MMT-IoT: Security Monitoring for IoT and 5G

Edgardo Montes de Oca
(edgardo@montimage.com)
Vinh Hoa La
(vinh@montimage.com)

Fed4FIRE+ - Open Call Experiments - Virtual Review

November 19th 2020

Agenda

- **Experiment description**
  - Concept and objectives
  - Background and motivation
  - Experiment setup
- **Demo**
- **Results Obtained and Findings**
  - w-iLab.t test
  - Log-a-Tec test
  - MMT-IoT achievements
- **Business impact**
- **Feedback**

Experiment Descriptions (1/5)

Concepts and Objectives

CONCEPTS

- MMT-IoT: Security solution for IoT networks.
- It performs complex network event correlation.
- Uses network events to detect security incidents.
- Network radio sniffing technology.

OBJECTIVES

- Analyse the performance and **scalability** of MMT-IoT:
  - Determine the limits and how to scale further.
- Perform **security** analysis in real deployments:
  - Detection of typical attacks in IoT.

General Objective: Provide a general view of the MMT-IoT solution and its efficiency in real-life scenarios.

Experiment Descriptions (2/5)

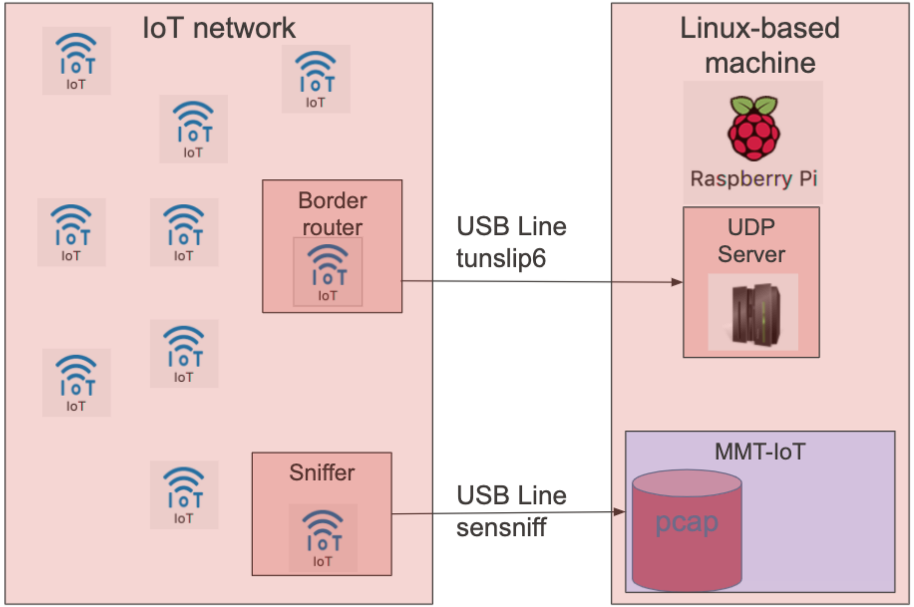
Background and Motivation

- Montimage developed an IoT security solution called MMT-IoT
  - PoC in the context of H2020 ANASTACIA project.
    - Tested in emulated scenarios.
    - No physical deployment was made so far.
- Montimage increased the Technical Readiness Level (TRL) of this solution from TRL 3 (PoC) to TRL 4 (validation in lab/testbeds) thanks to F4Fp-SME-Stage 1.
- MMT-IoT represents a new asset in the ecosystem of Montimage that we aim to exploit.
- In participating in F4Fp-SME-Stage 2, Montimage improved the solution to reach TRL 6.

