Securing IoT Networks through Moving Target Defence

Advanced Cybersecurity

Andrei Vlădescu[1] Prof. dr. ing. Ion Bica[2]

Jun 23, 2025

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

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

State-of-the-Art & Where We Fit

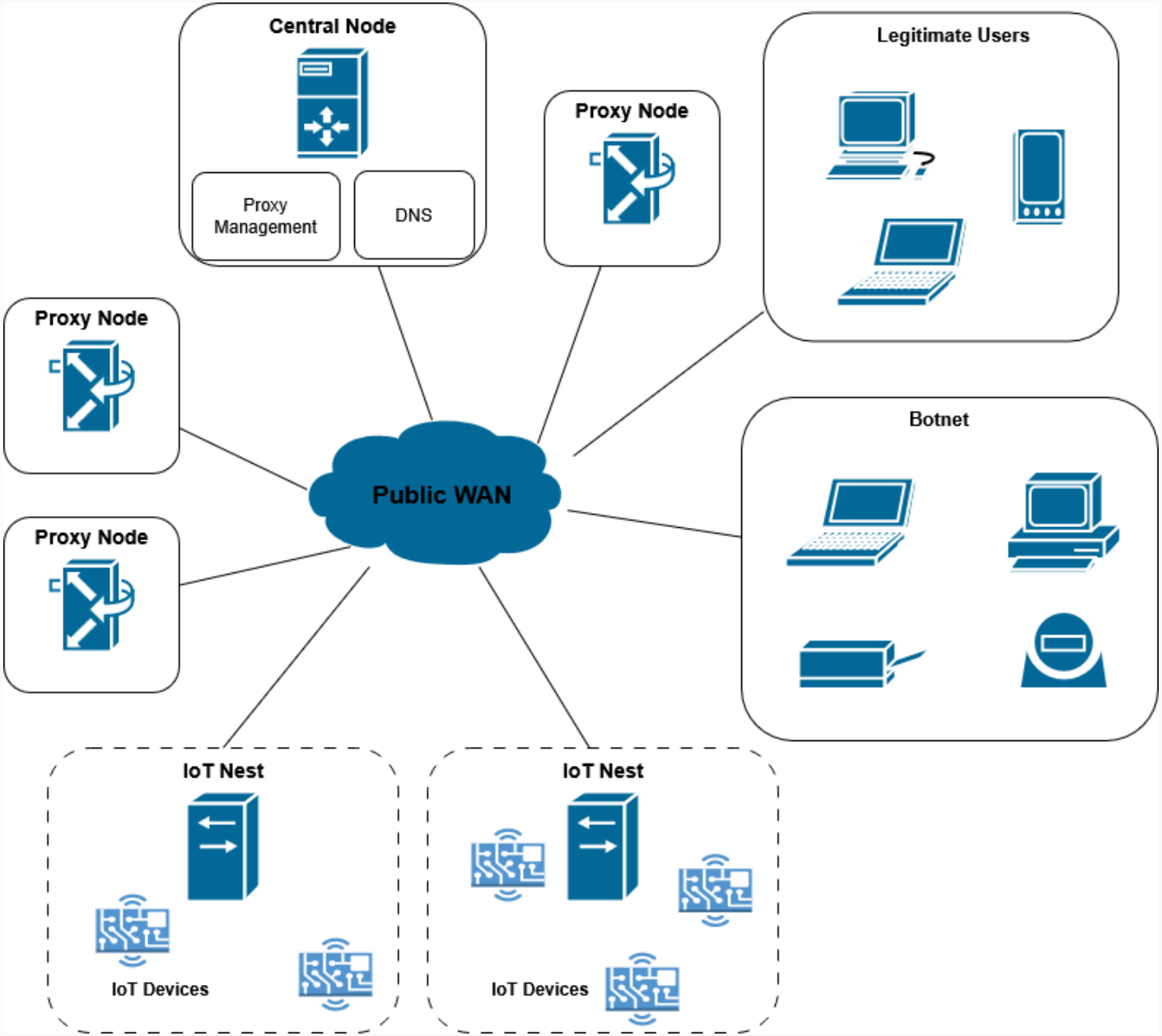
- Mutable Networks (MUTE) – crypto-shuffled IP/port mapping
- Random Host Mutation (RHM) – edge IP shuffling
- OF-RHM (OpenFlow) – SDN-based randomization

