MMT-IoT: A DPI Security Solution for IoT

GOALS

- Perform security analysis in real deployments:
  - Detect typical attacks (DoS/DDoS, Node failure, incorrect FCS) in IoT/5G.
- Analyse the performance and the scalability of MMT-IoT:
  - Determine limits and how it can scale further.

General Objective:

Evaluate the MMT-IoT solution and its efficiency in real-life scenarios.

CHALLENGES

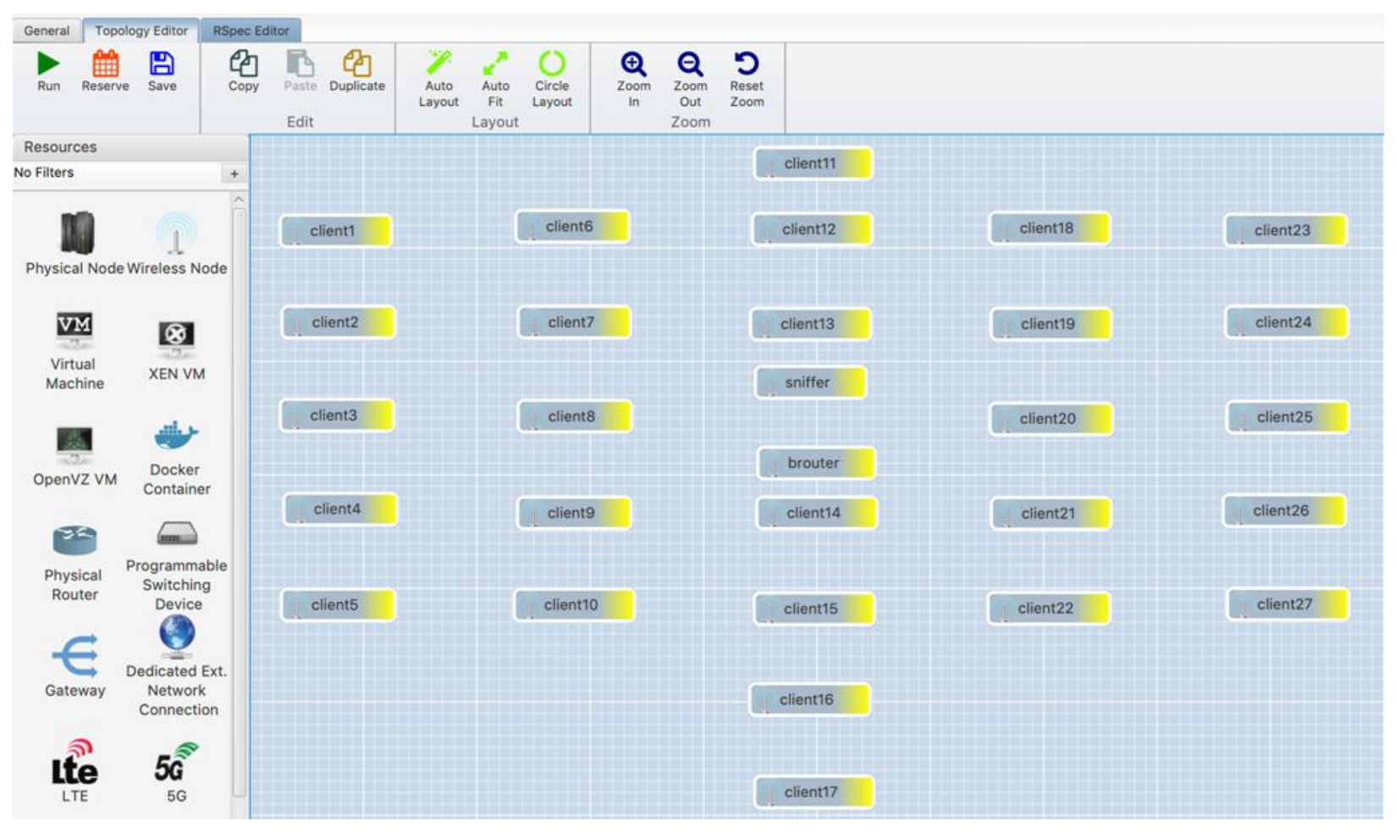
- Adaptations were needed to deploy in real IoT devices:
  - Initial Proof of Concept was developed in an emulator.
  - Development on real radio drivers was required.
- Communication with existing IoT deployment required technical efforts:
  - Fine tuning of the radio parameters to allow communications between two IoT nodes.

