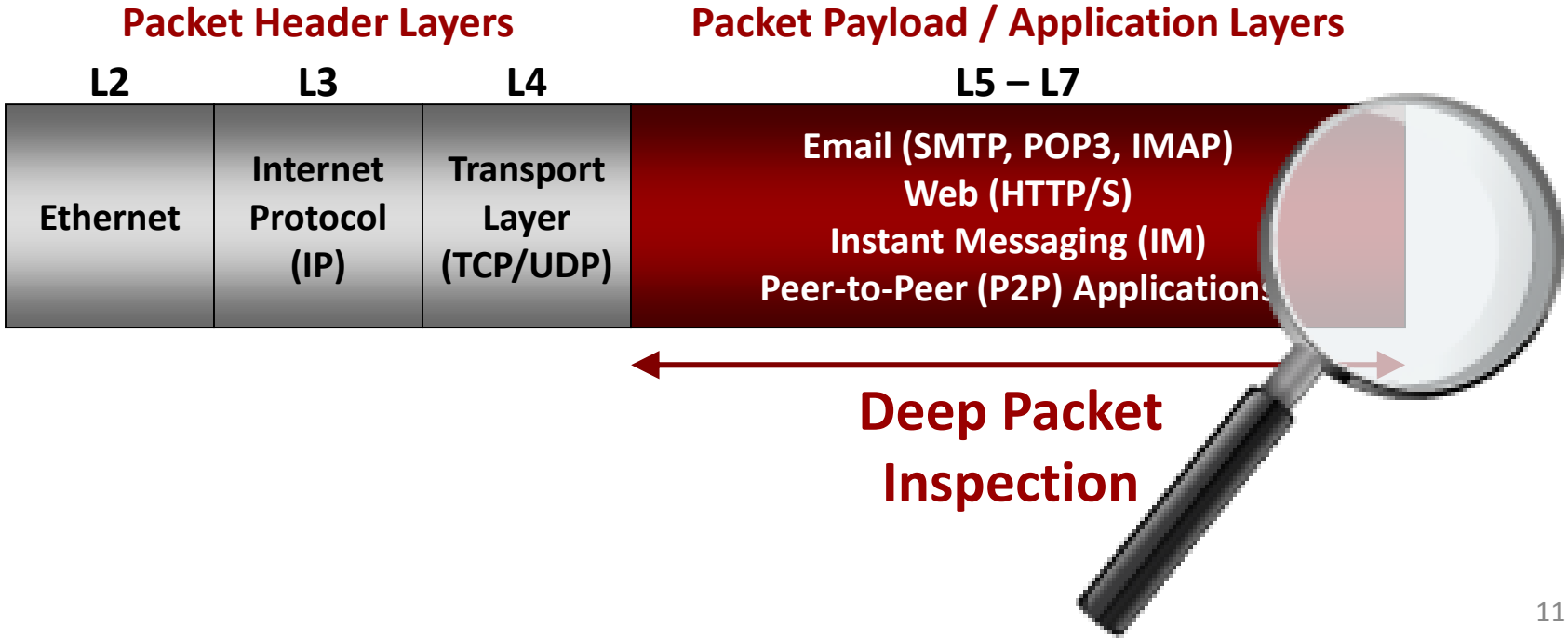
Deep Packet Inspection Based Monitoring

What is DPI

- Application classification
- Traffic attributes extraction

What is DPI

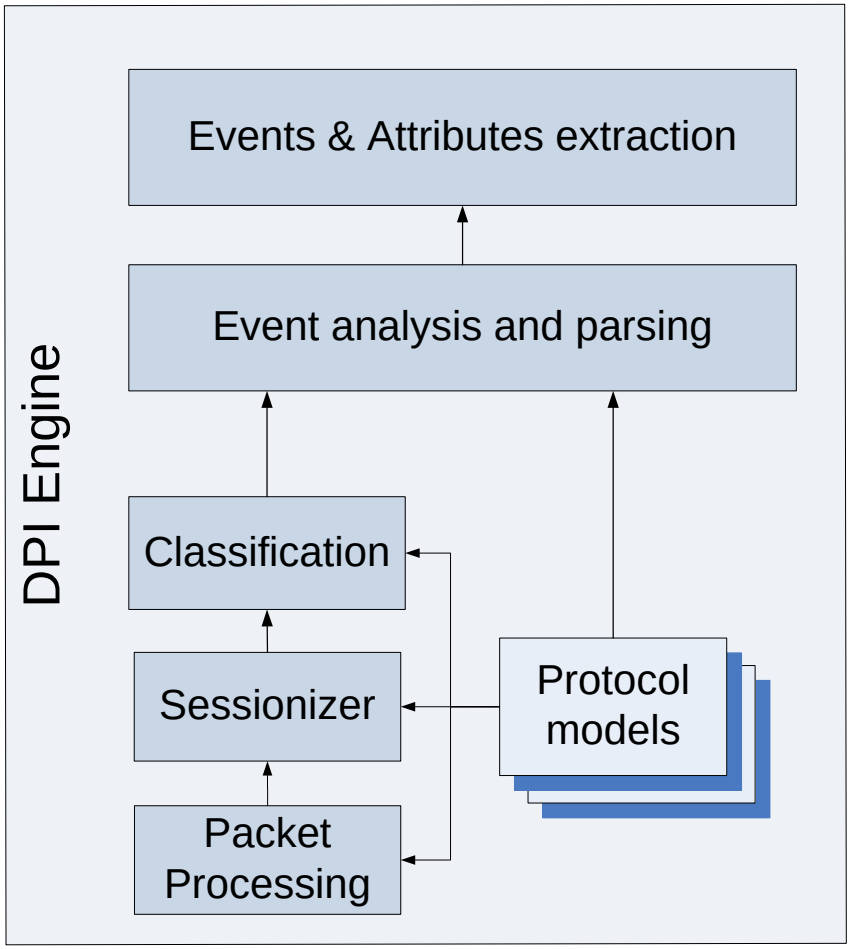
- Technology consisting of digging deep into the packet header and payload to “inspect” encapsulated content
  - Content may be spread over many packets



Why to 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
- Security
  - Understand network attacks
  - Core component in next generation firewalls
- Etc.

Inside DPI



- Group packets belonging to the same session
- Application classification
  - Detect application type (Skype, Bittorrent, etc.) or application family
  - Considered as the core of DPI
- Protocol decoding and attribute extraction
  - Parse the packet structure (this depends on the protocol & application)
  - Get protocol attributes (IP @, port numbers, …)
  - Get session attributes
  - Events and attributes may involve different packets
    - Attached file of an email

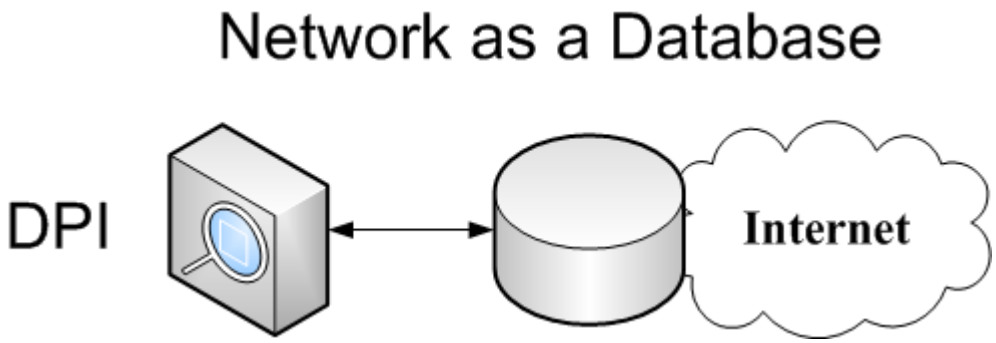
From classification to attributes and events extraction

- Application classification is a first step towards accurate traffic information extraction
  - How can we get the HTTP method (Get, Post, etc.) if we don't know the type of the traffic
  - When the application type is known decoding becomes "easy"
- What are traffic attributes?
  - Meta-attributes: timestamp, data source etc.
  - Protocol field derived from the packet data: IP@, attachment size, encoding type, etc.
  - Flow parameter: packet mean size, inter-arrival delay, packets lost, reordered, etc.
  - The application class can be considered as a traffic attribute

Attribute extraction with DPI

- With the extraction capability, DPI can provide input for security analysis

- Imagine the network as a database and DPI as an engine to extract data from this database!



Network as a Database

- Select flow_id Where (application = email AND attachment is executable)

- Select user_id, perceived_quality Where (application = Video AND protocol = RTP AND perceived_quality < 1)

Security Monitoring with DPI Using MMT

Abstract description

Challenges

Security properties

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” after 10 seconds
- The idea:
  - Monitor the network looking for the occurrence of properties.

