IEEE/IFIP Network Operations and Management Symposium
8-12 May 2023 // Miami, FL // USA

A Scalable Cyber Security Framework for the Experimentation of DDoS Attacks of Things

Davi D. Gemmer (UFMG), Bruno H. Meyer (UFPR),

Emerson R. de Mello (IFSC), Marcos Schwarz (RNP),

Michelle Wangham (UNIVALI), Michele Nogueira (UFMG)

MENTORED

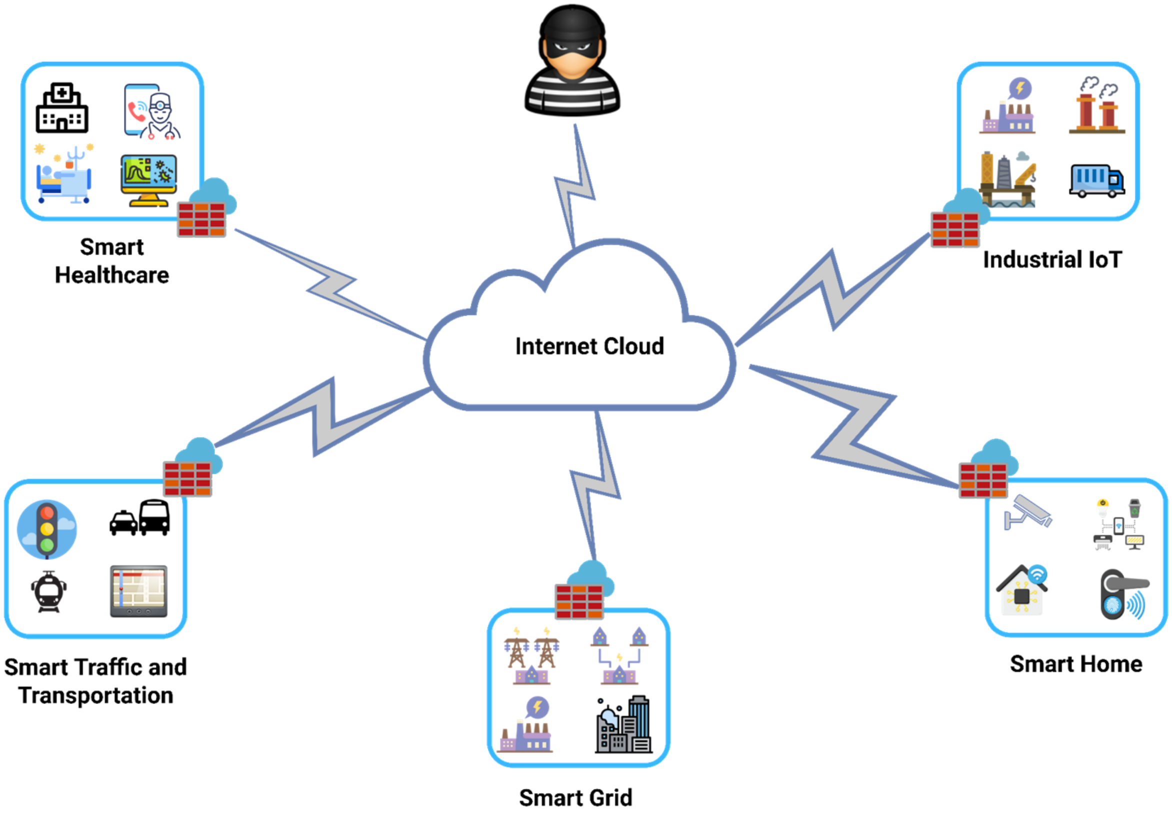
FAPESP

cgi.br
Comitê Gestor da
Internet no Brasil

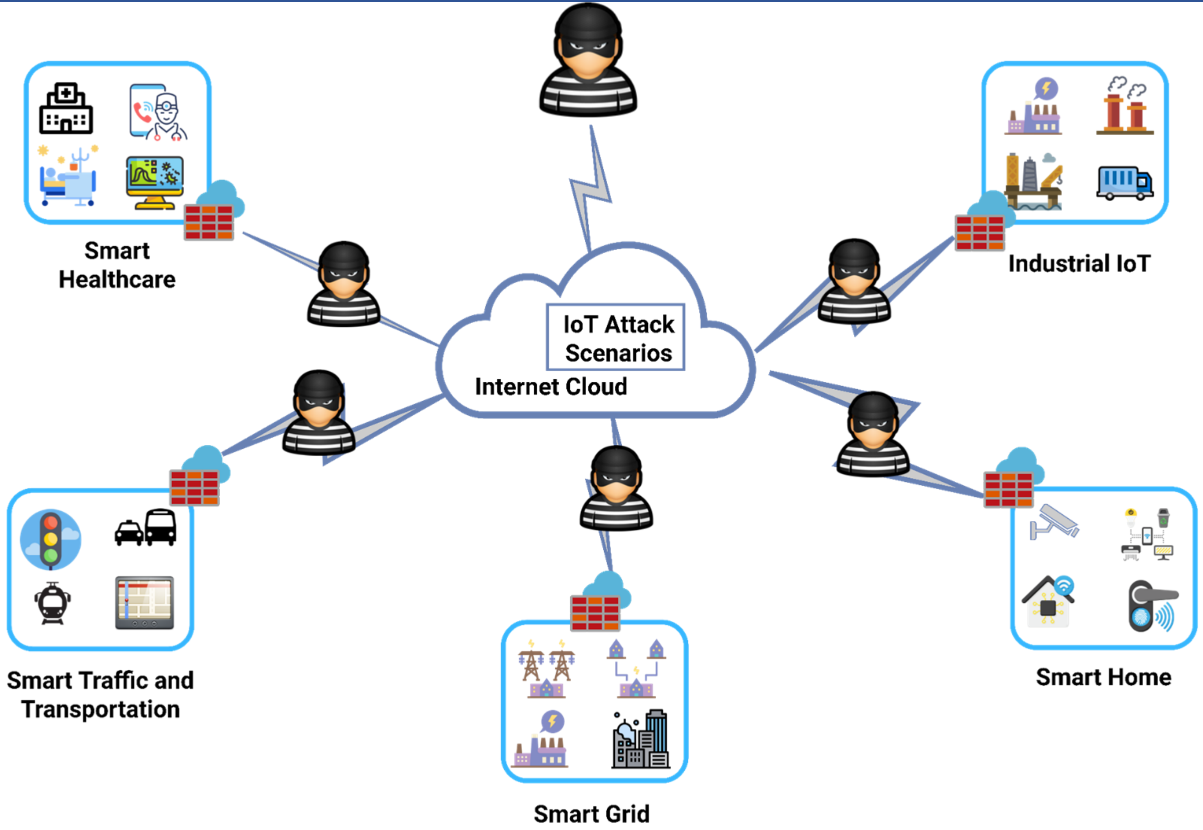
Agenda

- Introduction
- Related Work
- Cyber security framework for DDoS of Things (DoT)
- Mentored testbed
- Case study
- Concluding remarks

