Securing Power Distribution Grid Against Power Botnet Attacks

Eversource Energy Cyber Security Project Phase II

University of Connecticut: PI: Fei Miao (fei.miao@uconn.edu)
Co-PIs: Amir Herzberg, Sung Yeul Park
PhD Students: Lynn Pepin, S M Rakiul Islam
RTDS testbed collaborator: Thi Ha Nguyen

Apr 1, 2021

UCONN

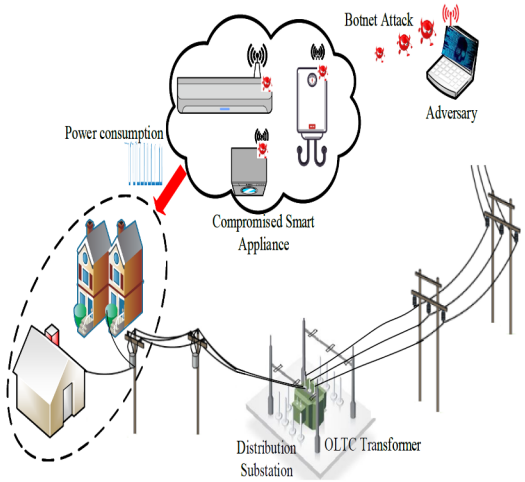
Motivation

- The growing market for high-wattage smart devices (water heaters, air conditioners) allows for a new class of botnet attacks that can leverage controlled load to damage the power grid (e.g., OLTC).

1)The transmission network has protection schemes such as load shedding (”**Not Everything is Dark and Gloomy: Power Grid Protections Against IoT Demand Attacks”, usenix 19,** https://www.usenix.org/conference/usenixsecurity19/presentation/huang) not good research and evaluation on the distribution network side yet.

2) Such a botnet (multiple smart devices) is a power botnet. Attackers make load and voltage fluctuate through manipulating power botnet.

3) Voltage fluctuation makes tap of OLTC change frequently, which can fast wear down OLTC , an expensive power equipment .



Power Botnet Attack against Power Distribution Grid

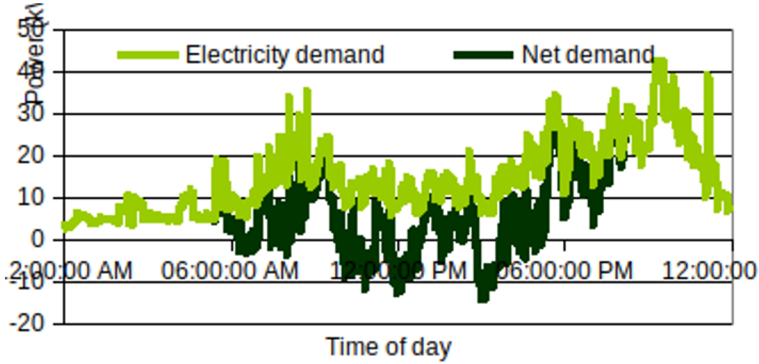
Challenges & Objectives

- Load data are **aggregated**, can not only simulate load change from a single device or household caused by attack
- Design and analyze different power botnet attack strategies, from aggressive (relatively easier to be detected) strategy, to advanced strategies that try to avoid detection and location by the system
- No dynamic model appropriate for model based attack analysis or detection/localization method design
- Design detection and localization schemes based on machine learning (data-driven methods)
- OpenDSS generated distribution network data for attack analysis, detection and localization methods design
- RTDS demo

System and Data Description

- Each **node**: multiple households (e.g., 40), the number of households is based on the capacity of each node

