Outline

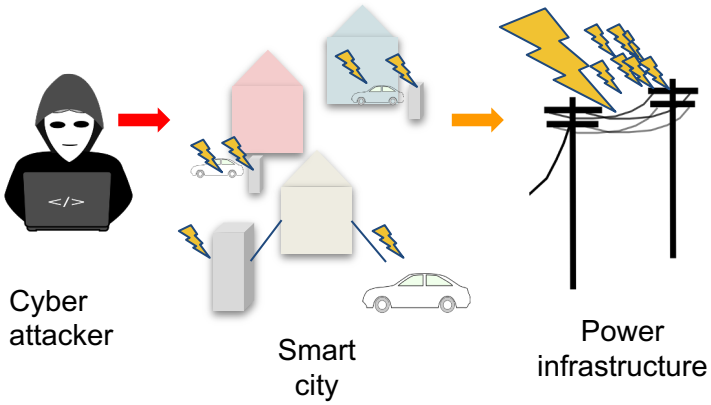
- Introduction: Power Botnets
- Co-Simulation and Two Stage Training
- Simulated Attack Results
- Next phase

Introduction: Power Botnet Attacks

Motivation: The increasing prevalence of high-wattage smart devices represents a new vulnerability for power infrastructure: **Vulnerable high-demand devices at the grid edge.**

An attacker controlling many of these devices can cause **unnatural demand spikes** to cause **hardware damage**, even **blackouts**. (*See "BlackIoT" by Soltan et. al., 2018*).

This is a **cyber-attack** against power-infrastructure which targets **consumers at the edge**, rather than internal / SCADA computer systems.

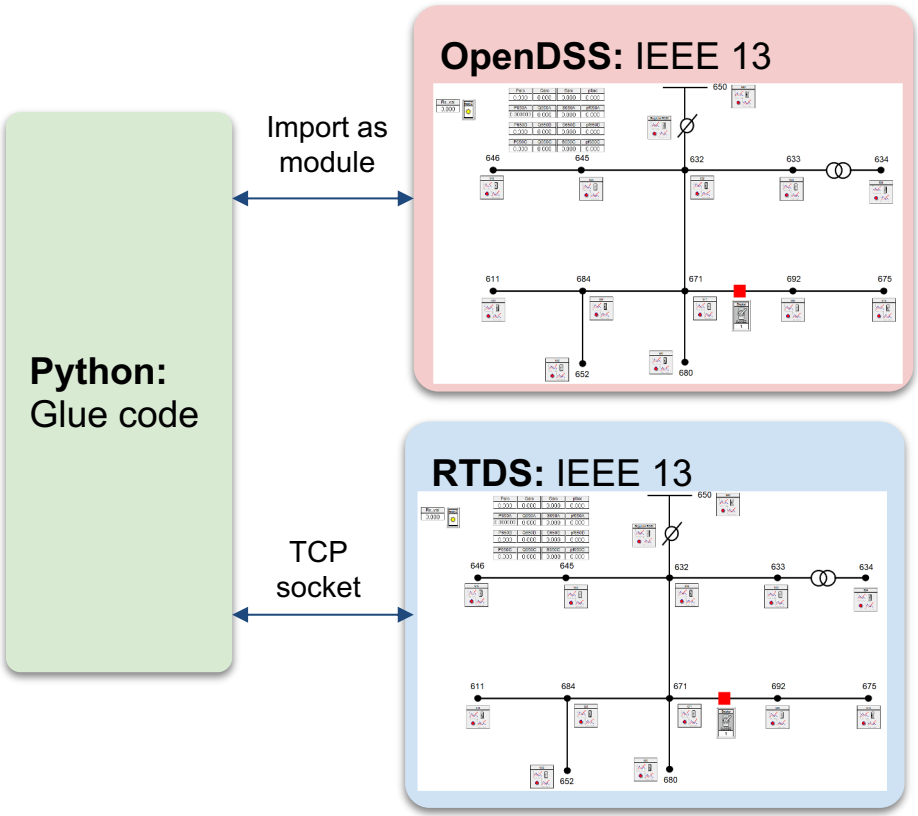


Research summary:

1) Design and analyze various power botnet attack scenarios
2) Design detection and localization schemes based on machine learning
3) Verify physical system botnet attack resiliency using HIL co-simulation between OpenDSS and RTDS

Co-Simulation

- OpenDSS and RTDS share IEEE 13 simulation
- Python glue code and machine learning model interacts with both simulators