Security monitoring using DPI: Abstract description

- Example: SQL injection
  - www.abcd.com/page?name=**Select * Where 1**
  - The events to be detected
    - HTTP GET request
    - URL parameter contains SQL statement
  - The property
    - It is **not allowed** to have a URL parameter containing SQL statement in an HTTP GET request
  - If the property is detected on the network then most probably there is an attack attempt!
- Nice Theory! But very challenging

Security monitoring using DPI

- Challenges
  - The number of events that can occur on a network is huge!
    - Solution: Use DPI for the events extraction
    - Group events/attributes by application and add new ones when needed
  - The expressivity of the properties (need to combine time and logical constraints)
  - Complex analysis and processing especially in high bandwidth links
    - Optimization techniques, multi-core implementations, smart traffic filtering

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 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

Properties Expressivity

- A security property is composed of 2 parts:
  - A Context
  - A condition to verify

- The “Context” and “Condition” of a property are composed of:
  - Simple events
    - Conditions on attributes (IP @ equal to 1.2.3.4)
  - Complex events linked by
    - Logical operators (AND/OR/NOT)
    - Chronological operator (AFTER/BEFORE)

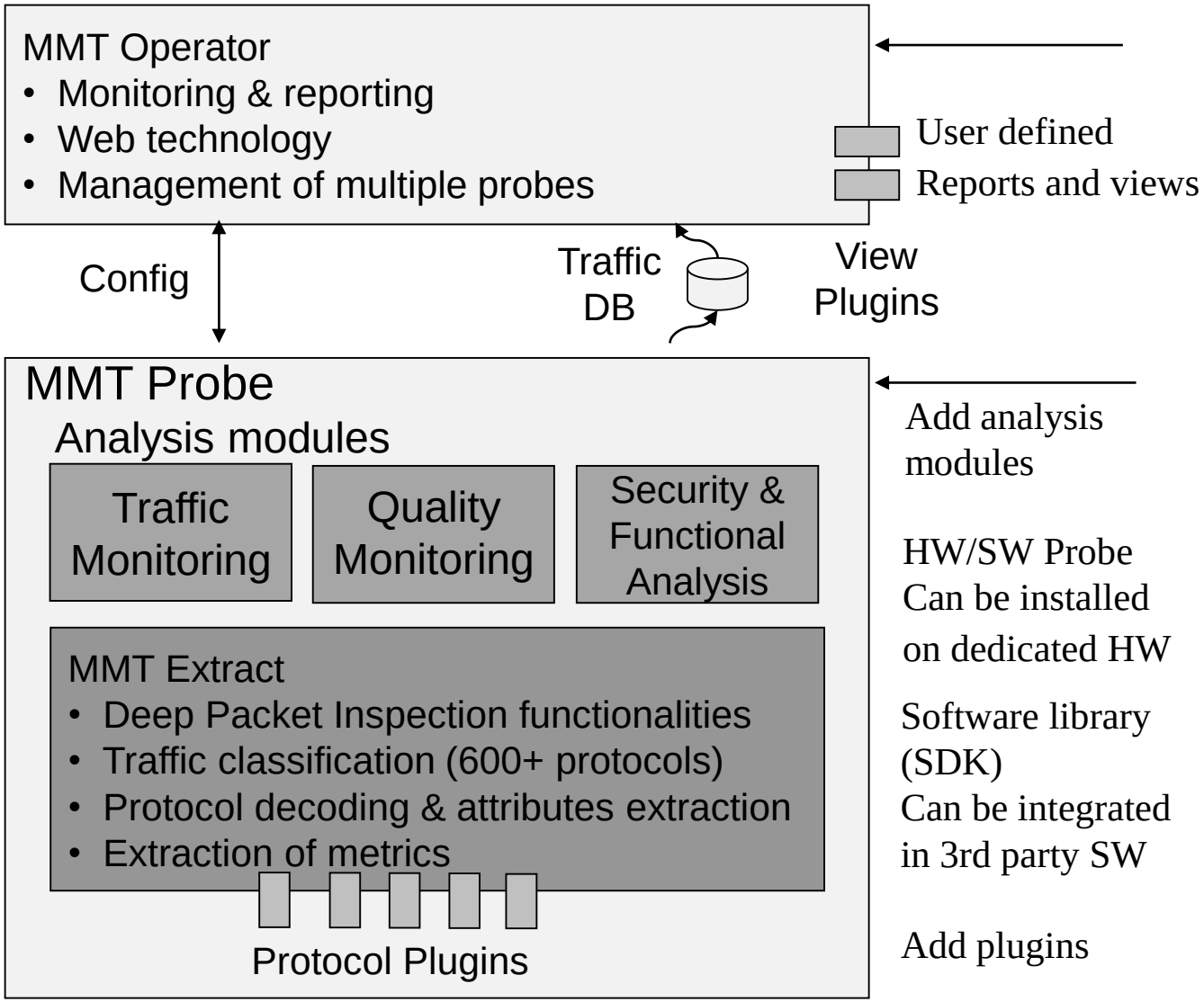
Properties Expressivity

- A security property is composed of 2 parts:
  - A Context
  - A condition to verify

If an HTTP Response is received (this is the context)

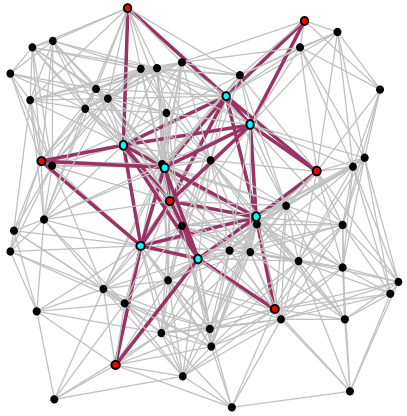
Then an HTTP request should have been received **before** (condition to verify)

Montimage Monitoring Tool (MMT)

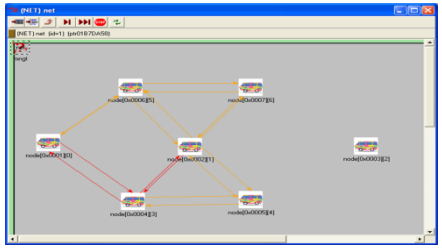


Thales Case Study: Ad-hoc waveform networking protocols

- Technical challenges
  - Automatic network : no initial planning
  - Network continuity whatever are the stations in the network
  - “on the move” automatic network re-organization and operation
  - End-to-end heterogeneous user services transmission : voice, messages
  - Decentralized mesh network. no Base Station
  - Nodes collaborate to ensure connectivity and participate in the routing task



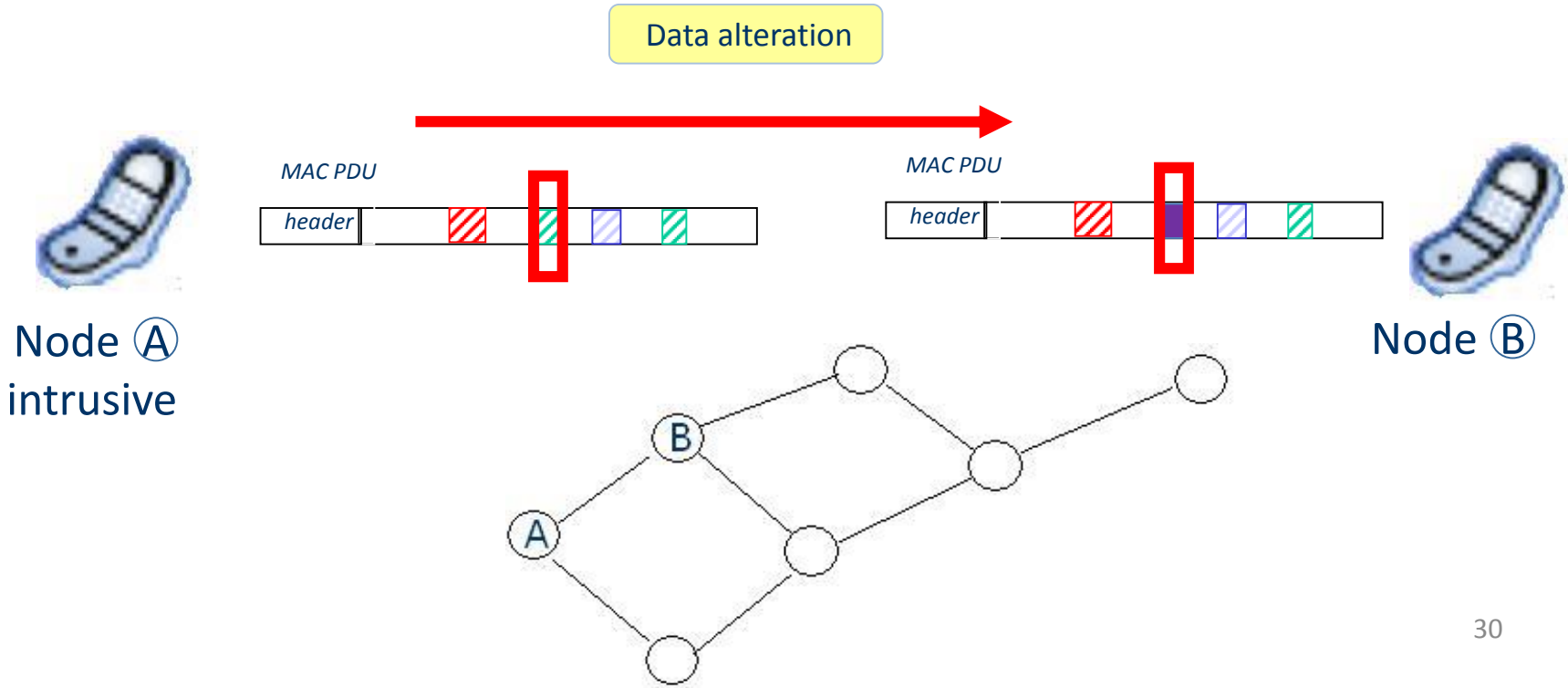
- Main scope of radio protocol case study: vulnerability analysis based on over-the-air info exchanged at physical layer
  - Frames analysis, data alteration, replay, denial of service, tampering and misuse, and combination of the threats