Experiment Descriptions (3/5)

Experiment setup (1/3): General architecture

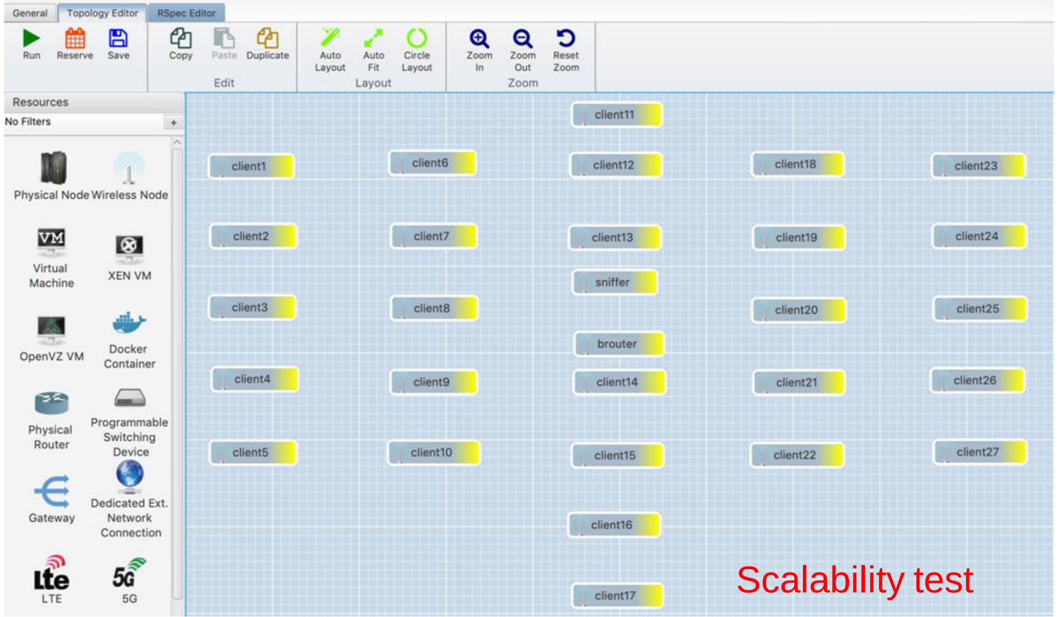
- Border Router: the edge device placed between the IoT network and the traditional IP network. It acts as the gateway collecting the sensed data sent by the IoT 6LoWPAN devices.
- Client: The clients and the Border Router self-organise among themselves to form a 6LoWPAN network.
  - **Normal** clients report sensed data every 10 seconds
  - **Attacker** client behaves interchangeably in the three modes (Normal, DoS attack and Dead modes).
- Sniffer: capturing all network frames and streaming them to the host.
- MMT-IoT: analyses IEEE 802.15.4/6LoWPAN traffic.



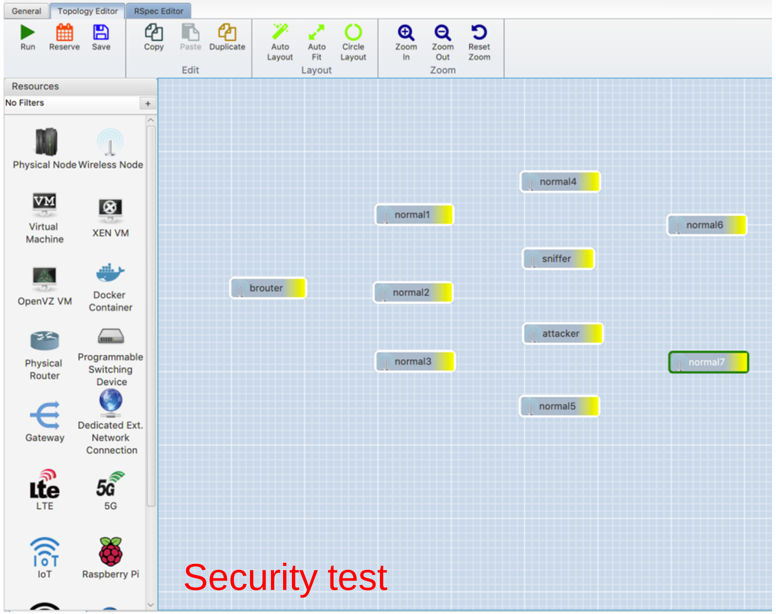
Experiment Descriptions (4/5)