Proposed Architecture

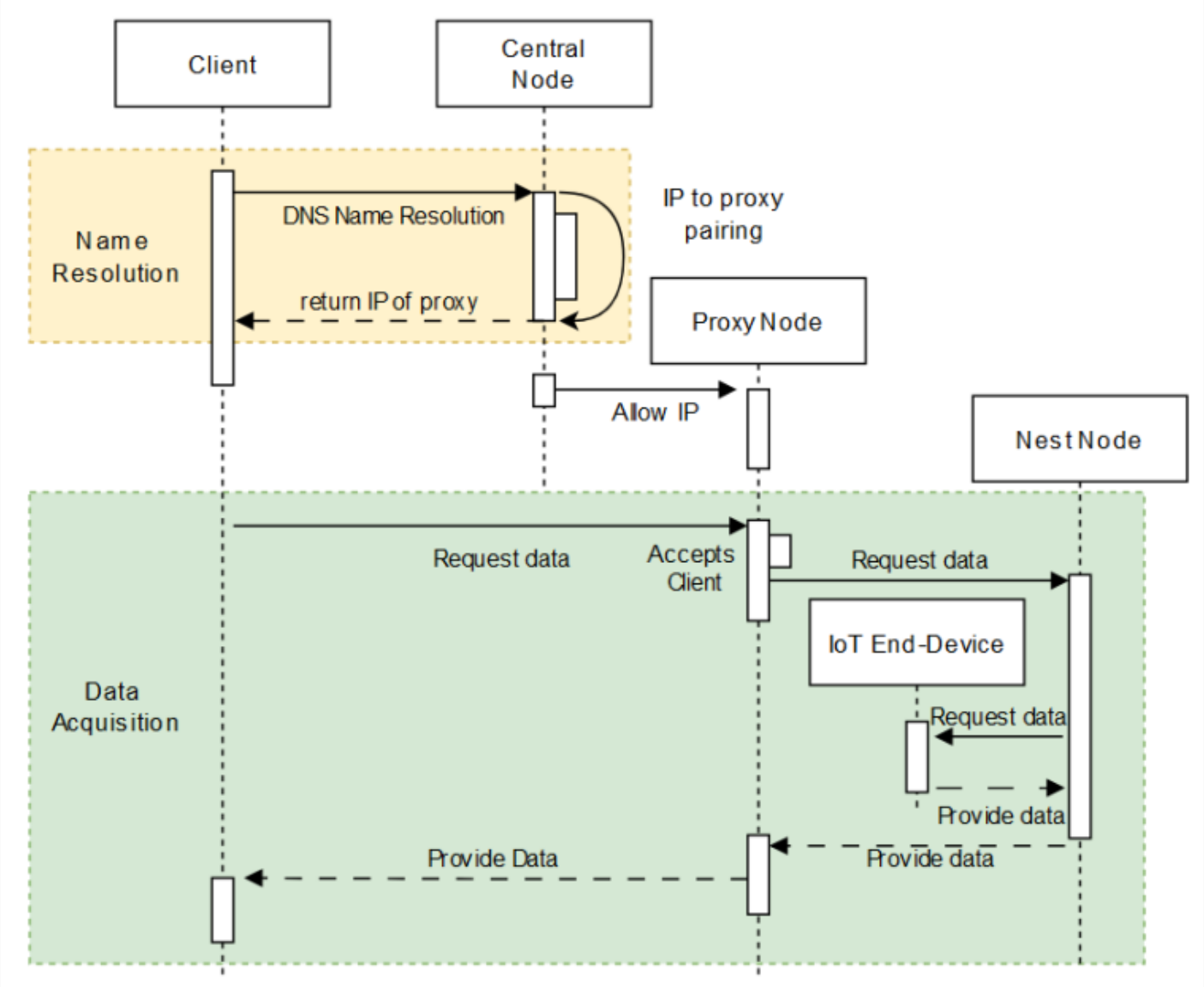
Threat Model

- Botnet-driven volumetric DDoS (SYN/UDP flooding)
- Target: resource-constrained IoT devices (no IDS/ACL)

