UCI University of California, Irvine

Secure-by-Design & Self-Secured Control with Anomaly Detection in Smart Grid

Arnav Malawade, Anomadarshi Barua, Mohammad Al Faruque

March 08, 2018

Contributions

- **A co-simulation platform (Secure Grid Simulator) to simulate new and existing cyber-physical attacks.**
  - ➢ Identified common vulnerabilities/attack methodologies and their effects on different components of the smart grid.
  - ➢ Impact of attack on physical infrastructure at distribution level.
- **Self-Secured Control with Anomaly Detection and Recovery in BMS of DER’s.**
  - ➢ CGAN will capture the dynamic behaviour of the control loop in order to detect any anomaly resulted from the attacks, and to recover from the attack by predicting the correct state of system.

Common Cyber-Physical Attacks on Smart Grids

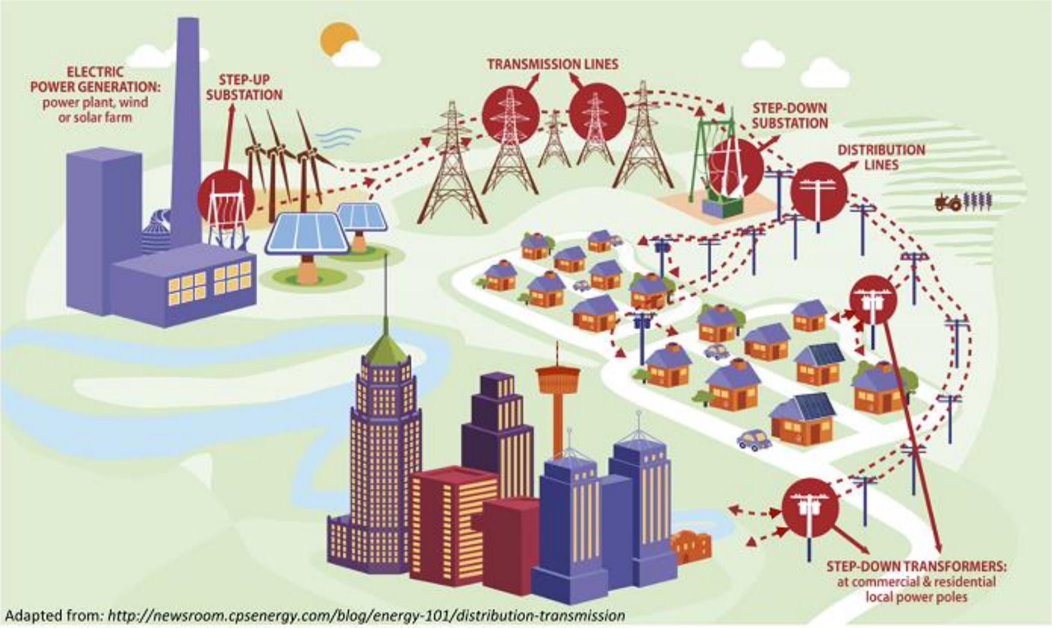
Major Attack Models	Minor attack models	Attack Domain	Consequences
Integrity Attacks	• False Data Injection (FDI) • Flooding	• Through cyber domain i.e. changing the senders and receivers IP address • altering the current and voltage info of the user • altering price info	• Loss of data integrity • Prevent accurate grid-state estimation • Financial loss
Confidentiality Attacks	• Eavesdropping	• Through cyber domain i.e. extracting data from HAN, AMI network	• Loss of confidential user info
Availability Attacks	• Denial of Service Attack (DoS) • Distributed Denial of Service Attack (DDoS)	• Through cyber domain i.e. imposing delay in the communication network (Time Delay Attack) • Damage to physical components causing blackouts	• Loss of service • Prevent accurate grid-state estimation • Financial loss

Our Area of Focus and Methodology

- Area of focus : **Toaster to Transformer (T2T)**

- Study the impact of various cyber-physical attack methodologies on smart appliances (i.e., HVAC, EV chargers), Distributed Energy Resources (DER), capacitor banks.