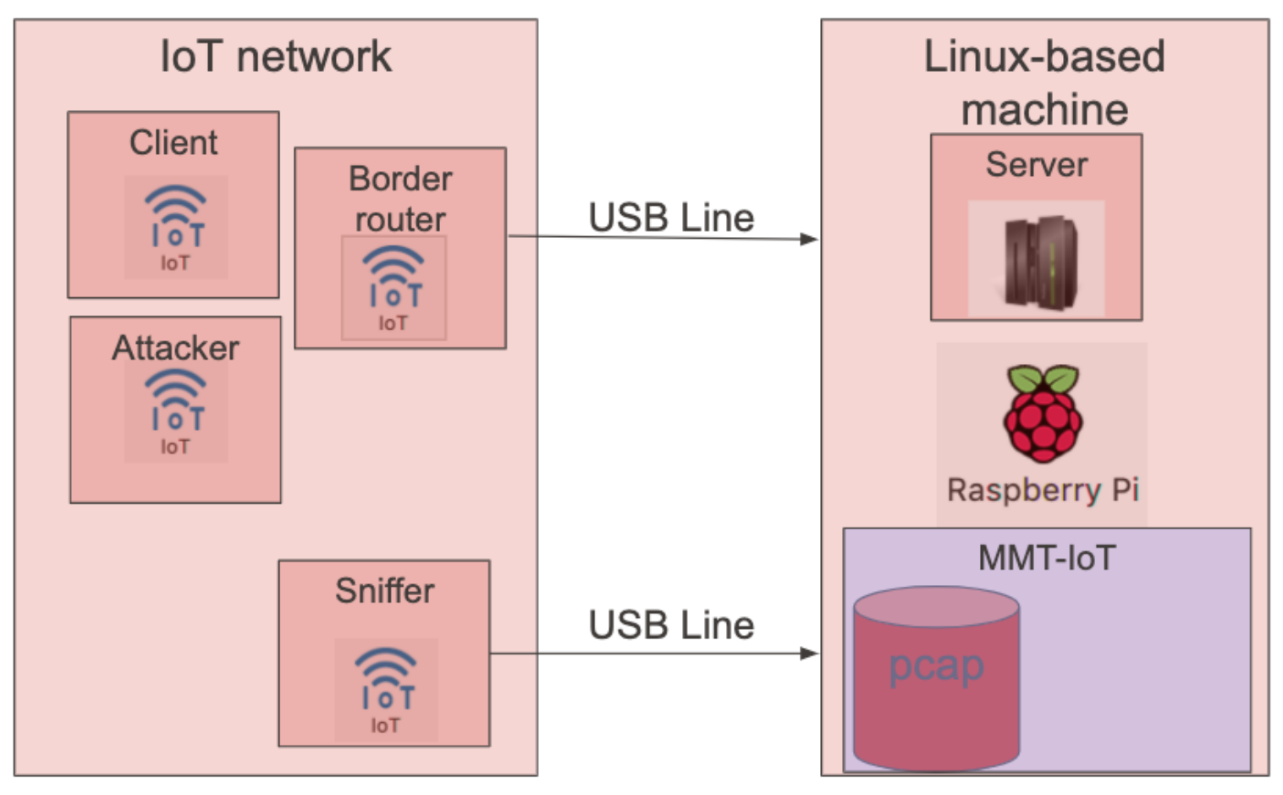
DEMO SETUP

Experiments performed using the w.iLab.t NUC nodes and Log-a-Tec testbed, both with Zolertia Re-Mote IoT Devices.

Sniffing part was run on the Zolertia motes, and analysing part on the Linux-based machine (NUC machine for w.iLab.t and Raspberry Pi for Log-a-Tec)

MMT-IoT used as security analysis engine, for detecting attacks on the IoT network (e.g., DoS/DDoS, Node failure, incorrect FCS)