Experiment setup (2/3): w-iLab.t (imec)

- Reserved nodes on iMinds, deployed nodes using jFED
- **Scalability** test: 27 clients (attackers and normal ones), 1 sniffer, 1 border router
- **Security** test: 7 normal clients, 1 attacker, 1 sniffer, 1 border router



Scalability test

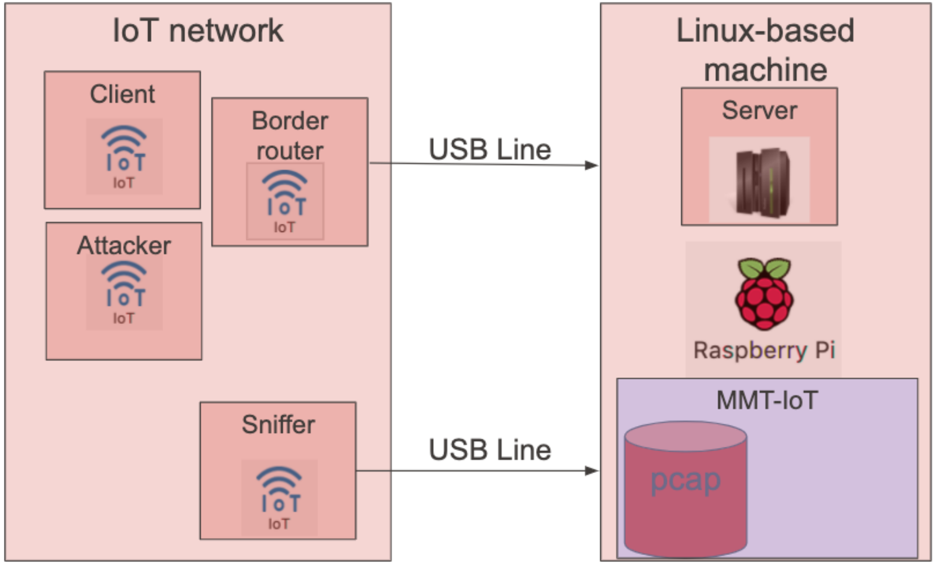


Security test

Experiment Descriptions (5/5)

Experiment setup (3/3): Log-a-Tec (JSI)

- 4 Zolertia-Remotes: Border Router, Sniffer, Attacker, Client
- A Raspberry Pi provides the Linux-based machine
- The devices were sent to JSI and placed at different positions near running Log-a-Tec testbed