System Architecture

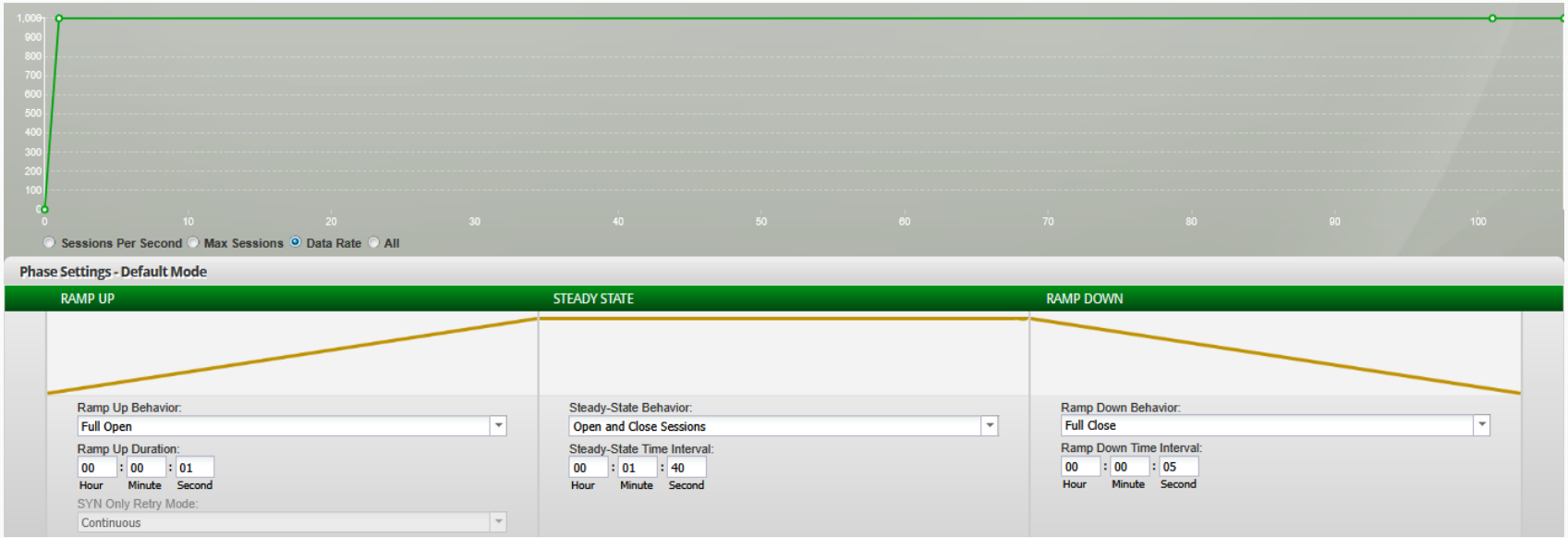


Defence Workflow

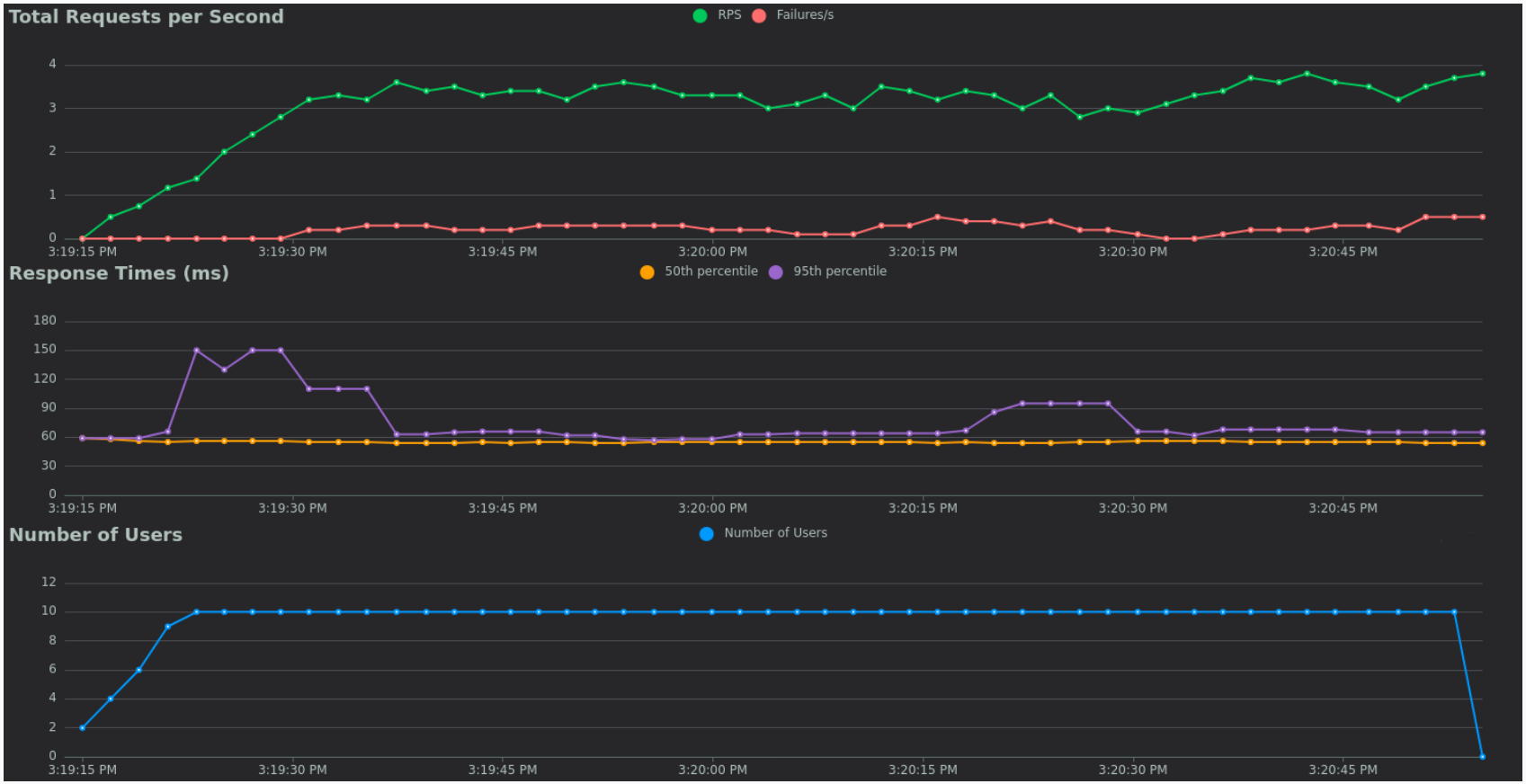


