Review SME Experimenting – Continuous Open Call: MMT-IoT

Edgardo Montes de Oca, Diego Rivera

Montimage

6th FED4FIRE+ Engineering Conference

Athens, October 15th - 16th, 2019

Experiment Descriptions (1/4)

Concepts and Objectives

CONCEPTS

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

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 simple attacks in IoT/5G.

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

Experiment Descriptions (2/4)

Background and Motivation

- Montimage developed an IoT security solution.
  - This work has been done under the H2020 ANASTACIA project.
- It represents a new asset that Montimage aims to exploit.
- However, the development was in a PoC state:
  - The solution was tested in emulated scenarios.
  - No physical deployment was made so far.
- Montimage aimed to increase the TLR of this solution:
  - From TRL 3 (PoC) to TRL 4 (validation in lab/testbeds).

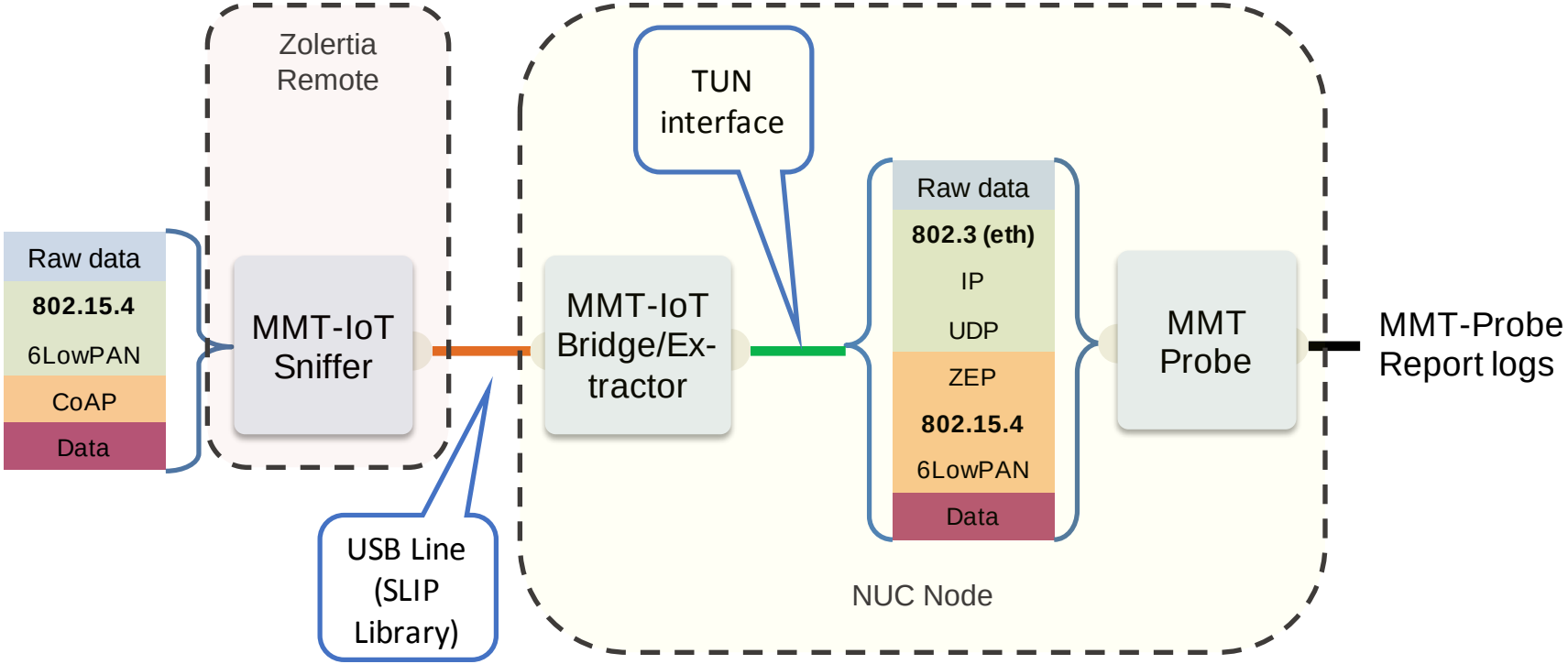
Experiment Descriptions (3/4)

Experiment setup

- Deployment in the w.iLab testbed.
- Makes use of the NUC nodes and Zolertia ReMote IoT nodes.
- The idea was to map NUC nodes to a defined distribution using jFED Design.