IoT has amplified security challhenges



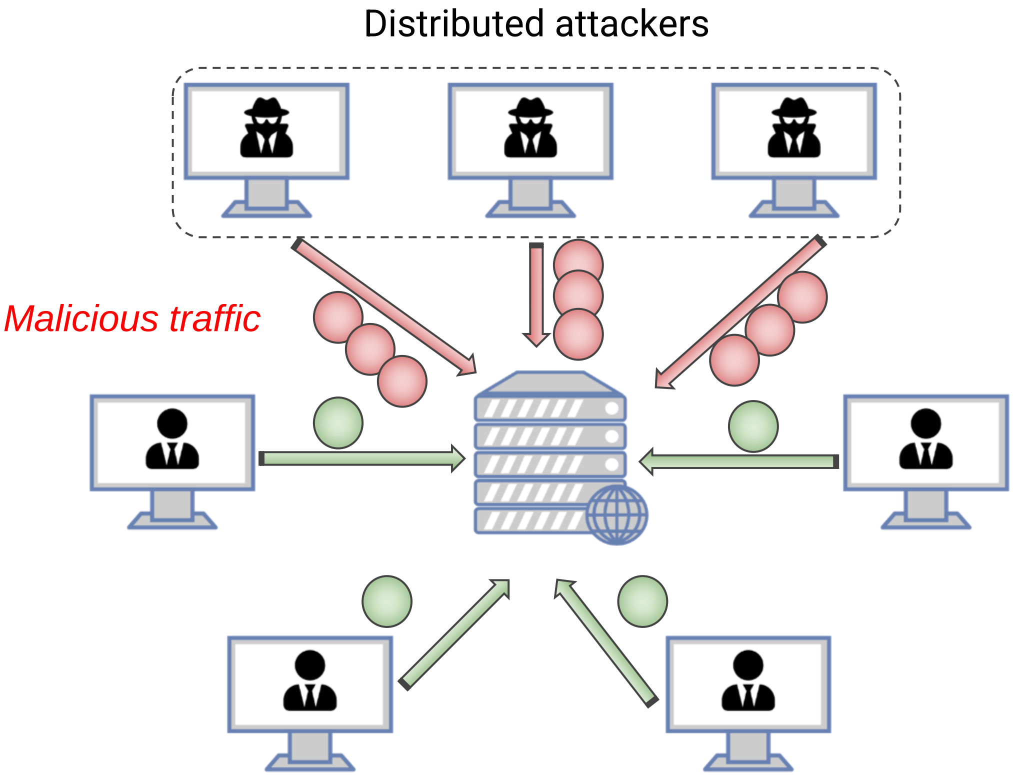
Security of IoT devices



DDoS Attacks

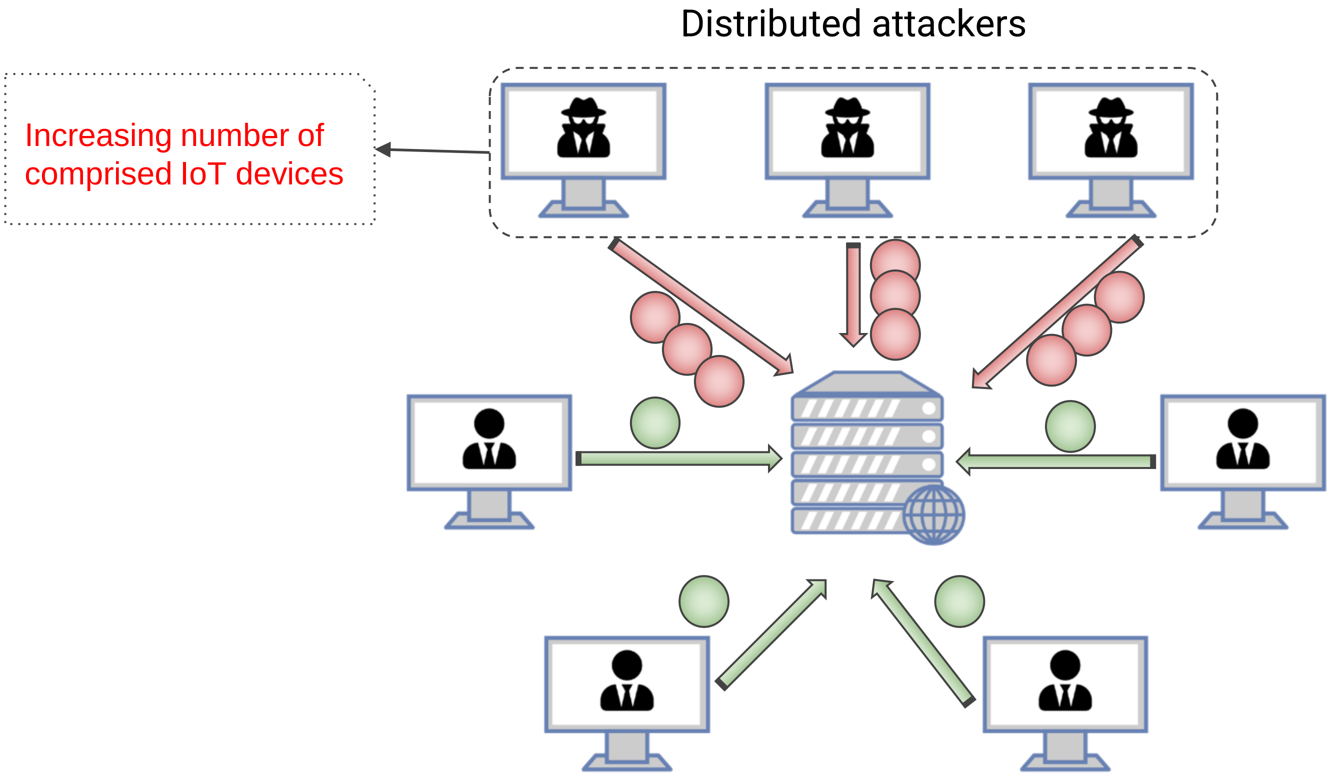
If an attacker has access to several devices

- 🟢 Benign traffic
- 🔴 Malicious traffic
- Clients
- Attackers
- Server (DDoS Target)
- Failed connection



Extended the size of DDoS (DoT Attacks)

- 🟢 Benign traffic
- 🔴 Malicious traffic
- Clients
- Attackers
- Server (DDoS Target)
- Failed connection