Results & Insights

Ixia Breakingpoint Data Rate Curve

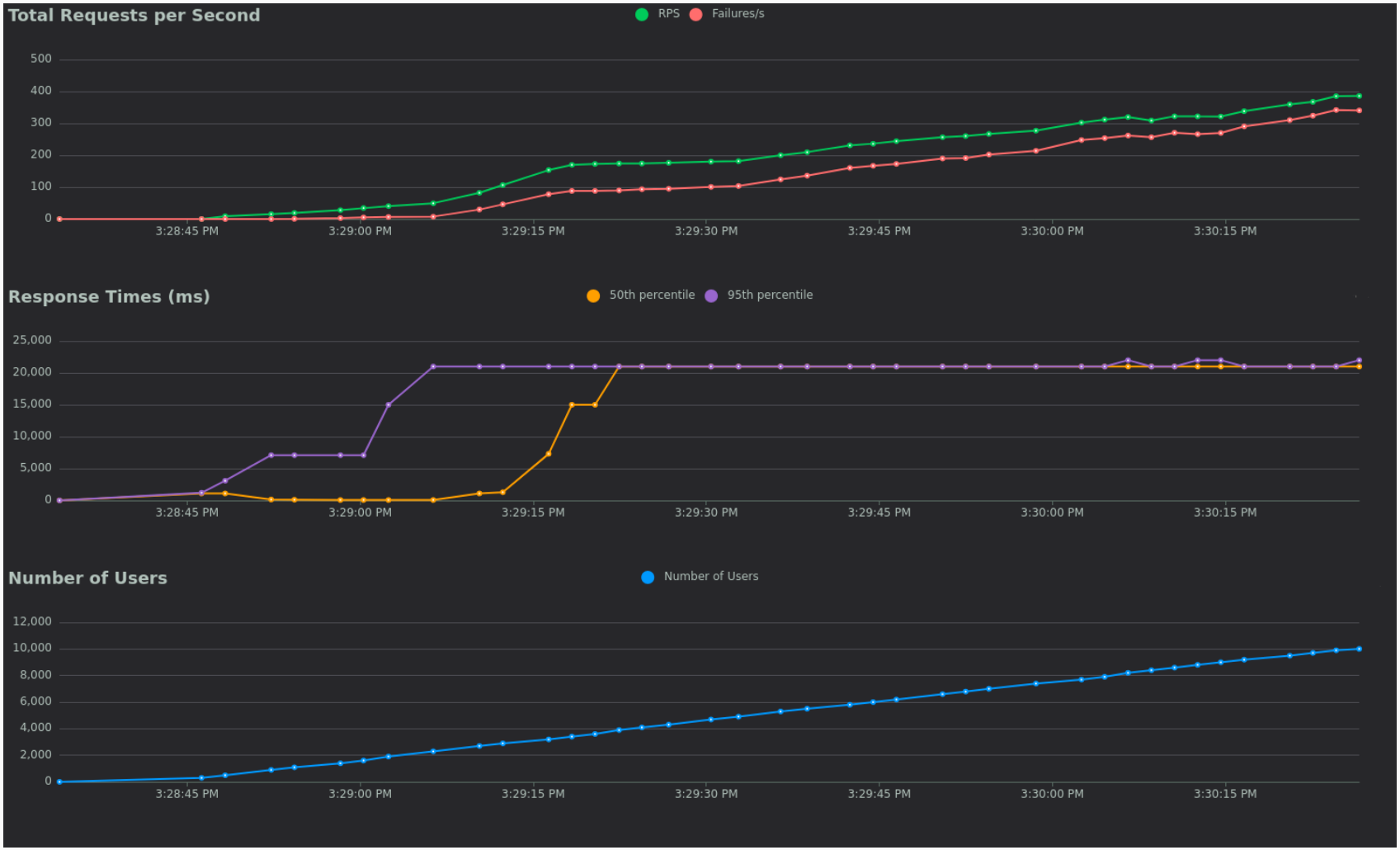


Nominal Usage

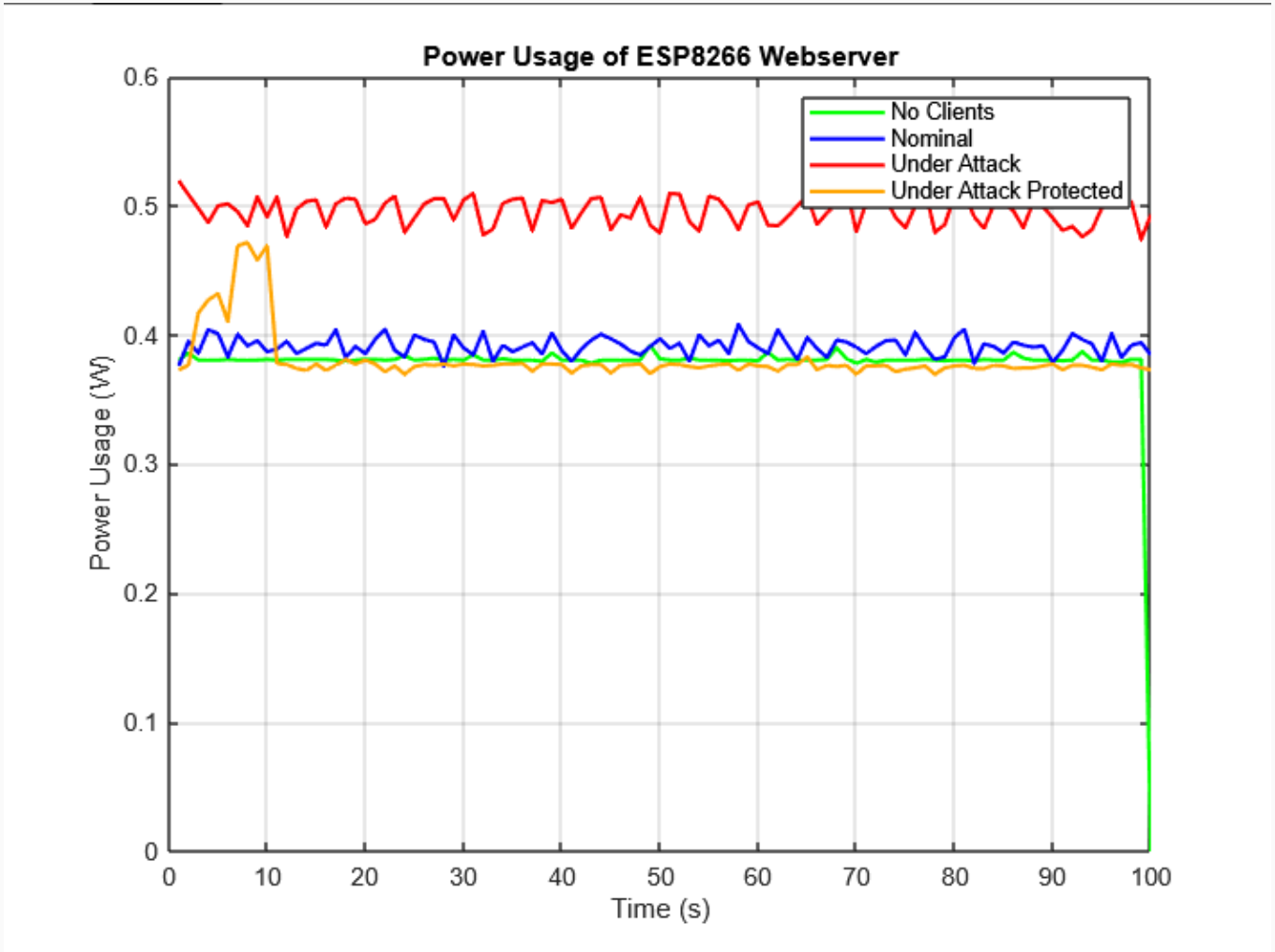


Statistics

Unprotected Attack



Power Draw


Power Usage of ESP8266 Webserver
No Clients
Nominal
Under Attack
Under Attack Protected
Power Usage (W)
Time (s)
0
0.1
0.2
0.3
0.4
0.5
0.6
0
10
20
30
40
50
60
70
80
90
100

Q&A

Thank you!

Any questions?