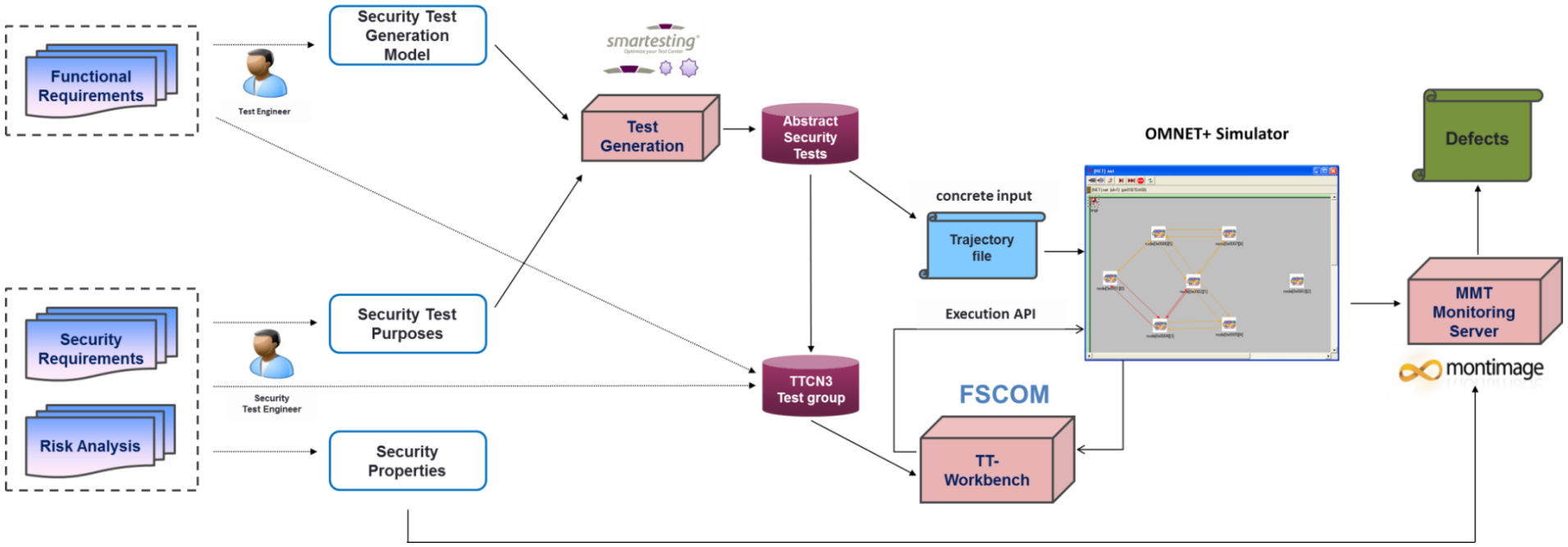
DIAMONDS

Network threats and vulnerabilities

- Detection of potential attacks
  - Link spoofing, Data alteration, Flooding attack, Blackhole attack, Denial of service, Replay …