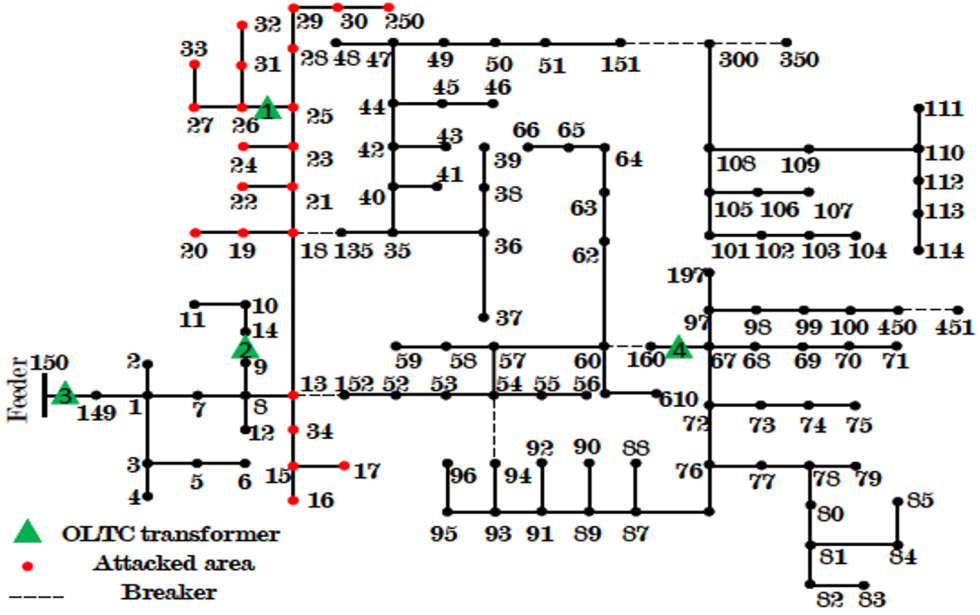
- Each **household**: one **water heater**, two **air conditioner**
- The attacker can control x% of water heaters (and air conditions for future work), to impact
  - →1) the **load** of each household can be altered
  - → 2) the **aggregated load** of each node can be altered
  - → 3) the **voltage** at each OLTC can be altered
  - → 4) increase the frequency of **tap changes**
- Attacked area: Selected nodes around OLTC



One example of node load file

- Data source: Centre for Renewable Energy Systems Technology (CREST) (Real household power consumption data)

Attack Model



Test system: IEEE 123 node test case
(More cases: 16,34,36 nodes topologies, etc.)

Attacker's capabilities

- Knowledge of network, the distribution grid topology and the parameters of the OLTC transformers.
- Knowledge of voltage V_{Ct} to decide
  - -Time to manipulate the power botnet;
  - - Number of water heaters to cause tap operation.

Power Botnet Attacks strategy: Aggressive Attack (AA):

Attacker Goal: manipulate the IoT devices frequently to cause tap operations as much as possible while considering the vulnerable scenario.

Method: This attack occurs (turn on/off water heaters) only when the regulated voltage of OLTC is near to cause tap changes .

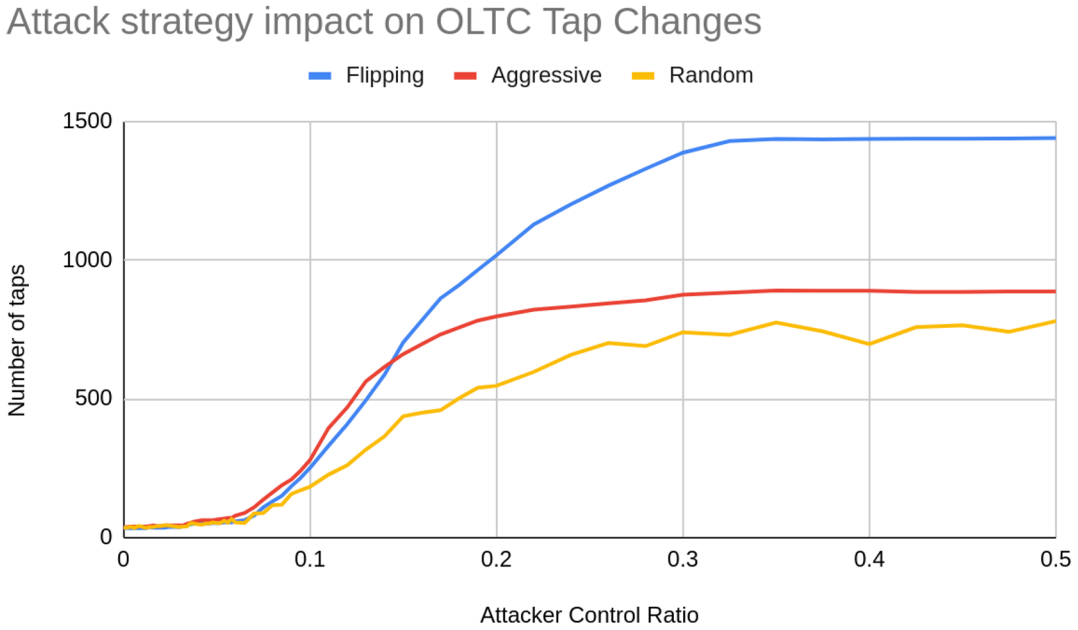
$V_{Ct} = |\tilde{V}_t + (R_C + jX_C)\tilde{I}_t|$
while $DB/2 - |V_{Ct} - V_{ref}| = |\Delta v| \leq \varepsilon$ **do**
  if $V_{Ct} \leq V_{ref}$ **then**
    turn on $f(|\Delta v|)$ water heaters
  else
    turn off $f(|\Delta v|)$ water heaters
  end

- The lasting time of each attack (e.g., 1 min)
- The attacker will manipulate a selected number of water heaters contained in selected nodes.