- **<u>We propose a simulation platform to enable the study of different cyber-physical attack methodologies and their impact.</u>**


ELECTRIC POWER GENERATION: power plant, wind or solar farm
STEP-UP SUBSTATION
TRANSMISSION LINES
STEP-DOWN SUBSTATION
DISTRIBUTION LINES
STEP-DOWN TRANSFORMERS: at commercial & residential local power poles

Adapted from: *http://newsroom.cpsenergy.com/blog/energy-101/distribution-transmission*

Cyber-Physical Attack Examples in T2T Domain

Cyber-Physical System	Direct Attack	Coordinated Attack
Smart Meters	DoS attack denying power to user	Coordinated DoS in an area causing localized blackout
Smart Thermostats	Induce high power usage by modifying heat/cool setpoints	High HVAC power usage between multiple homes to overload transformer
EV Chargers	DoS attack preventing charging/abnormal charging to damage EV battery	Coordination of charging to induce a high peak charging load to overload transformer
DER's	Increase grid load by charging battery banks directly from grid during peak times & discharging at off-peak times	Switching capacitor banks in/out can create reactive power imbalance and potential blackout
Communication Devices	Flood network to make state estimation difficult	network flooding/bad data injection to prevent physical attack detection

Approach

- “Existing security approaches are either inapplicable, not viable, insufficiently scalable, incompatible, or simply inadequate to address the challenges posed by highly complex environments such as the smart grid.” [1]
- Increased complexity of smart grid causes security state-space explosion
  - formal security analysis is infeasible

- **Need better tools for Design Space Exploration of Cyber-Physical Security**

- **What smart grid simulation tools currently exist?**

Existing Simulation Tools

Tool	Layer	Capabilities	Drawbacks
Gridlab-D	Physical	Detailed end-use appliance, equipment, and consumer models	Difficult to simulate complex control systems
OpenDSS	Physical	Good analysis of special applications like distributed generation, EV penetration, etc.	Lacks detailed consumption modeling
NS-2/NS-3	Communication	Simulates network protocols and event-driven behavior	Purely cyber-domain. No analysis of effects on infrastructure
PSLF	Physical & Communication	Load-flow, short-circuit, & transient-stability simulations + NS-2 Co-simulator	Lacks detailed consumption modeling
FNCS	Physical & Communication	Generic tool for connecting physical layer simulators with communication simulators	Focused more on utility rather than security
GridDyn-Modelica FMI Coupling	Physical & Communication	Uses Modelica FMUs to decouple GridDyn simulation from mathematical models. Integrates GridDyn sim with Gridlab-D and NS-3.	Focused more on utility rather than security

Limitations of Existing Tools

- Existing tools are primarily focused on:
  - ➢ Physical Security: Increasing robustness against physical equipment failure
    - ➢ Static failure modes & effects analysis [2]
    - ➢ Dynamic analysis using simulation tools
    - ➢ Generally only considers a pre-specified list of contingencies [1]
  - ➢ Cybersecurity: Securing communication networks
    - ➢ Bad-data detection mechanisms in SCADA [3]
    - ➢ Use of proprietary protocols in SCADA networks (security through obscurity)
- **Combined Cyber-Physical attacks can circumvent these defense mechanisms**
  - ➢ Stuxnet utilized a combination of cyber and physical attacks to destroy centrifuges used for Iran’s nuclear program

Methodology

- **Goal: Develop Tools and Methodology for the Analysis of Smart Grid CPS Security**
  - Identify potential attack methodologies
  - Simulate cyber physical attacks to determine impact
  - Use results to develop new methods for preventing attacks
  - Validate prevention strategies

- Classification and modeling of security risks enables the development of systems which are ***secure-by-design* (*design space exploration for security*)**