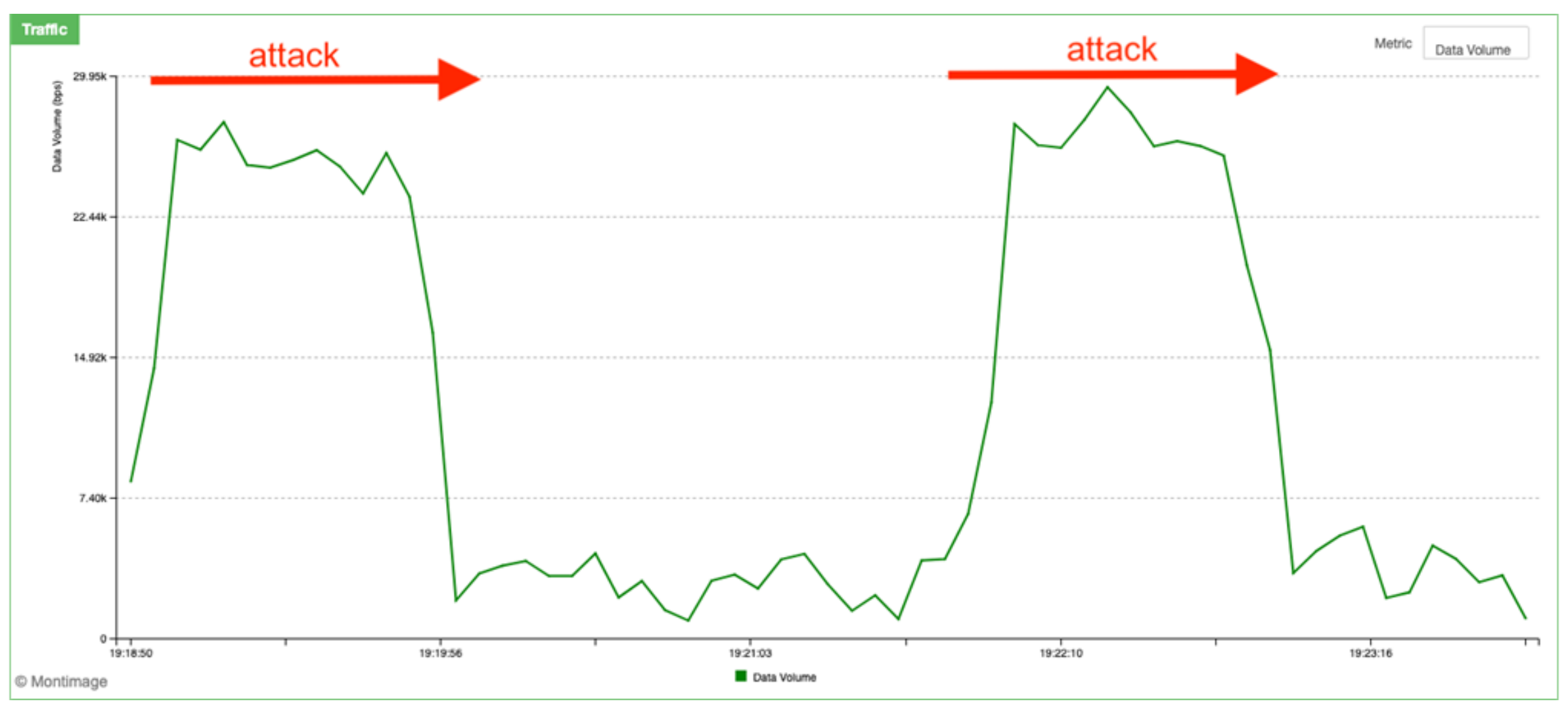




RESULTS

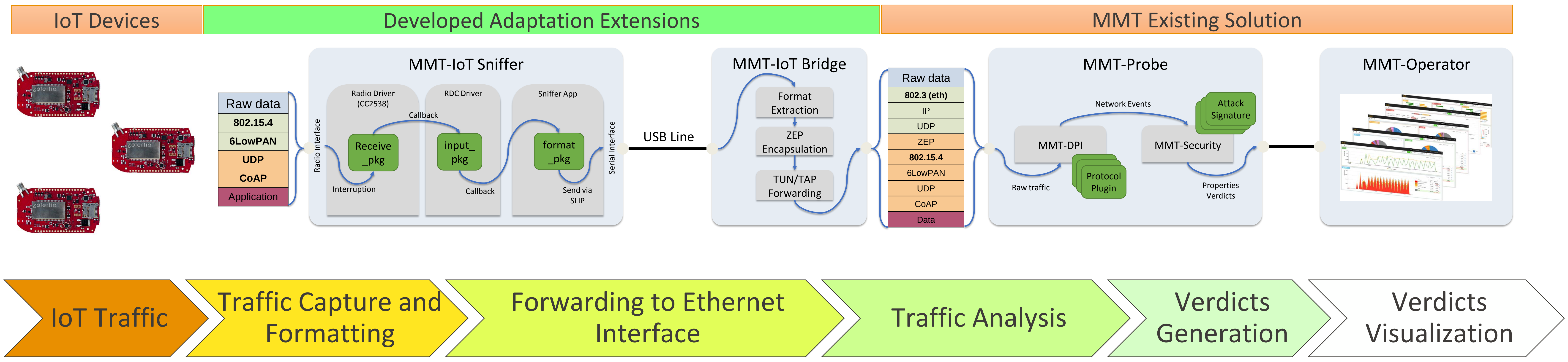
Scalability test with 27 clients showed that the solution is capable of dealing with a maximum traffic bitrate of 32Kbps, lower than the declared 50Kbps data rate of Zolertia's providers.

Security test showed that all the generated attacks (DoS/DDoS, Node failure, incorrect FCS) were alerted as expected.



MMT-IoT DESIGN

The *Montimage Monitoring Tool (MMT)* has been designed for traditional ethernet Networks. Adaptations were required to use DPI techniques in IoT environments. The general design of the MMT-IoT is shown below:



CONCLUSIONS

- The deployment allowed validating the MMT-IoT solution in a real Environment:
  - Detection of cyber attacks using DPI on IoT networks.
  - Findings of the maximal throughput that MMT-IoT can handle, the bottleneck (sniffer) and how in can scale further.
- Open questions:
  - What are the real limits if a more powerful dedicated node is used for performing the sniffing task.
  - What about other evasions / more sophisticated attacks on other IoT protocols?

ACKNOWLEDGMENTS & CONTACT

Work was supported by Fed4Fire+ (https://www.fed4fire.eu/)
Special thanks to ***imec*** and ***JSI*** that provided their testbed and support.
The initial development was done in the H2020 ANASTACIA project (http://www.anastacia-h2020.eu/).

Team:

- Edgardo Montes de Oca (edgardo@montimage.com)
- Wissam Mallouli(wissam@montimage.com)
- Vinh Hoa La (vinh@montimage.com)