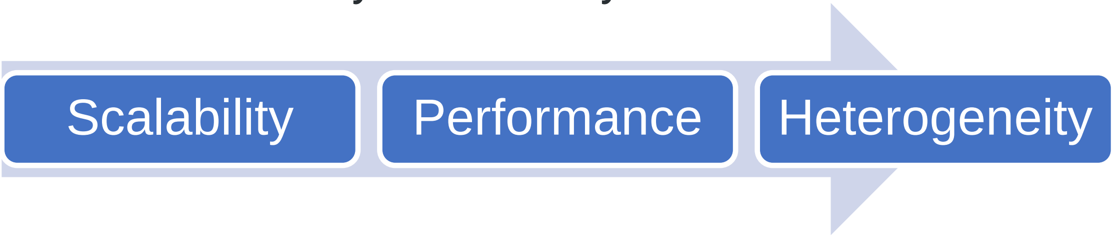


Distributed attackers

Increasing number of comprised IoT devices

Motivation

- Solutions to prevent, detect and mitigate DoT attacks require appropriate tools and methods to **test and validate** them
  - ○ Simulations
  - ○ Lack of realistic experimental environments that meet specific requirements for IoT cyber security



It urges a **framework** to support and guide the development of testbeds

Related Work

Experimental environments

testbeds focusing on cyber security

IoT testbeds

focusing on cyber security and IoT

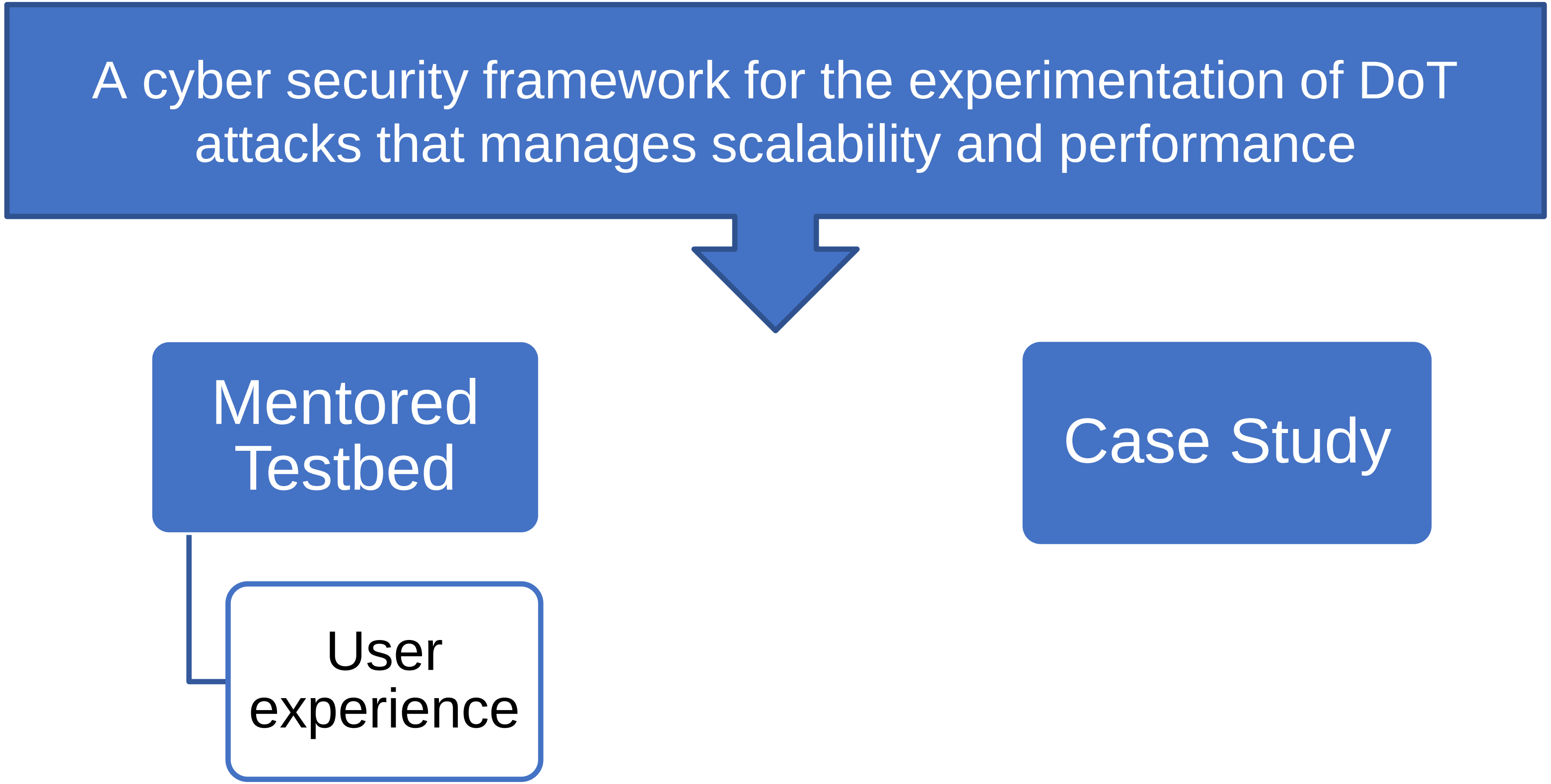
Related Work

- **DETERLab**: designed for large-scale emulation and experimentation; it ignores the context of wireless network
- **FIT IoT-LAB**: offers a platform for researchers to build, evaluate and optimize protocols, applications, and services; it lacks traffic isolation
- **Gotham**: is based on the GNS3 network emulator and provides a set of tools for experimenters to carry out DoS attacks; scalability is still an issue.
- **Takeoglu and Tosun**: low-cost testbed based on off-the-shelf hardware and open-source software (IoT devices); it also does not address scalability.
- **EdgeNet**: comprises virtual machines (VM) interconnected by Kubernetes-based implementation; it does not consider DoT attacks (with heavy network loads)

Problem

- There is still a place for improvement
- A need for well-defined references to assist in designing testbeds for cyber security, concerned with DoT attacks
- A gap defining the requirements to guide the implementation of realistic and geographically distributed environments (scalability and performance)
- Considering IoT devices heterogeneity

Purpose of this paper



A cyber security framework for the experimentation of DoT attacks that manages scalability and performance