IoT network

Client

Border router

Attacker

Sniffer

USB Line

USB Line

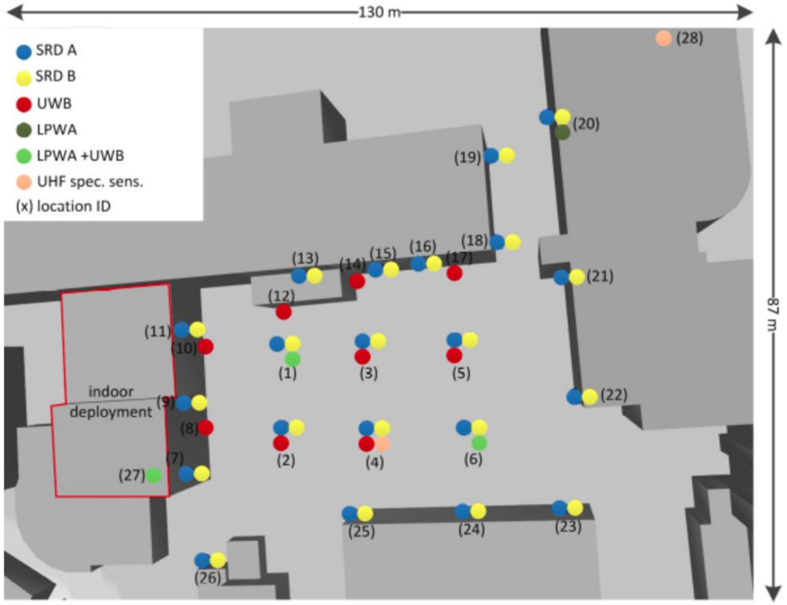
Linux-based machine

Server

Raspberry Pi

MMT-IoT

pcap

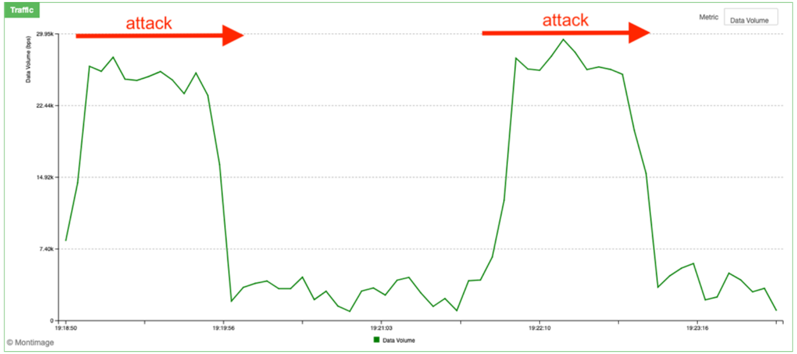


DEMO

Results Obtained and Findings (1/3)

w-iLab.t (imec)

- Scalability test:
  - Max data bitrate: 32 Kbps (Limit declared by Zolertia’s provider: 50 Kbps)
    - Physical factors affect the transmission, e.g., antenna, power, noise, etc.,
    - Such IoT devices are not always stable.
  - DDoS alerts were raised as expected when multiple nodes performed DoS attack



- Security test:
  - **Dead mode**, **DoS attack** and **incorrect FCS** (Frame Check Sequence) were correctly alerted.

Results Obtained and Findings (2/3)

Log-a-Tec (JSI)

- The sniffer captured not only traffic of Montimage's four devices but also the one generated by Log-a-Tec testbed (at least 10 nodes found)
- In general, more traffic was captured if:
  - The sniffer "S" (together with Montimage's equipment) is placed in a central position
  - The sniffer is placed close to the Border Router "BR" of JSI's network.
- **DoS attacks, Node failures** and **incorrect FCSs** (Frame Check Sequences) were correctly alerted
- Surprisingly, some **DDoS** alerts were observed although Montimage prepared only one Zolertia Remote acting as the DoS attacker.
  - Another node of IJS's testbed sending data at a very high rate?
  - JSI explained: "As Log-a-Tec devices use 6TiSCH standard, a node not receiving an acknowledgement for a sent packet would try to retransmit it (up to 8 packets in a row within a short interval of time, since the timeslot of the 6TiSCH is only 10ms)

Results Obtained and Findings (3/3)

Achievements and Lessons Learned

- We managed to perform all planned experiments despite that the deployment in IoT devices is not a simple task.
- A number of adaptations/modifications have been integrated to MMT-IoT so that the tool is able to work with IEEE 802.15.4/6LoWPAN traffic:
  - New plugins (for analysing and extracting the statistics).
  - Enabling the configuration of the netstack.
  - New security rules (for detecting misbehaviours)
  - New dashboards (for visualising the statistics and detections)
- MMT-IoT behaves as expected in real IoT environment.
  - Detecting security attacks
  - Determining the maximum throughput that depends mostly on the sniffing capacity.

Business impact (1/4)

Impact in Montimage's business

- Industrial-level validation of a new product (MMT-IoT) in a novel domain (IoT/5G):
  - Commercialisation of a version incorporating IoT networks in our existing products: **MMT-Box** solution for small networks and an **EPC-in-a-Box** solution for 4G/5G networks allowing monitoring network traffic in enterprises (e.g. Industry 4.0) or domestic networks.
  - Solution can be applied to a wide range of domains (e.g. smart cities, smart homes, e-health, manufacturing).
  - Demonstrator to convince future customers.