Two-Stage Training

(1) Train model against OpenDSS

Untrained Model

Python: Gathers data and trains model

OpenDSS: Simulate IEEE 13 and attacker

(2) Fine-tune, evaluate model against RTDS

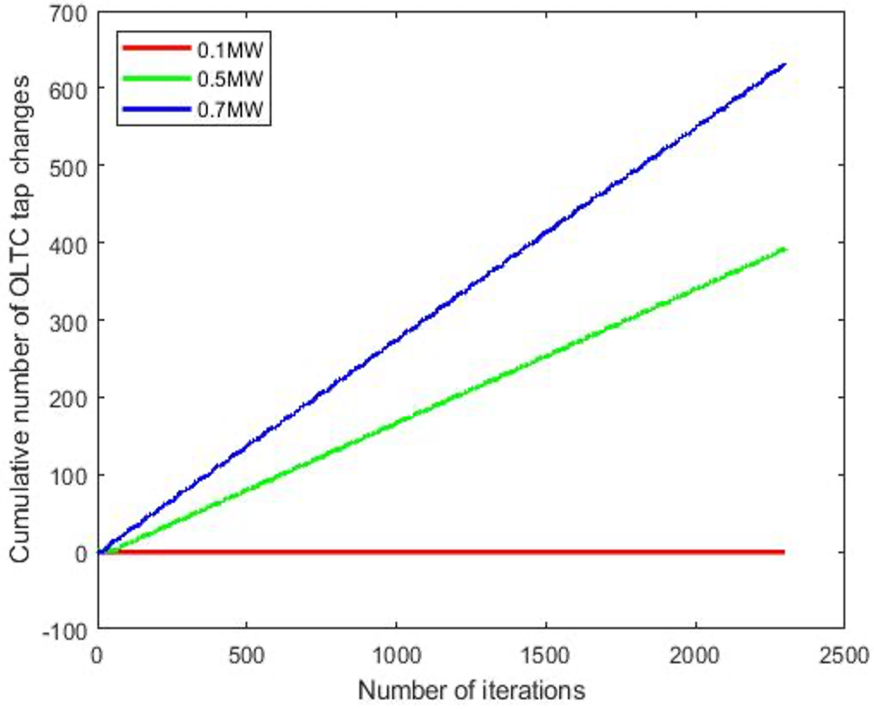
Trained Model

Python: Uses trained model, detects attacks

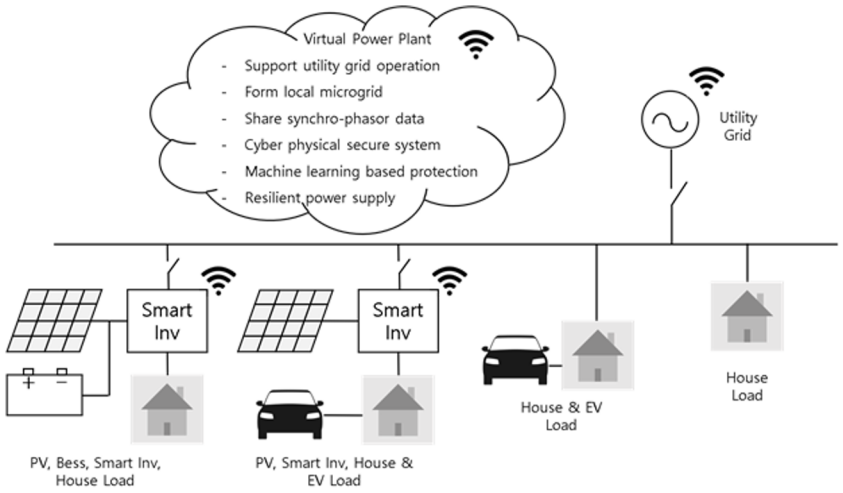
RTDS: Simulate IEEE 13 and attacker

Simulated Attack Results

1. “Flipping-attack” logic in Python, simulation in RTDS
2. More attacker power = more infrastructure damage



Next phase: Secure and Resilient Residential Photovoltaic Systems based on Smart Inverter and Battery Energy Storage Systems



Proposed secure, resilient residential power network

RTDS and Lucas-Nuelle testbed

Design smart inverter and virtual power plant

Build a testbed:

- RTDS will simulate grid-connected DERs
- Interface the RTDS with Lucas Nuelle power system hardware
- Synchrophasor capability will be added to the grid-connected inverter
- Survey cryptographic communication protocols
- High-level design of a secure communication standard