Experiment Descriptions (4/4)

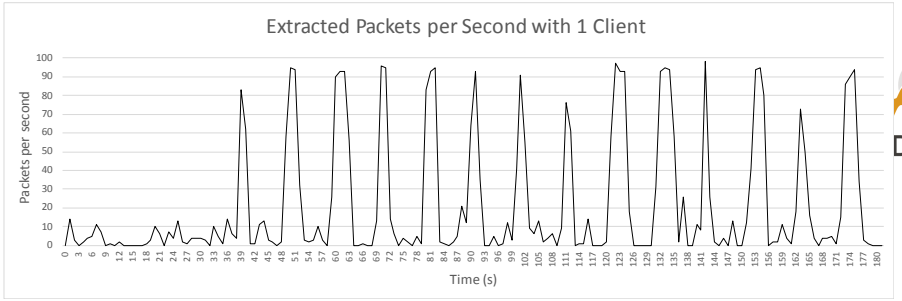
Solution Design

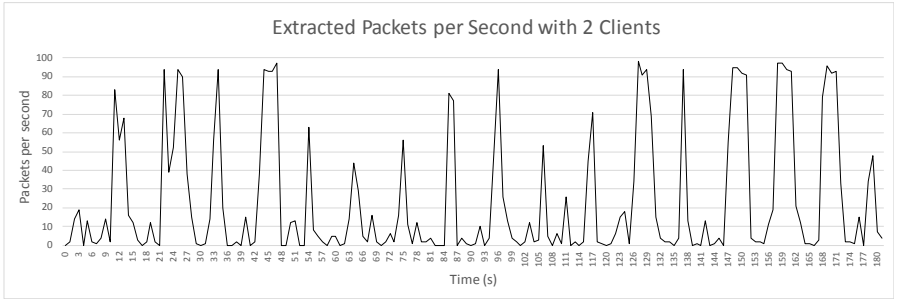


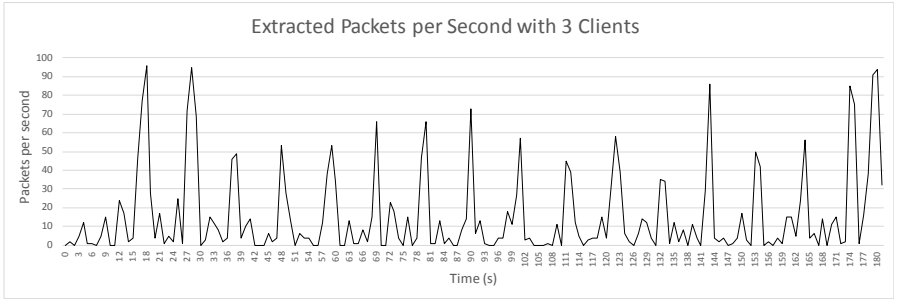
Project Results (1/3)

Measurements

- A first test (1 client) aimed to check the detection of a simple attack.
  - The attack was correctly detected.
- Tests were executed with different number of clients.
  - The idea was to perform initial scalation tests.
- These tests show that a maximum number of packets per sec. are extracted (probably due to the radio channel limits).