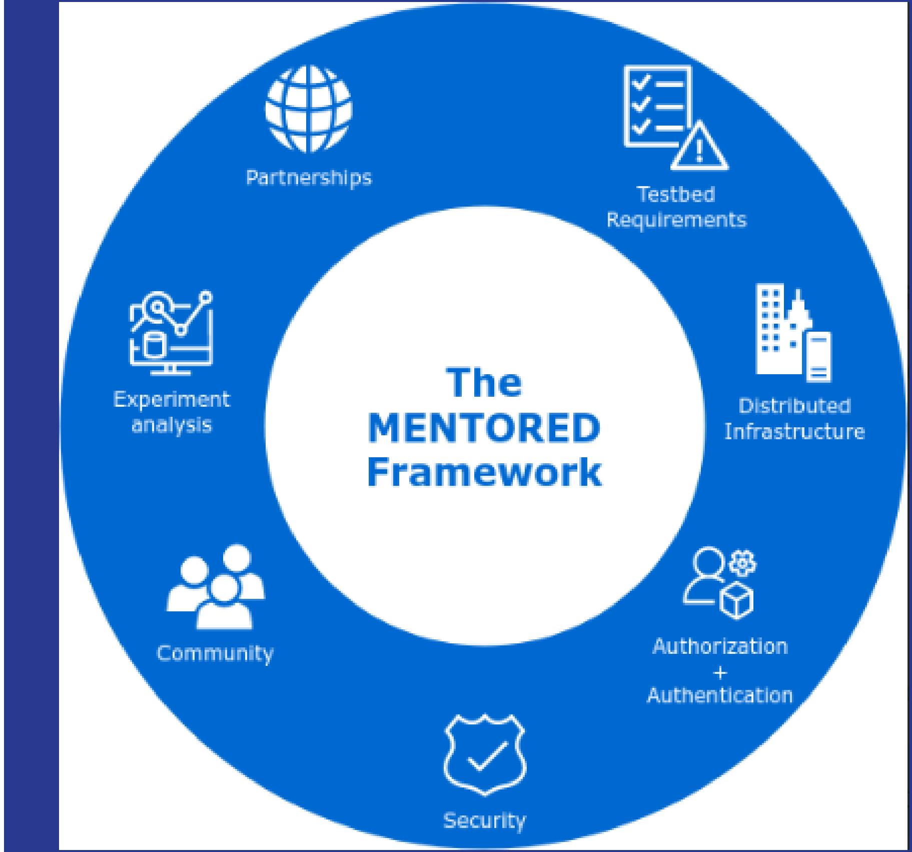
Mentored Testbed

User experience

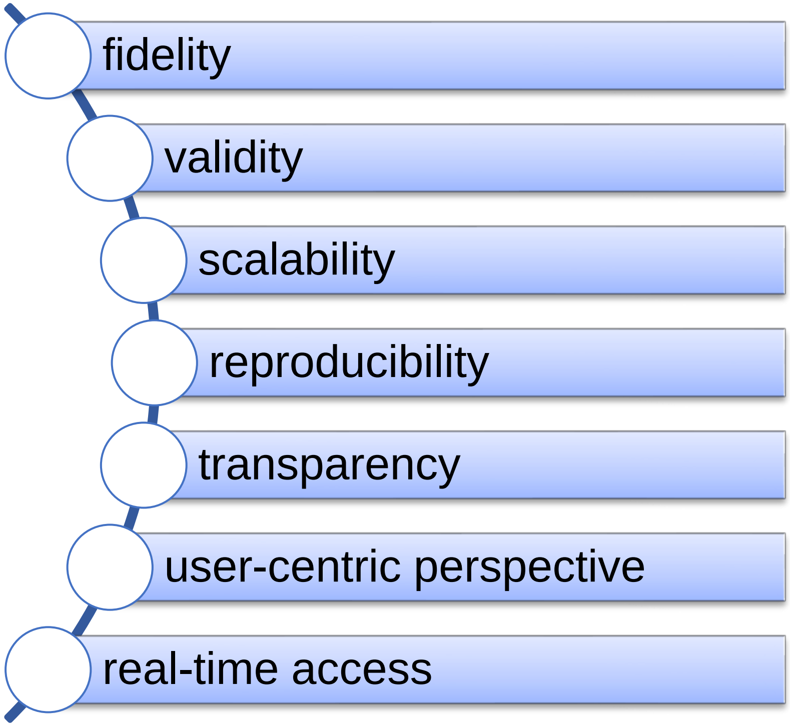
Case Study

Solution

Cyber security framework

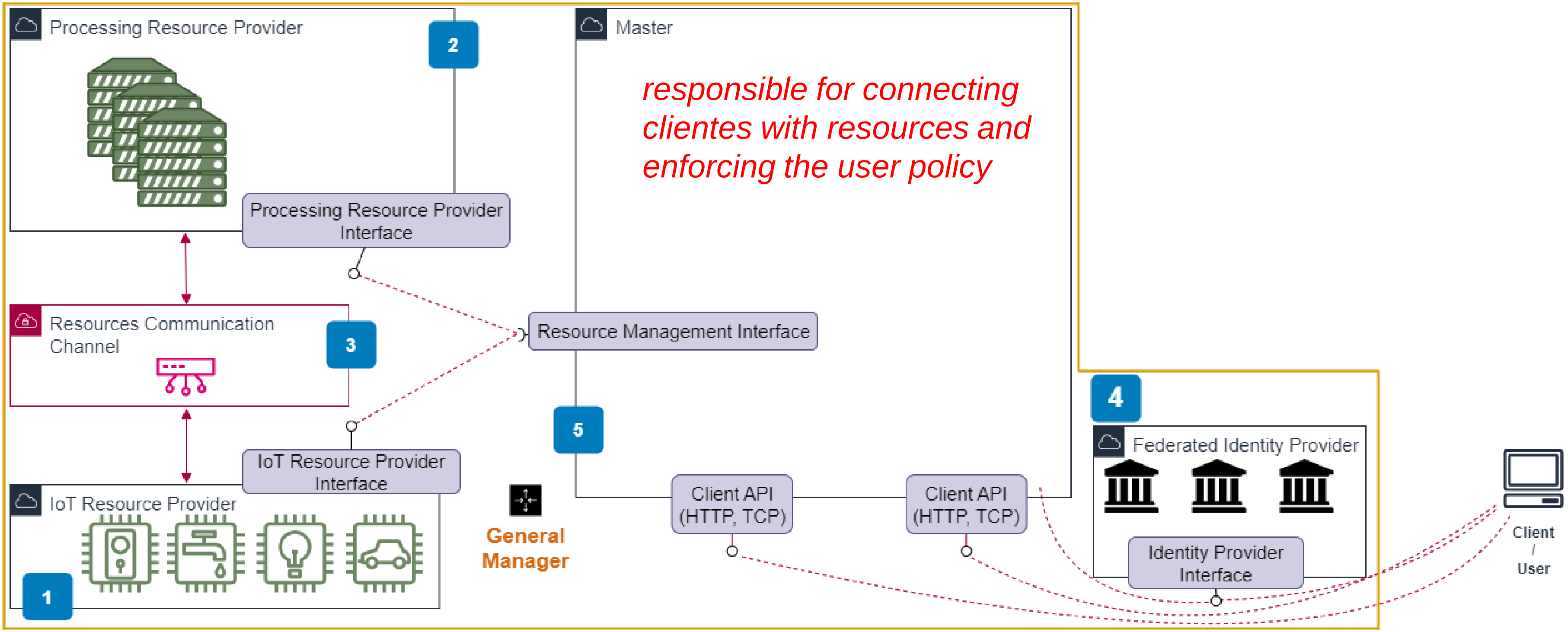


Framework Requirements



- fidelity
- validity
- scalability
- reproducibility
- transparency
- user-centric perspective
- real-time access