Business impact (2/4)

Value perceived. How FED4FIRE+ helped Montimage?

- Added value on implementing the solution on real IoT devices (e.g., Zolertia) in different contexts
  - Complex and expensive without Fed4FIRE+.
- Gain of knowledge about scalability and the bottleneck of the MMT-IoT solution.
  - Scalability testing in real environments better than in emulated scenarios.
- Adaptation to work on a real IoT environment.
  - Advance beyond a limited Proof-of-Concept phase.

Business impact (3/4)

Why did Montimage come to FED4FIRE+?

- Availability of different IoT deployments:
  - Federation of testbed infrastructures.
  - Access complex and expensive IoT deployments.
  - Speedup and improve the readiness of our solution.
  - Scalability testing in realistic scenarios.
  - Otherwise difficult to validate our solution.
- Collaboration with other stakeholders in different countries.
  - Small but effective financial support.

Business impact (4/4)

Follow-up activities

- An industrial paper being prepared for submission.
  - “Security Monitoring on real IoT-6LoWPAN testbeds”
- Marketing video:
  - https://drive.google.com/file/d/1mOZXNF5pNHO-Yti1G9_gbPTgKx_qZxyR/view?usp=sharing
- New IoT experimentations.
  - 10 more Zolertia Re-Motes newly purchased
- New H2020 projects and proposals
  - H2020 DigitBrain, H2020 Sancus, Green Deal (IoT for Ports, Fires)
- In contact with big industrials in France interested in the solution

Feedback (1/5)

Used Resources and Tools: jFed (1/2)

- Positive aspects:
  - Nodes can be configured in **a graphical manner** and/or by modifying/reloading the **RSPec text file**. It is, thus, easier for beginner users to design and configure simple experiments as well as for more experienced users to create/redo more complicated ones.
  - It is possible to save the **OS images** of the nodes for further reuse. Save a lot of time by avoiding re-installing the pre-required packages/tools.
  - **Scripts** can be added to be run at **OS boot** so that the nodes can be ready right after the experiment is launched.
  - **SSH connections** can be established so that one can intercept in real-time even when the experiment is running.
  - It is possible to **download/upload** files and repositories between a node of the experiment and our jFed host machine, as well as among the experiment nodes.

Feedback (2/5)

Used Resources and Tools: jFed (2/2)

- Points to be improved:
  - Transferring files sometimes slow (some bytes/s)
  - JFed experimenter could be frozen if the manipulation is done too quickly, especially when requesting online resources (e.g. select the saved OS images)

Feedback (3/5)

Used Resources and Tools: Testbeds

- w-iLab.t platform:
  - The “bare metal” access allowed us to easily deploy our software and test it with no further limitations.
- Log-a-Tec platform:
  - A bit more complicated because we had to deploy everything on the devices before sending them by post.
  - Happily SSH connection was provided so that we could debug whenever we needed and the partners at JSI were really helpful for performing the experiments.
  - However, with no possibility of directly accessing their testbed, we were not able to perform a more complete set of tests involving different configurations.

Feedback (4/5)

Documentation and support

- The documentation provided was quite extensive and based on the experience gained from the first phase, we had no problem setting up and running the experiments.

- We had to contact the individual testbeds for dedicated technical questions and everything was cleared up via email in a timely manner.

Feedback (5/5)

Procedure / Administration

- Administration work: level of work is not at all excessive.
- Feedback from platform operators: really responsive and helpful.
- Writing documents: effort required is not very high with respect to the effort allocated to the developments and experiments.
- Attendance to conference calls: none during the execution of the work, participation after will not represent much effort.

montimage

FED4FIRE

Co-funded by the European Union

Co-funded by the Swiss Confederation

This project has received funding from the European Union’s Horizon 2020 research and innovation programme, which is co-funded by the European Commission and the Swiss State Secretariat for Education, Research and Innovation, under grant agreement No 732638.

Thank you!

WWW.FED4FIRE.EU