Code Improvements of OpenDSS

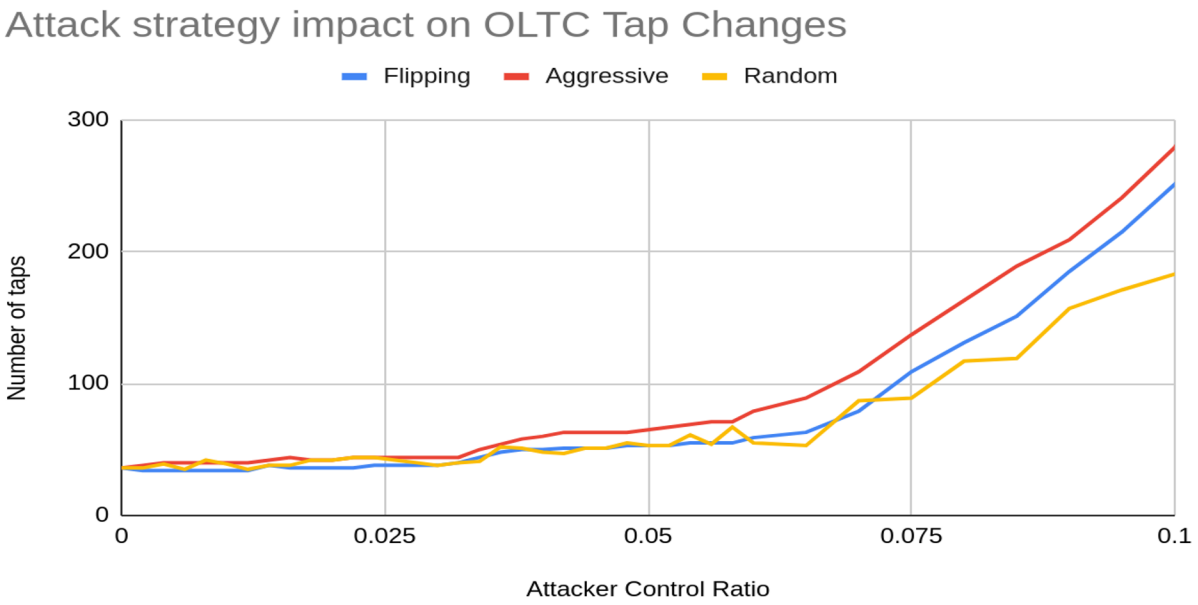
- New code rewritten in Python 3, using OpenDSS libraries.
  - Now **portable**, runs on most modern operating systems.
  - More **accessible** to develop with. Repository will be shared.
- **Modular** rewrite separates power-grid model and attacker code.
- **Easier to implement** new Attacker algorithms.
- **Wrapper scripts** allows quick generation of new simulations via **Bash**.
- Simulation system is **documented** and with **thorough examples.**
- Plenty of **example scripts** of data-generation to learning-model pipeline.