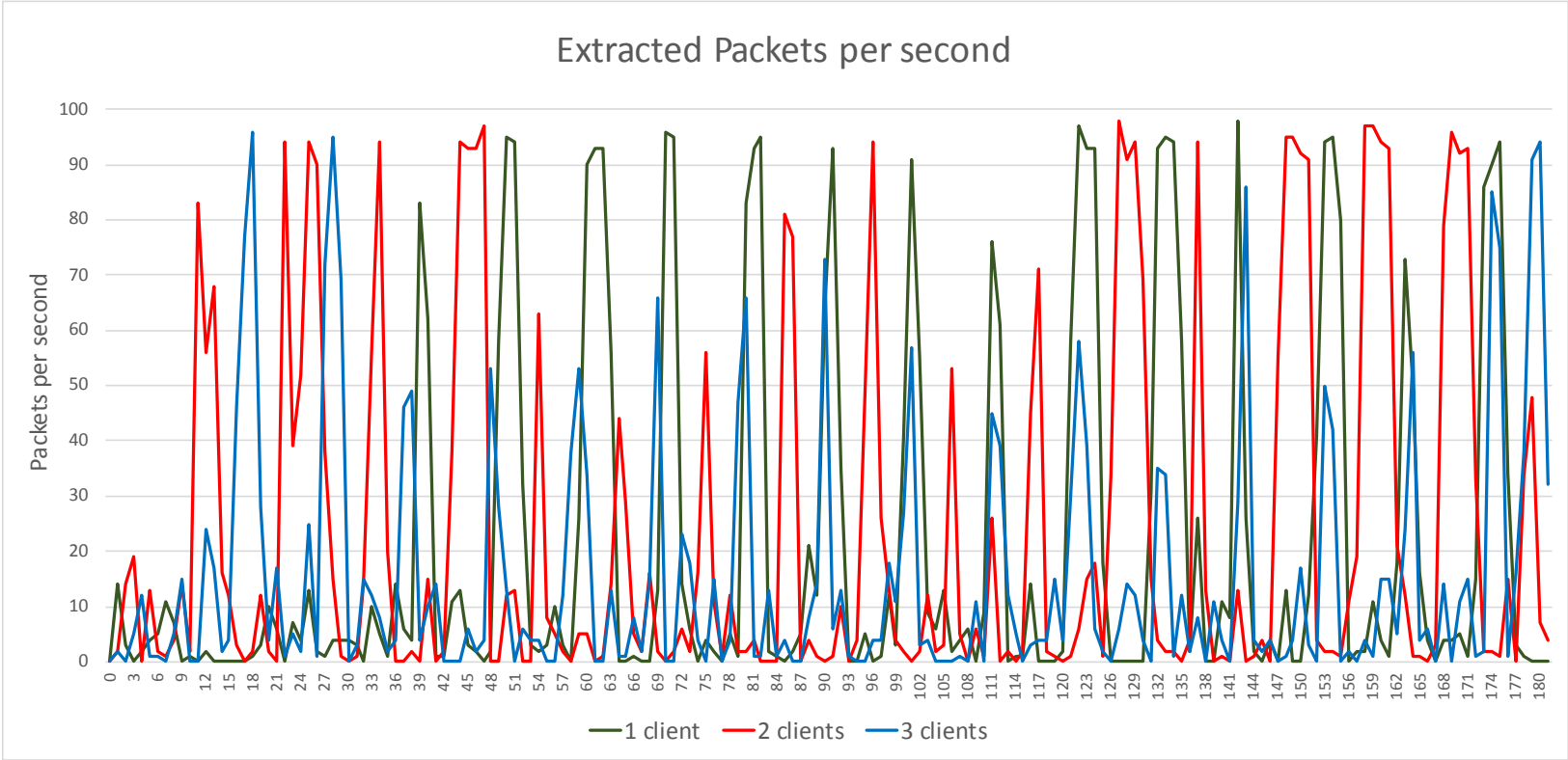






Project Results (2/3)

Measurements



Project Results (3/3)

Lessons Learned

- Deployment in IoT is not a simple task.
  - Despite this, we managed to deliver the solution.
- MMT-IoT behaves as expected in the w.iLab testbed:
  - MMT is capable of extracting packets, and detecting attacks.
- Performance is an open issue:
  - Need to study the limits in the extraction of packets and determine if it is due to the channel limits or other causes.
- This makes it interesting to continue the experimentations.

Business Impact (1/4)

How FED4FIRE+ helped Montimage?

- Gain of knowledge:
  - The deployment of our tool in different realistic IoT-based environments.
  - The performance/scalability of our solution and identification of the improvements needed.
- Proof of Concept working on real IoT testbeds:
  - Requirements from different IoT-based architectures
  - Issues to be addressed: performance, scalability and genericity.

