Securing IoT Networks through Moving Target Defence

CSCS25

Andrei Vlădescu[1] Prof. Dr. Ion Bica[2]

May 28, 2025

[1] University Politehnica of Bucharest (UPB)
[2] "Ferdinand I" Military Technical Academy

Outline

Introduction

Context & Motivation

- Explosion of IoT devices in smart homes, healthcare, critical infrastructure
- Resource constraints & lack of built-in security
- IoT as attractive targets for large-scale DDoS attacks

Research Objectives

- Evaluate Moving Target Defence (MTD) for IoT security
- Integrate MTD with Software-Defined Networking (SDN)
- Evaluate the solution in a public network

Technical Primer

Moving Target Defense (MTD)

- Dynamically alters attack surface
- Examples: ASLR, ISR, honeypots/honeynets
- Increases attacker uncertainty and cost

Software-Defined Networking (SDN)

- Separation of control plane (controller) and data planes (switches)
- Northbound API: apps $\rightarrow$ controller
- Southbound API: controller $\rightarrow$ forwarding devices

State-of-the-Art & Where We Fit

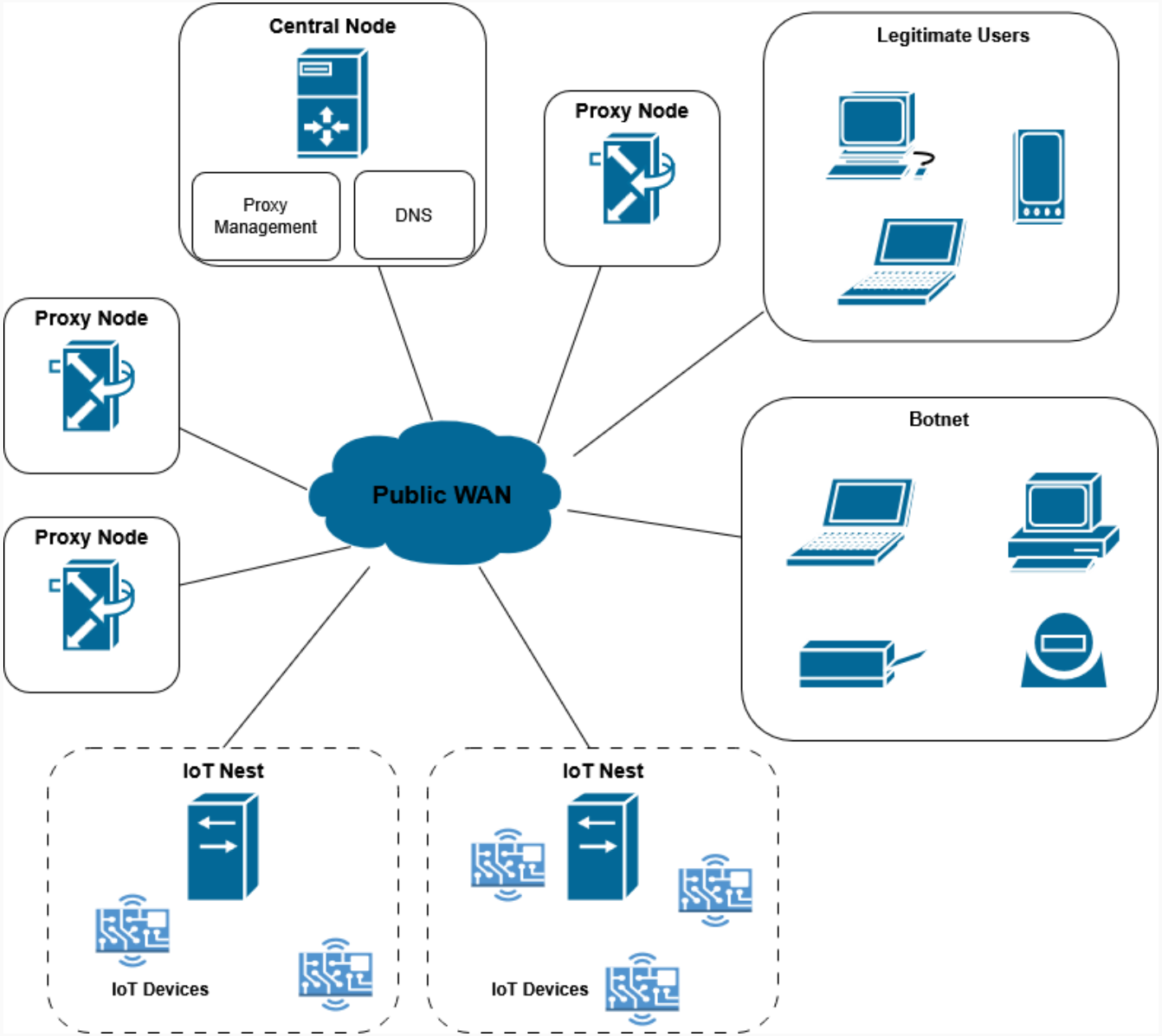
- **Mutable Networks (MUTE)** – crypto-shuffled IP/port mapping
- **Random Host Mutation (RHM)** – edge IP shuffling
- **OF-RHM (OpenFlow)** – SDN-based randomization