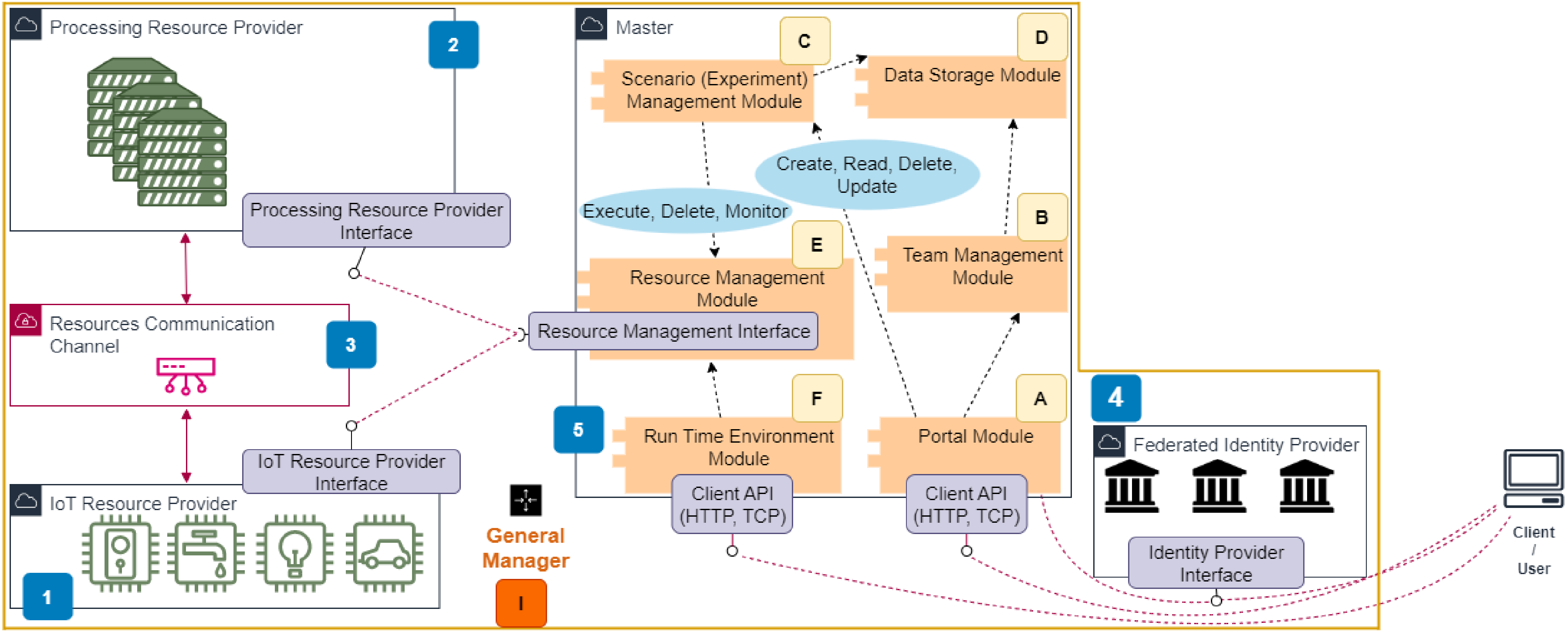
Framework Entities



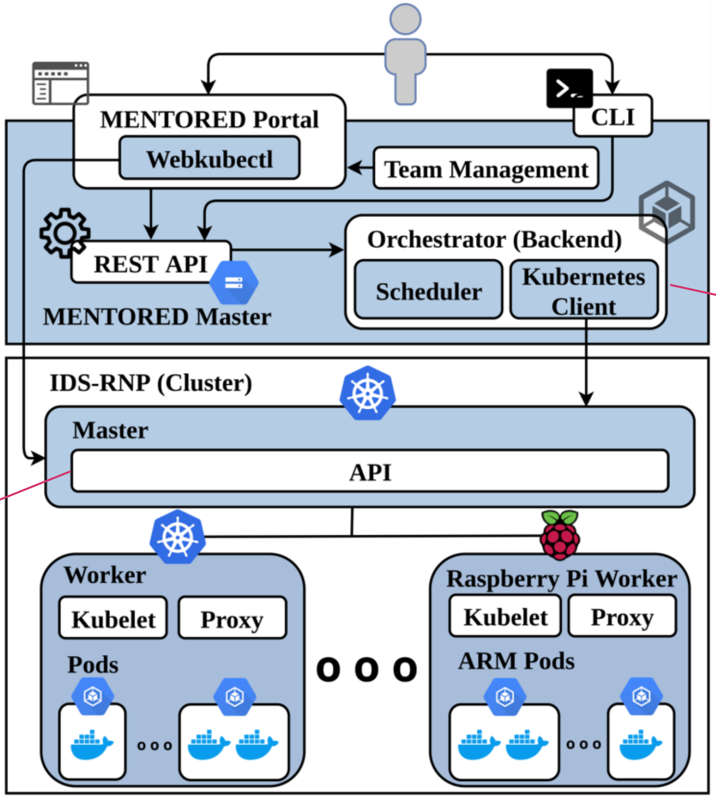
Processing Resource Provider
2
Processing Resource Provider Interface
Master
Resource Management Interface
Resources Communication Channel
3
IoT Resource Provider Interface
IoT Resource Provider
1
5
General Manager
Client API (HTTP, TCP)
Client API (HTTP, TCP)
4
Federated Identity Provider
Identity Provider Interface
Client / User

responsible for connecting clientes with resources and enforcing the user policy

Framework Modules


Processing Resource Provider
2
Processing Resource Provider Interface
Resources Communication Channel
3
IoT Resource Provider Interface
IoT Resource Provider
1
Master
C
Scenario (Experiment) Management Module
D
Data Storage Module
Create, Read, Delete, Update
Execute, Delete, Monitor
B
Team Management Module
E
Resource Management Module
Resource Management Interface
F
Run Time Environment Module
A
Portal Module
5
Client API (HTTP, TCP)
Client API (HTTP, TCP)
General Manager
I
4
Federated Identity Provider
Identity Provider Interface
Client / User