Business Impact (2/4)

How FED4FIRE+ helped Montimage?

- Stage 1 project:
  - Shows the feasibility of obtaining high quality solution and helped identify the issues that would be interesting to address.
  - Demonstrator to convince future customers.
- Industrial-level validation of a new product (MMT-IoT):
  - Commercialization after one final testing phase.
  - Solution can be applied to a wide range of domains (e.g. smart cities, smart homes, e-health, manufacturing).

Business Impact (3/4)

Concrete results and follow-up

- Publication of results in ICTSS (http://ictss2019.centralesupelec.fr):

IoT Network Monitoring and Test of an Industrial Solution on Fed4Fire+ Platforms

Diego Rivera, Edgardo Montes de Oca, Wissam Mallouli, Ana Cavalli, Brecht Vermeulen, and Matevz Vucnik. In the proceedings of the 31th IFIP International Conference on Testig Software and Systems IFIP-ITCSS 2019. Paris, October 15-17, 2019.

- Application to Phase 2
- H2020 cascading calls and proposals:
  - IoT monitoring in trains, manufacturing, city…
- Planned demonstration in booth:
  - European Cyber Week

Business Impact (4/4)

Why did Montimage choose 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.

Feedback (1/5)

Used Resources and Tools

- Montimage used the w.iLab testbed:
  - Reserved 16 NUC devices on the “datacenter” floor.
- Testing plans were arranged with LOG-a-TEC testbed:
  - However, logistic issues delayed the deployment.
- In w.iLab, we reserved test time:
  - Montimage used effectively 25% of that time.
  - This is due to last-minutes adaptations necessary for deploying.
- Deployment was made with the help of jFED tool:
  - During initial tests, we found a bug in the tool.
    - The jFED tool was experiencing unexpected crashes on macOS, not allowing to connect via SSH into the remote machines.
  - This was fixed a few days later.

Feedback (2/5)

Used Resources and Tools

- w.iLab is a platform with several advantages:
  - The reservation system allows locking the resources needed.
  - Root access to the NUC nodes allows flexible deployment of software.
  - Software tools allow easy deployment of the software (jFED).
- Some disadvantages:
  - Old and updated tutorials still coexist.
  - Information is not always 100% clear, and most of the times, too technical.

Feedback (3/5)

Used Resources and Tools

- LOG-a-TEC platform is an attractive platform for 5G:
  - Central management of the deployed software.
  - 5G and IoT nodes coexist in the deployment.
- Montimage planned deployment on this platform:
  - Platform restrictions were considered and an alternative deployment was agreed:
    - Physical deployment of MMT-IoT solution.
    - On-site execution of attacks.
  - Despite this, logistic issues would have delayed the project (timeframe too short for sending and deploying the devices).
- To avoid these delays, only w.iLab was used for all the planned tests.

Feedback (3/5)

Used Resources and Tools

	w.iLab	LOG-a-TEC
Planned test	Initial Scalability Test	Deployment and Detection Test
Involved nodes	5	3
Goals	• Stress MMT-IoT Sniffer • Determine its limits • Discover potential optimization points	• Deploy along with deployed devices. • Trigger attacks in real IoT environments • Detect basic attacks using Sniffer
Advantages	• Root access to NUC and IoT nodes. • Remote software deployment (jFED)	• Deployment with IoT nodes already deployed
Limitations	• Access to “known” network.	• IoT nodes non flashable. • Connectivity with new IoT nodes is challenging. • On-side deployment requires substantially more time

Feedback (5/5)

Added Value of FED4FIRE

- FED4FIRE provides a diverse set of resources and facilitates setting up experiments:
  - This is a cost-effective advantage for experiments by SMEs.
- The easiness to deploy is a huge advantage:
  - This allows companies to run PoC solutions.
- At larger scale, these platforms can be used for validation on real scenarios:
  - A large-scale deployment requires longer planning and more effort.
  - However, the flexibility of FED4FIRE platform allows running experiments on different platforms and configurations.


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.

WWW.FED4FIRE.EU