Proposed Architecture

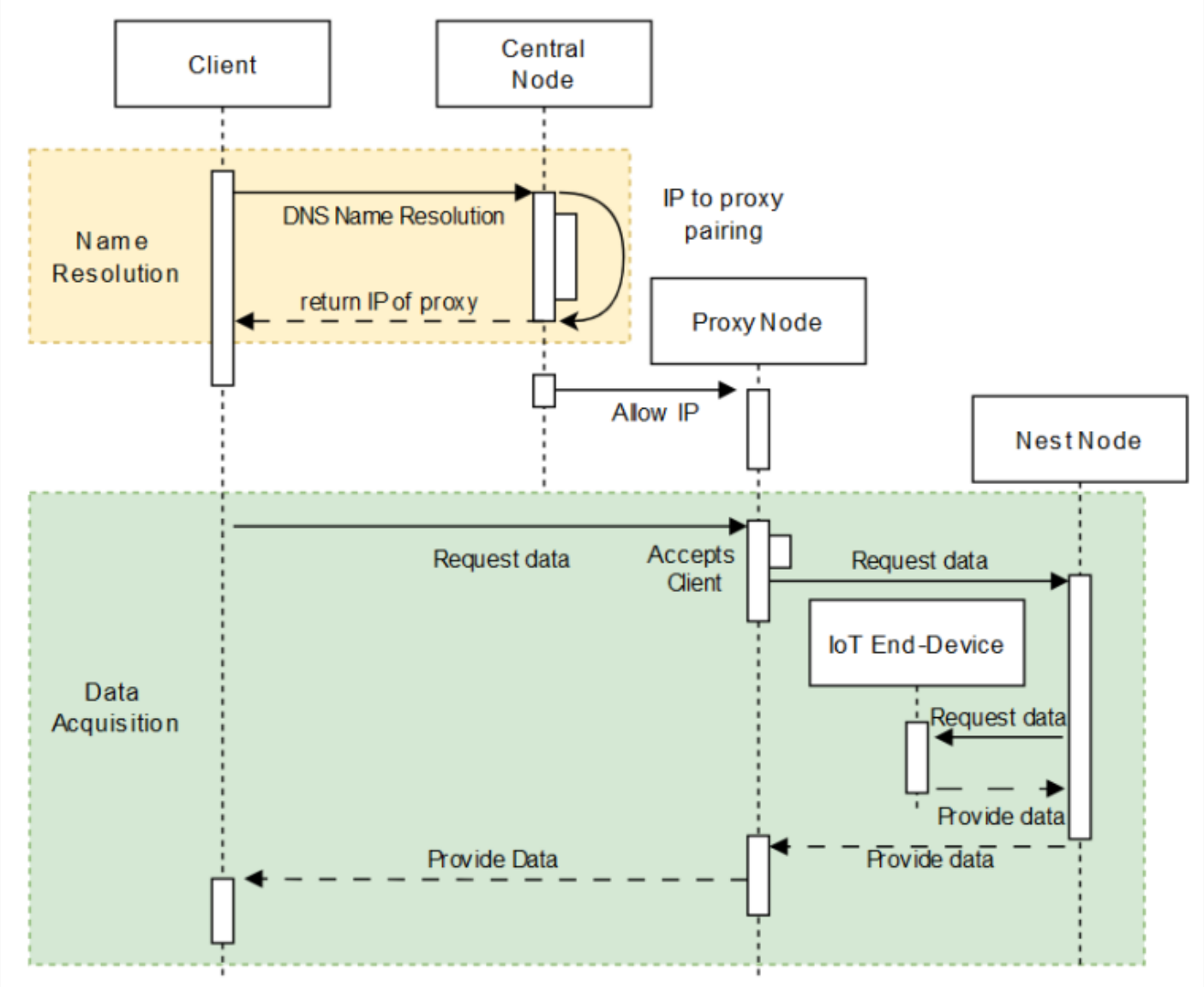
Threat Model

- Botnet-driven volumetric DDoS (SYN/UDP flooding)
- Target: resource-constrained IoT devices (no IDS/ACL)
- Reconnaissance & Exploitation threat vectors also considered

System Architecture



Defence Workflow



Defence Workflow

Case I - Botnet is not connected

1. Recon is done to find the IP address of the proxy
2. Botnet floods directly to the IP
3. Botnet is blocked by the proxy

Defence Workflow

Case II - Botnet is connected

1. Bots flood the IPs of the proxies assigned to them