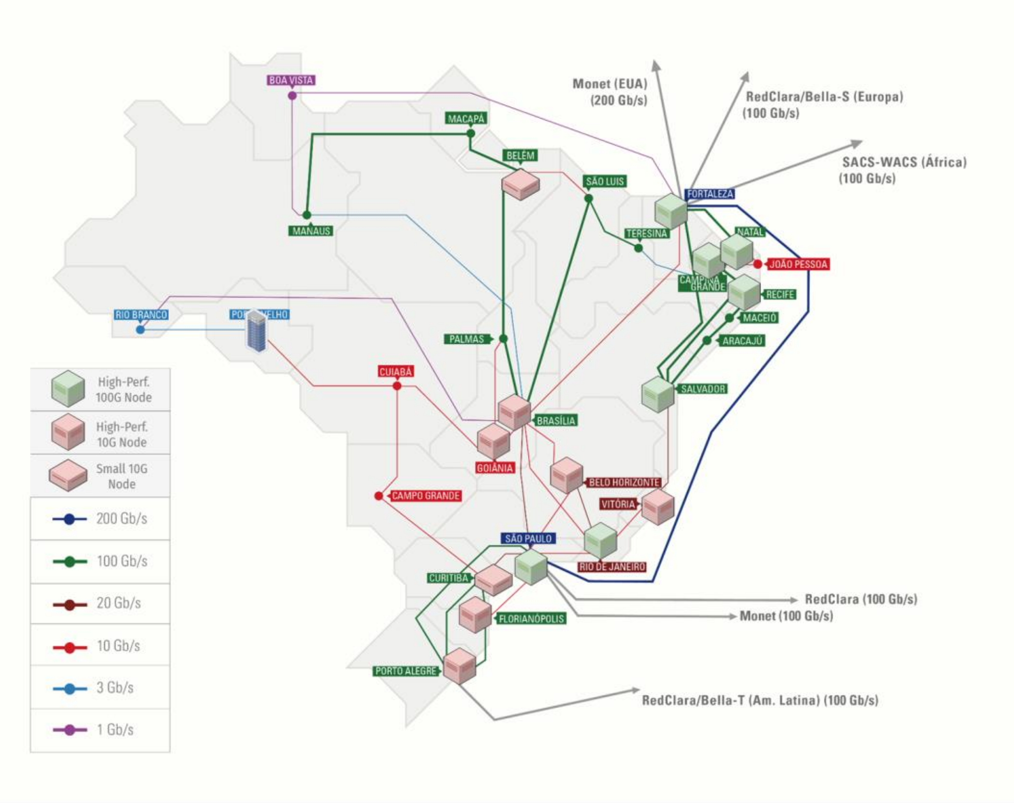
Mentored Testbed



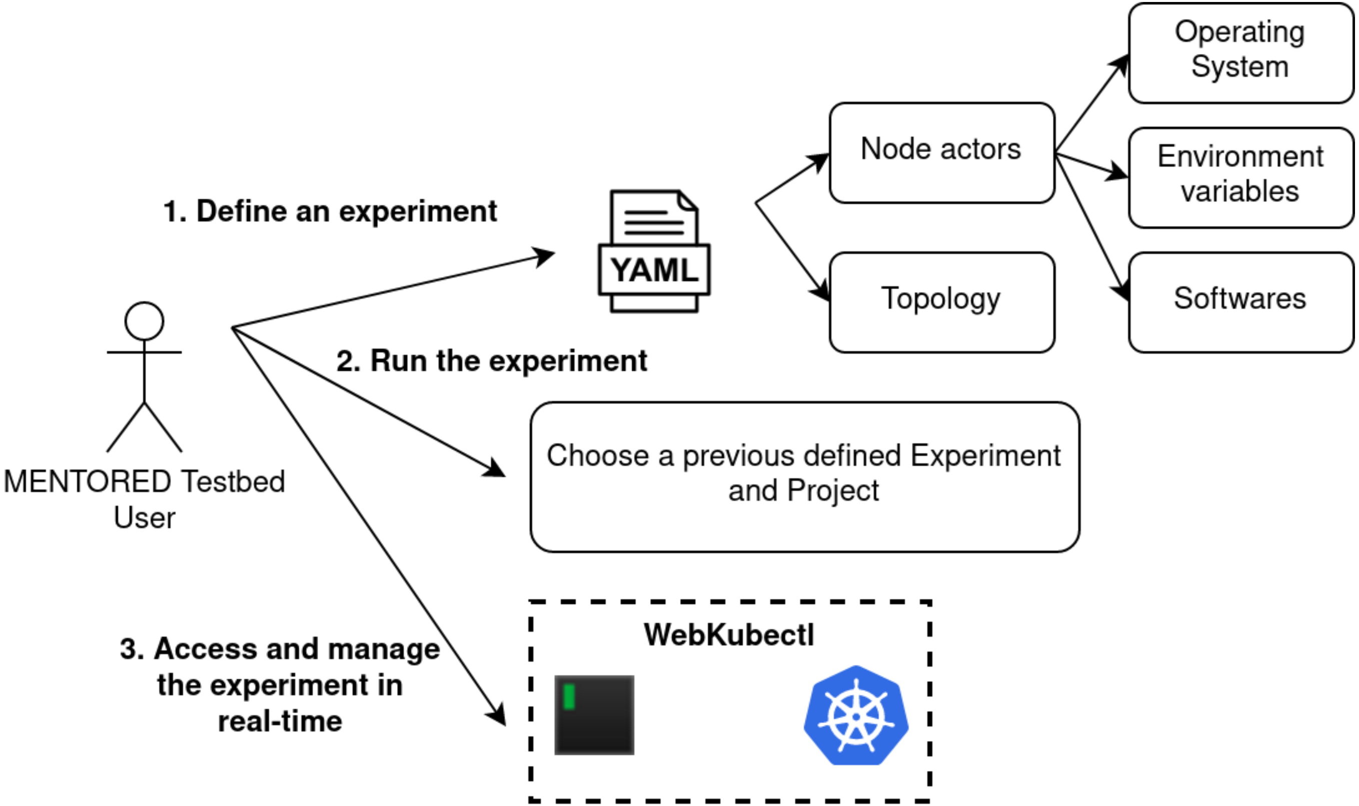
Backend: code executed on the server

KnetLab operations

IT Infrastructure - IDS-RNP



User perspective



MENTORED Testbed User

1. Define an experiment

2. Run the experiment

3. Access and manage the experiment in real-time