Attack strategies increase the number of tap operations

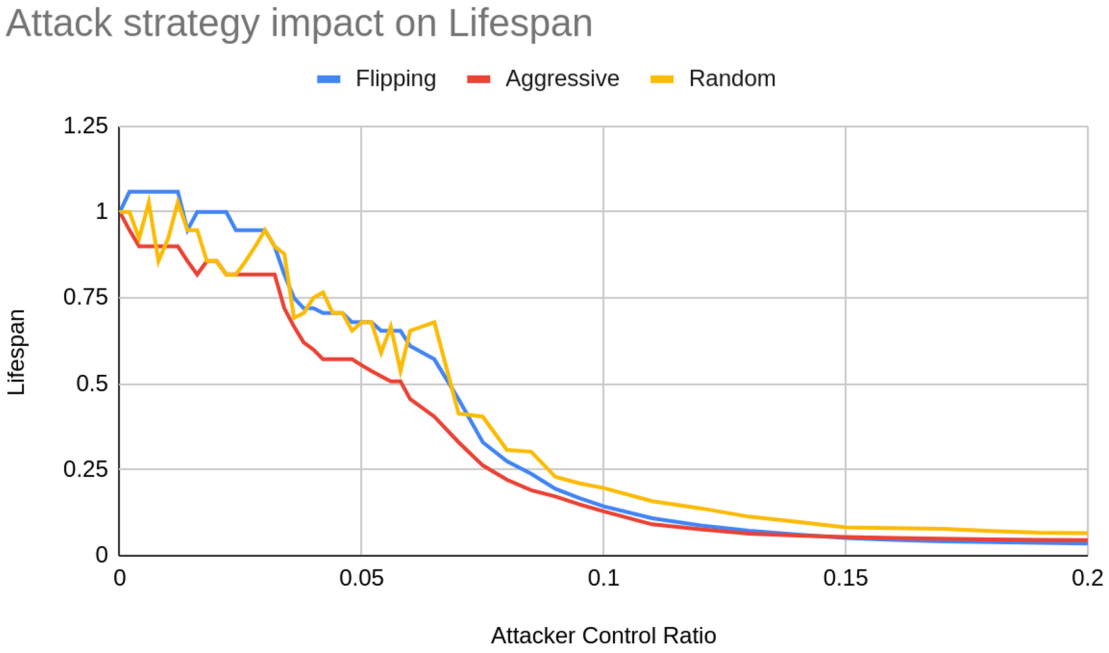


- **Attacker control ratio**: What percent of demand attacker can control
- These strategies **increase the number of tap operations**.
- The normal amount of taps (no attacker) is 36.

Tap changes versus Attacker Control Ratio Chart



Increased tap operations decrease lifespan



- Using 36 taps-per-day as a baseline, we can see how different strategies impact OLTC lifespan.
- “Flipping” and “random” strategies are simplistic strategies.
- At even 10% control, the OLTC will only last 13% of its rated lifespan.

Learning to Detect and Localize Power Botnet Attacks

Goals: The goal is to map grid-state time series to answer if an attack is in the system or to answer what nodes the attacks occur.

- Location detection formalized as multi-label time-series classification problem.

Challenges: This is new ground, and required significant exploration:

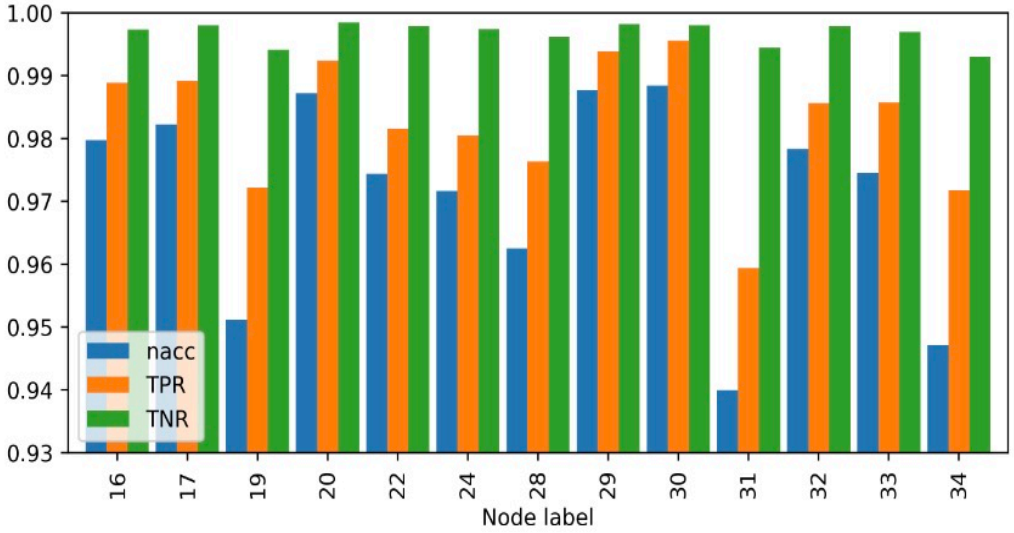
- No prior work, needs to investigate useful machine learning methods.
- Identifying realistic and useful data features to learn on, based on simulation data.