2. Proxy will detect the flood and flag the IPs
3. Master Node will renew the IP address of the proxies from the ISP's DHCP server
4. Legitimate users will be able to connect again to the DNS

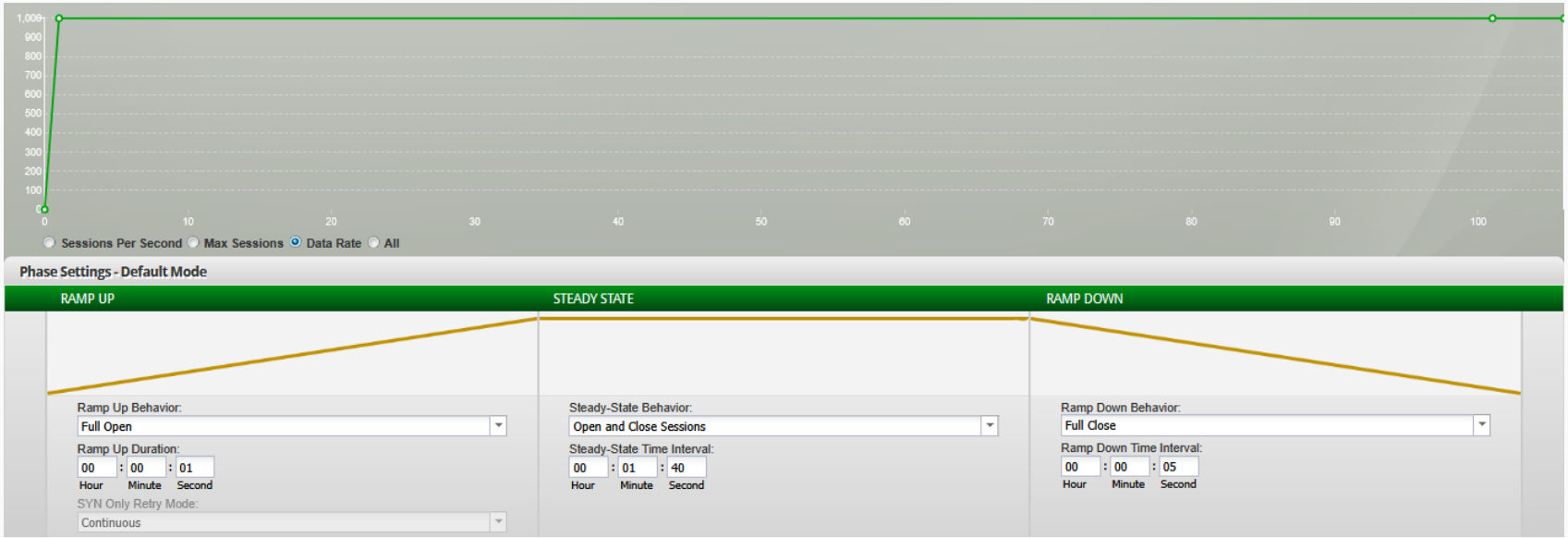
Results & Insights

Simulation Environment

- Simulated Internet inside VMs and Docker
- ESP8266 microcontroller HTTP service
- Locust framework & Ixia Breakingpoint for traffic generation
- Power usage measurement using a lab bench power supply
- Scenarios: baseline, nominal load, volumetric DDoS