Choose a previous defined Experiment and Project

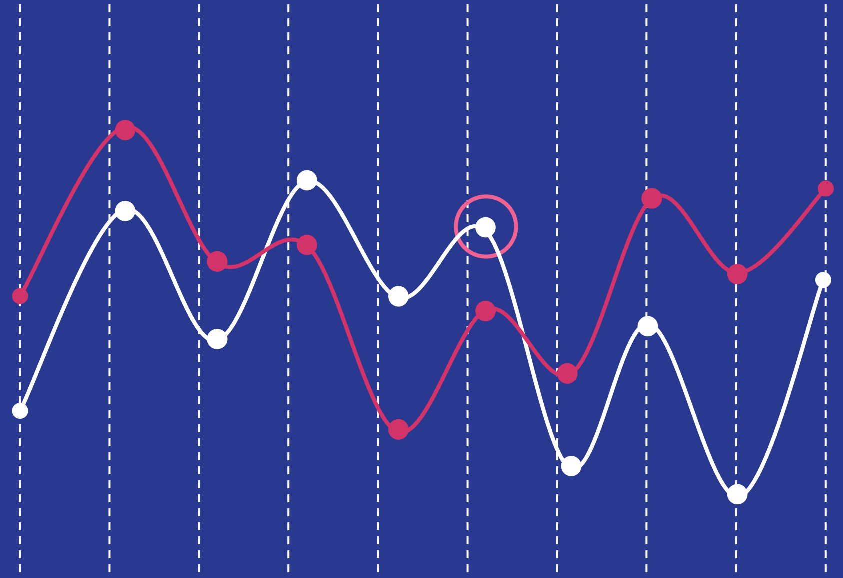
WebKubectl

IT Infrastructure

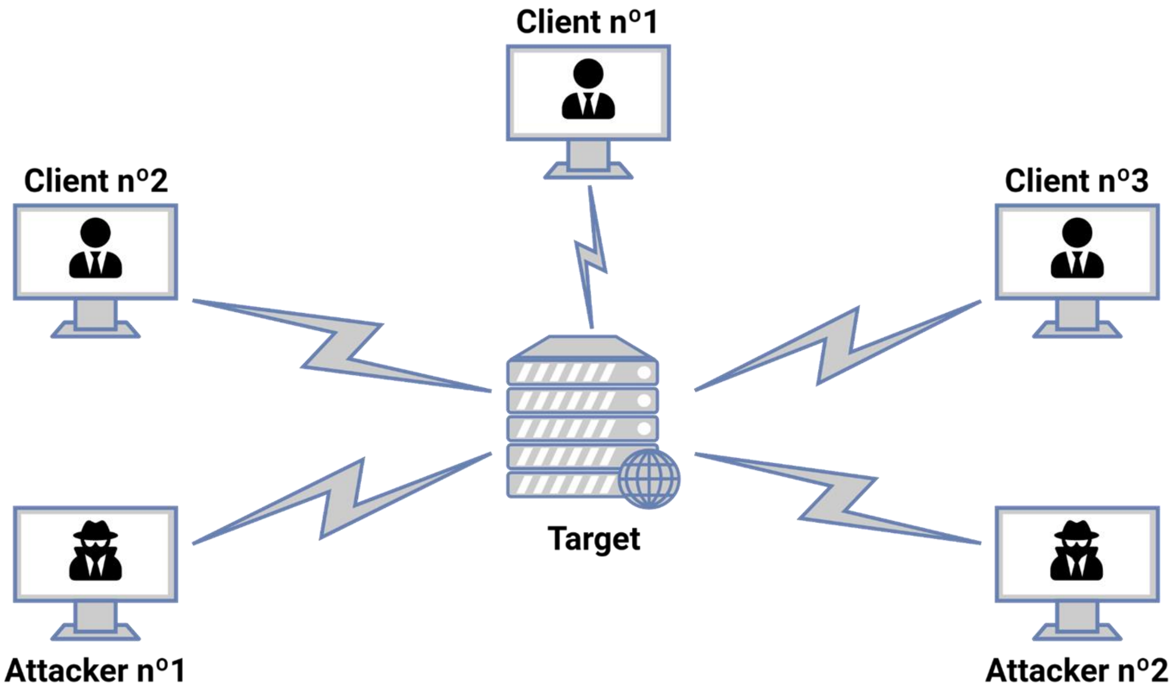
- Frontend
  - React.js

- Backend
  - Kubernetes
  - Python 3
  - Kubernetes Python API
  - Webkubectl
  - Django (Development of a REST API)
  - Knetlab