Learning to Detect Power Botnet Attacks

Data description:

- Electrical measurement vectors sampled per-minute from simulated OLTC.
  - Voltage, current, and power, phase angles thereof.
  - Tap positions of OLTC.
- Each minute is labelled with “attacker active” or “attacker inactive”.
- Other information is encoded with each simulation:
  - Which nodes contain devices controlled by the attacker
  - Month, date of the week being simulated
  - The PV penetration o the system

Location-Detection Results Graph

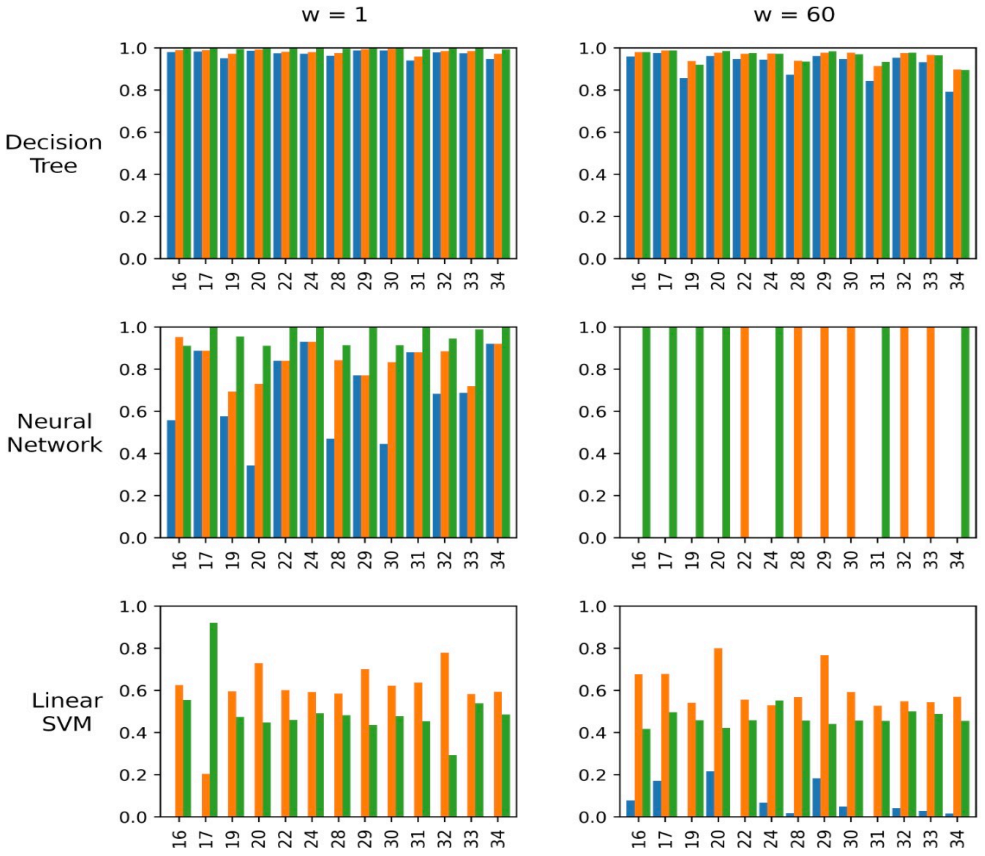


Machine Learning method: Decision Tree

- 256 simulation samples
- A random set of 6 nodes is chosen for each.
- Very high metrics for each node, improvement from previous results.

Normalized accuracy nacc is compared to a ‘guess majority” baseline, where Norm Acc = 0 is no improvement.

TPV and **TPVR** are the true positive and negative predictive values, respectively.



Comparison of the impact of learning methods and of window sizes w (mins) on classifier performance. Vertically, we see the performance of a decision tree classifier, a best-effort neural network classifier, and a linear SVM classifier. Horizontally, we see the impact of different choice for window size w. Here we see decision trees perform the best, especially so when w = 1.

Conclusion

1. Evaluated the damage of power botnet attack on the hardware wear down, lifespan of targeted OLTC.
2. Developed and analyzed machine learning methods to detect the presence of an attack and locate the grid nodes containing compromised devices.
3. New OpenDSS + Python tool with attacker implemented outside simulation loop.

Results based on recent submission to ACM Transactions on Cyber-Physical Systems (under revision)

Future Work

- Improve current localization methods to get higher accuracy rates. Code and Data deliverables.
- Moving towards **semi-supervised and unsupervised** learning methods (training data for detection and localization does not need to be fully labeled attack).
- RTDS Simulator Demo
- Renewable energies and related devices

- Questions:

fei.miao@uconn.edu