Simulation Environment

Ixia Breakingpoint Data Rate Curve

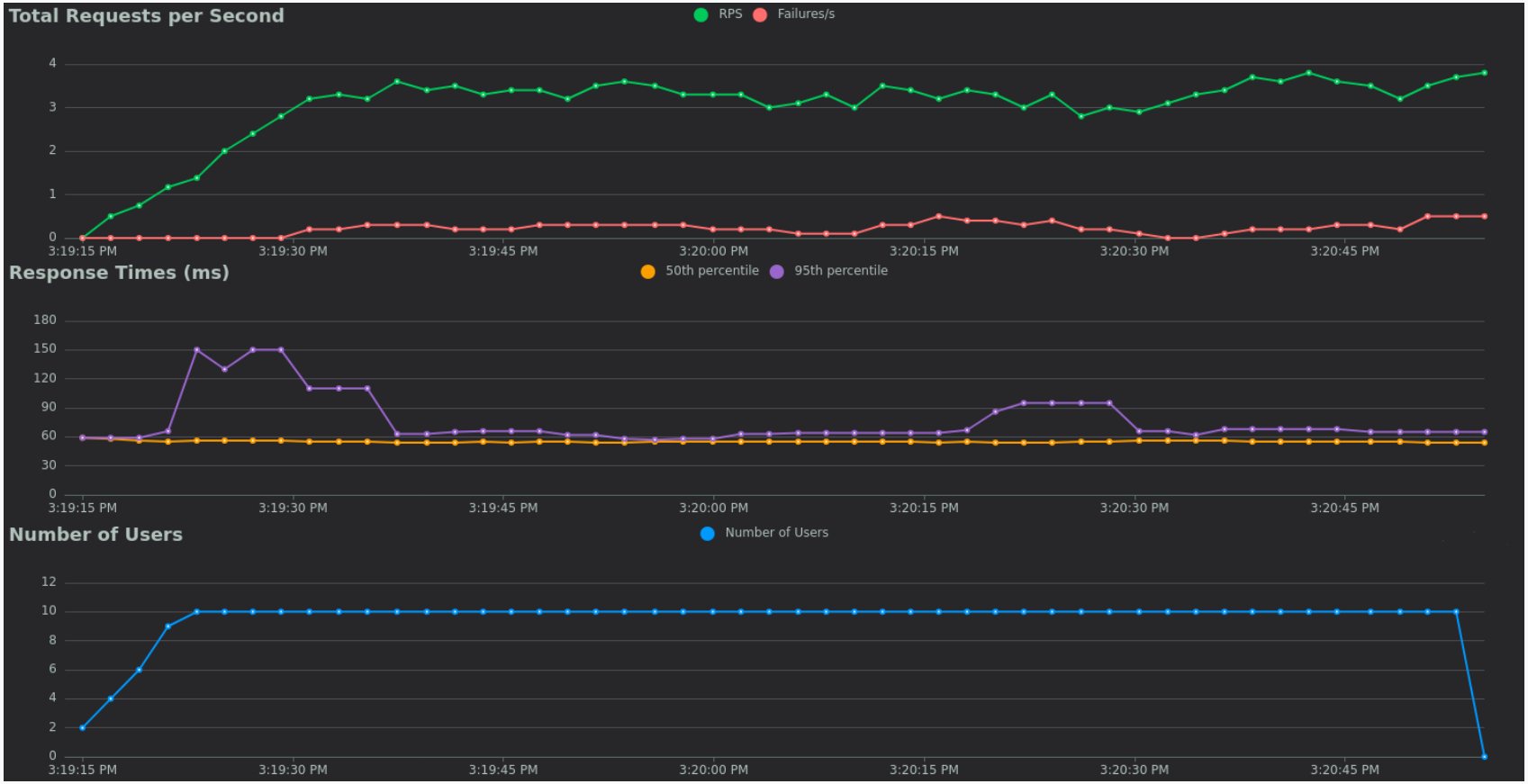


Evaluation Metrics

- **Latency**
- **Failure Rate**
- **Power Usage**

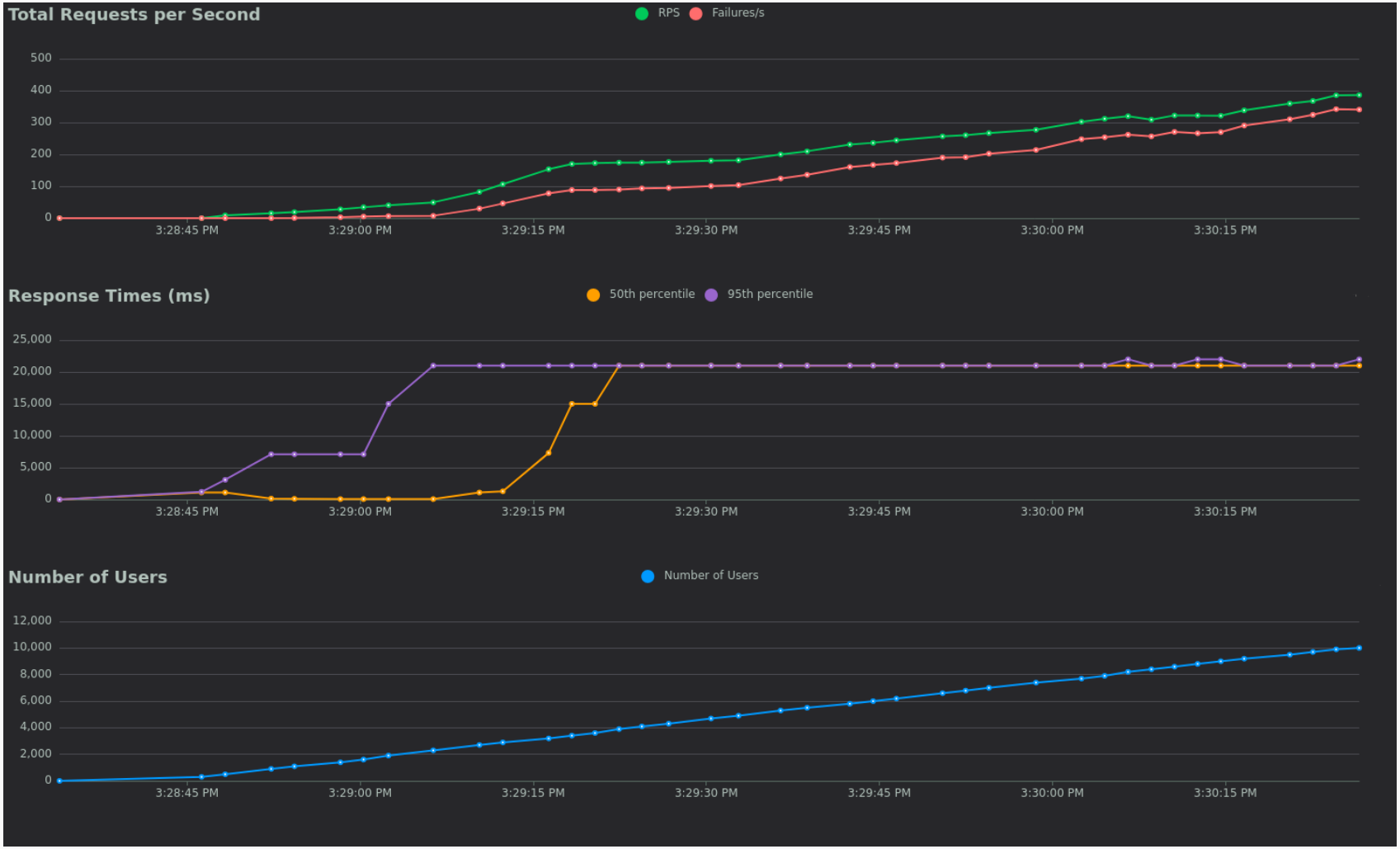
Statistics

Nominal Usage