Case Study



Simple DDoS scenario



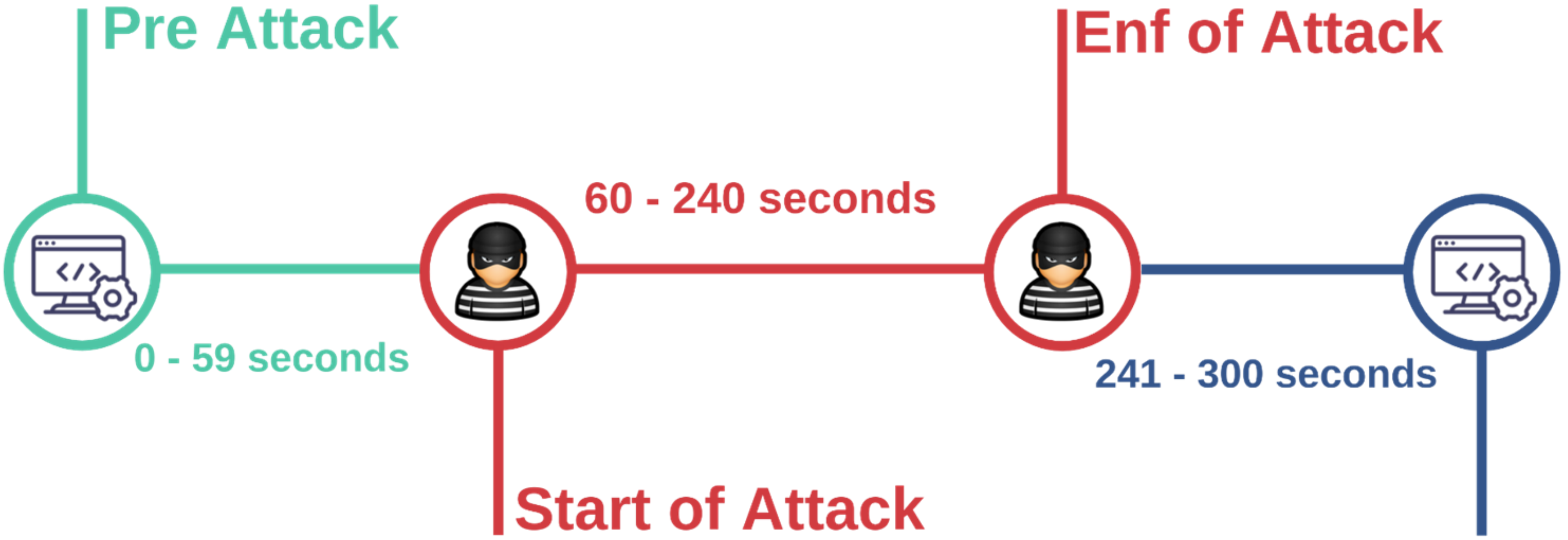
DDoS Target: Web Server NGINX

Client: Resquest at 0.5 second intervals

Attacker: Use hping software for attack, make 100 requests per second

Results

Application example



Pre Attack

0 - 59 seconds

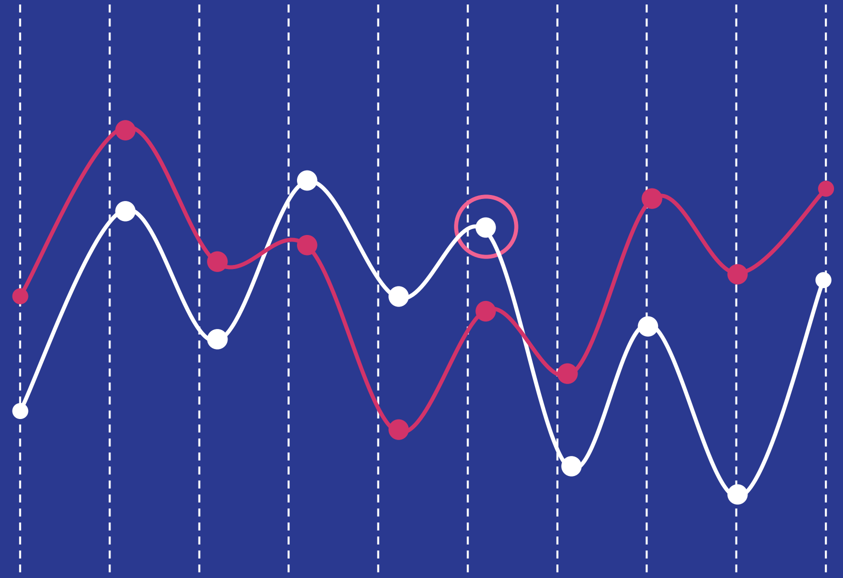
60 - 240 seconds

Start of Attack

Enf of Attack

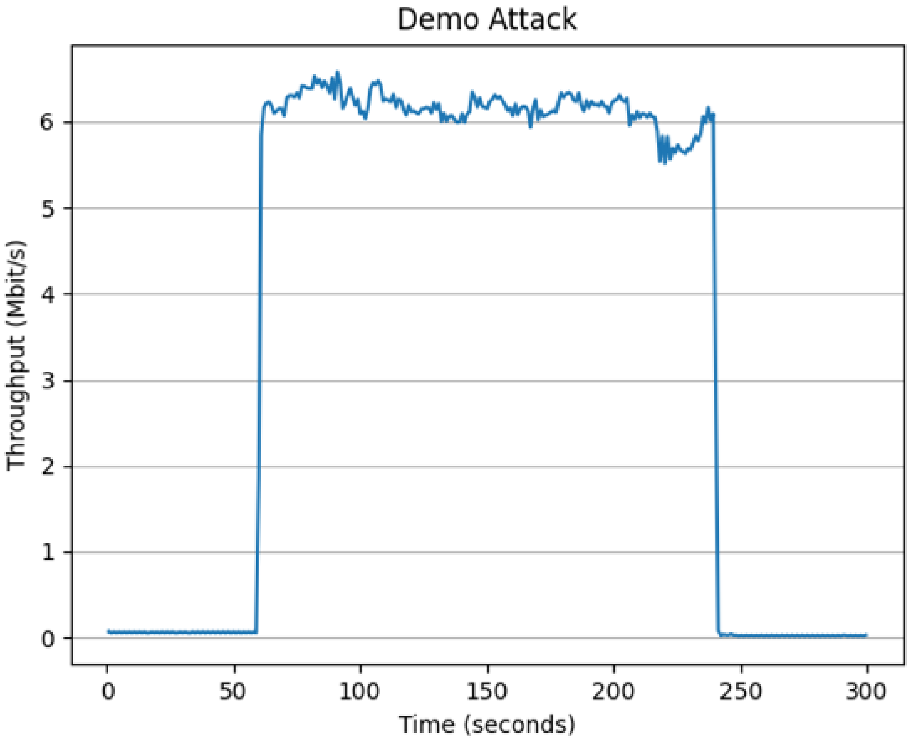
241 - 300 seconds

Results



Results

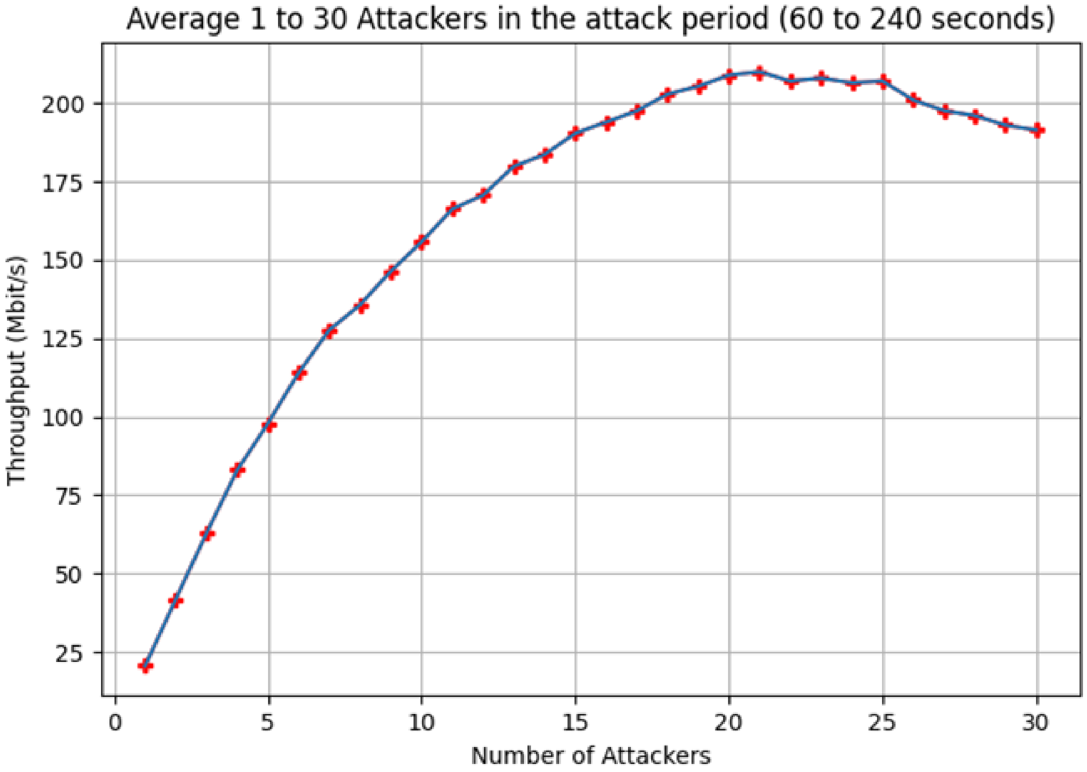
Distributed scenario



Results

Local scenario

- Scalability
- Local scenario: optimal number of attackers per region



Concluding Remarks

- Experimental environments are essential (DoT attacks)
- Framework as a reference to design scable testbed
    - Requiriments, entities and modules
- MENTORED: The Brazilian testbed for IoT cybersecurity
    - Takes advantage of well-known technologies (Kubernetes)
    - Topology modeling through .yaml files
    - REST API in the execution of the experiment
- Preliminary tests – study case

Future Works

- Other scenarios
  - E.g., a higher number of physical and virtual nodes

- Evaluate other technologies for creating virtual networks
- Analyze other attack scenarios (e.g slowloris)

Thank you! Any Questions?

Michelle S. Wangham

wangham@univali.br

IEEE/IFIP Network Operations and Management Symposium
8-12 May 2023 // Miami, FL // USA

A Scalable Cyber Security Framework for the Experimentation of DDoS Attacks of Things

Davi D. Gemmer (UFMG), Bruno H. Meyer (UFPR),
Emerson R. de Mello (IFSC), Marcos Schwarz (RNP),
Michelle Wangham (UNIVALI), Michele Nogueira (UFMG)

MENTORED

FAPESP

cgi.br
Comitê Gestor da
Internet no Brasil