A Tool For Smart Grid CPS Security

- **Secure Grid Simulator (SGS):** A GridLAB-D-based simulation tool with Matlab/Simulink-based control system

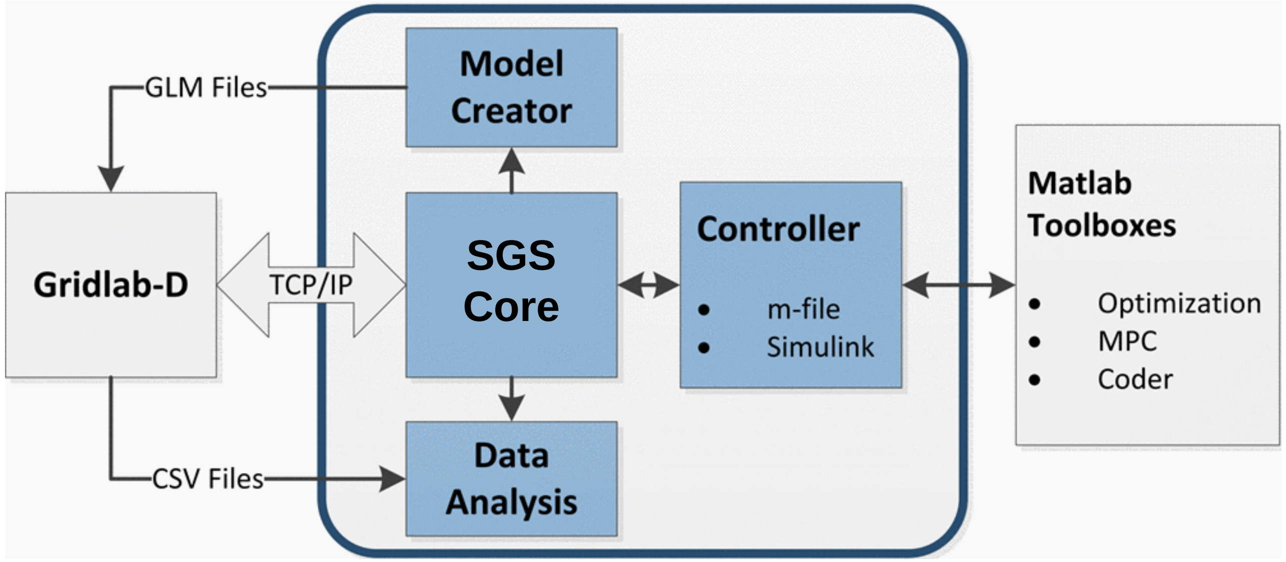
- **Focused on enabling *secure-by-design CPS development***

- Enables simulation of **cyber-physical attacks** on residential smart grid
  - Impact of attack on physical infrastructure at consumption/distribution level
  - Physical impact of stealthy and/or coordinated attacks
  - Identify ways to increase resilience of infrastructure against CPS attacks
  - Test/validate CPS attack prevention methodologies

Functionality

- Uses standardized Gridlab-D model files
  - ➢ GLM files used to specify Gridlab-D model and appliance/occupant schedules
  - ➢ Gridlab-D performs simulation at each time step

- MATLAB/Simulink-based control system [4]
  - ➢ .m files used to implement control algorithms on model components
  - ➢ Can adjust model parameters at every time step
  - ➢ Enables more complex control system simulation than Gridlab-D alone