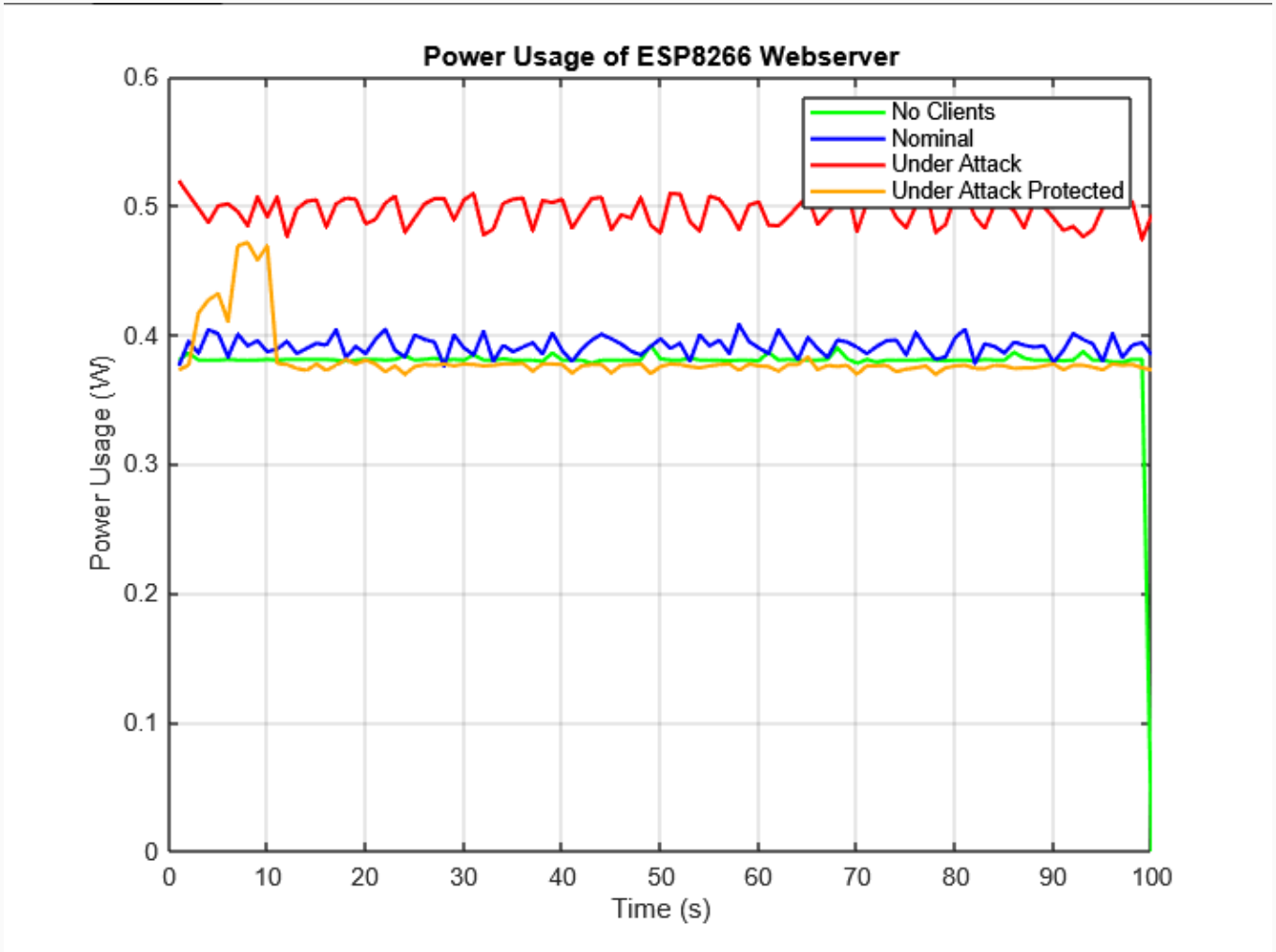
Statistics

Unprotected Attack



Statistics

Power Draw



The Good, the Bad & the Lag

- **Advantages**:
  - Cheap-ish
  - Increases attacker cost
  - Easy to implement in public WAN networks
  - Modular, device agnostic approach
- **Limitations**:
  - Overhead from ISP IP changes is a wildcard
  - Needs complementary security measures
  - Will need to be fine tuned for different services

Q&A

Thank you!

Any questions?