Testing architecture



- ***SMARTESTING***
  - Security test generation model and test purposes specification
  - Generation of test scenarios denoting attacks using Certify-it
- ***FSCOM***
  - TTCN3 test cases specification
  - Test execution using TT-Workbench

- ***MONTIMAGE***
  - Specification of 19 security properties
  - Client /Server architecture
  - Notification of exchanged PDUs
  - Parsing and extraction of relevant information
  - Online analysis of captured PDUs and detection of attacks occurrences

Security Rules Specification : Example

- **Security requirement:** Every node must periodically send a notification message that includes the list of its neighbors on its allocated service slot.
- **Attack scenario 1:** A malicious node sends a message on a non-allocated service slot. This provokes slot reallocation. If done repeatedly, it provokes denial of service.
- **Specified security properties**
  - If one node receives two successive MSG_SPHY_DATA_IND messages from the same source, then these two messages must to be separated by 50 slots (Prop 1).
  - If one node receives two MSG_SPHY_DATA_IND messages from different sources, then these two messages must have two different slot ids (Prop 2).

Analysis results: Attack Scenario 1

Security rules summary results

Id	Description		
1	SECURITY RULE: If one node receives two successive MSG_SPHY_DATA_IND messages from the same source, then these two messages must be separeted by 50 slots (in the case of slot reallocation, this property is no longer correct)	24	8
2	SECURITY RULE: If one node receives two MSG_SPHY_DATA_IND messages from different sources, then these two messages must have two differents time slots (in the case of slot reallocation, this property is no longer correct)	0	0
3	SECURITY RULE: If node A receives from B an MSG_SPHY_DATA_IND message claiming A as a neighbor, then this means that A received from B at least 3 MSG_SPHY_DATA_IND messages in the last 4 periods (On	12	5
4	SECURITY RUL		0
5	SECURITY RUL		0
6	SECURITY RUL		0
7	SECURITY RUL		8
8	SECURITY RUL		0
9	SECURITY RUL		8
10	SECURITY RUL		0
11	SECURITY RUL MSG_SPHY_DA		1
12	SECURITY RUL		0
13	SECURITY RUL		0
14	SECURITY RUL		0

1		SECURITY_RULE: If one node receives two successive MSG_SPHY_DATA_IND messages from the same source, then these two messages must be separeted by 50 slots (in the case of slot reallocation, this property is no longer correct)
		EVENT 1: MSG_SPHY_DATA_IND message
		- - - - - - timeslot=000257
		- - - - - - MSG_SPHY_DATA_IND.SLOT_ID = 255
		- - - - - - THALES_META.NODE_ID = 3
		- - - - - - MSG_SPHY_DATA_IND.ADDRESS_SOURCE = 1
		- - - - - - MSG_SPHY_DATA_IND.SLOT_TYPE = 0
		- - - - - - THALES_META.MSG_CODE = 8193
		EVENT 2: MSG_SPHY_DATA_IND message
		- - - - - - timeslot=000297
		- - - - - - MSG_SPHY_DATA_IND.SLOT_ID = 295
		- - - - - - THALES_META.NODE_ID = 3
		- - - - - - MSG_SPHY_DATA_IND.ADDRESS_SOURCE = 1
		- - - - - - MSG_SPHY_DATA_IND.SLOT_TYPE = 0
		- - - - - - THALES_META.MSG_CODE = 8193

Some Results

- A plugin for “data/fields values” extraction from collected messages has been developed for layer 2 protocols and services.
  - More than 20 messages are parsed.
- Identification of 5 attack types and generation of different test scenarios simulating intruder nodes.
- A set of 19 “security” properties have been specified and checked by Montimage
  - Mainly properties dealing with
    - the right order of messages
    - ensuring availability of specific fields
    - ensuring the right structure and length of transmitted messages
- At least one security property is violated for each attack occurrence

THANK YOU

Wissam Mallouli
wissam.mallouli@montimage.com

Some of the material used in these slides come from the Internet

Thanks to “them”