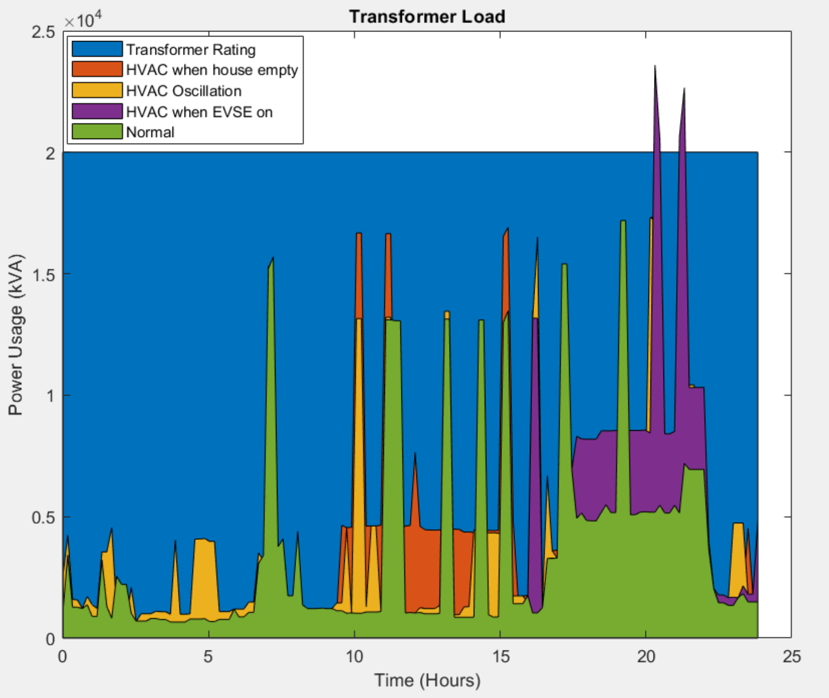
Example – Attacking Household HVAC Controls

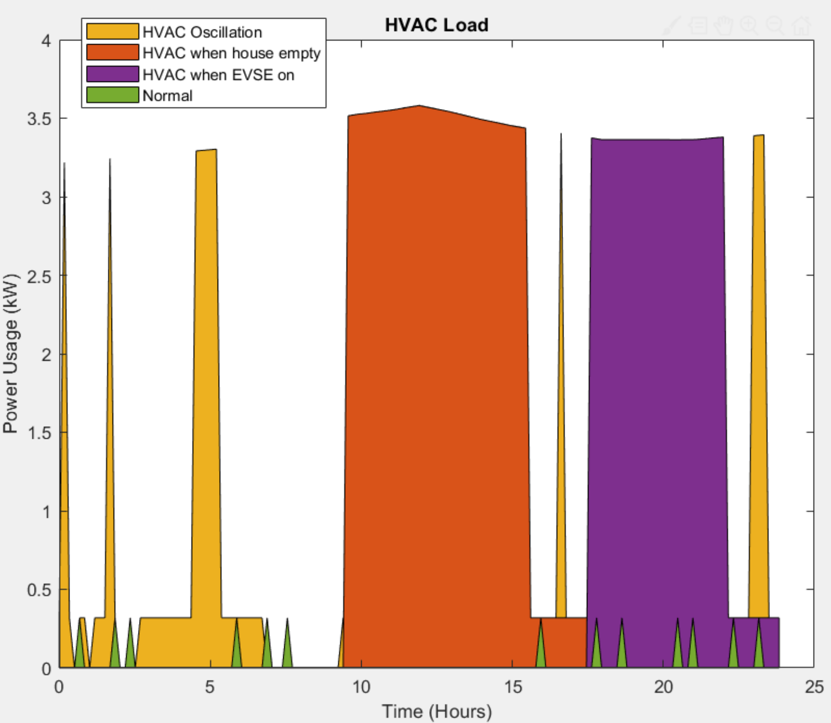
- Use Case:
  - Smart thermostats can be used to decrease energy use when occupants are not home and use up to 28% less electricity [5]
  - Smart thermostats are often internet-connected IoT devices which are susceptible to hacking [5]

- Attack Model:
  - Direct Load-Altering Attack: Attacker could exploit smart thermostat to ***increase*** load when occupants are not home

- Direct Impact:
  - Increased power consumption
  - Increased peak transformer load
  - Potentially dangerous in-home temperatures
  - Potential damage to HVAC hardware

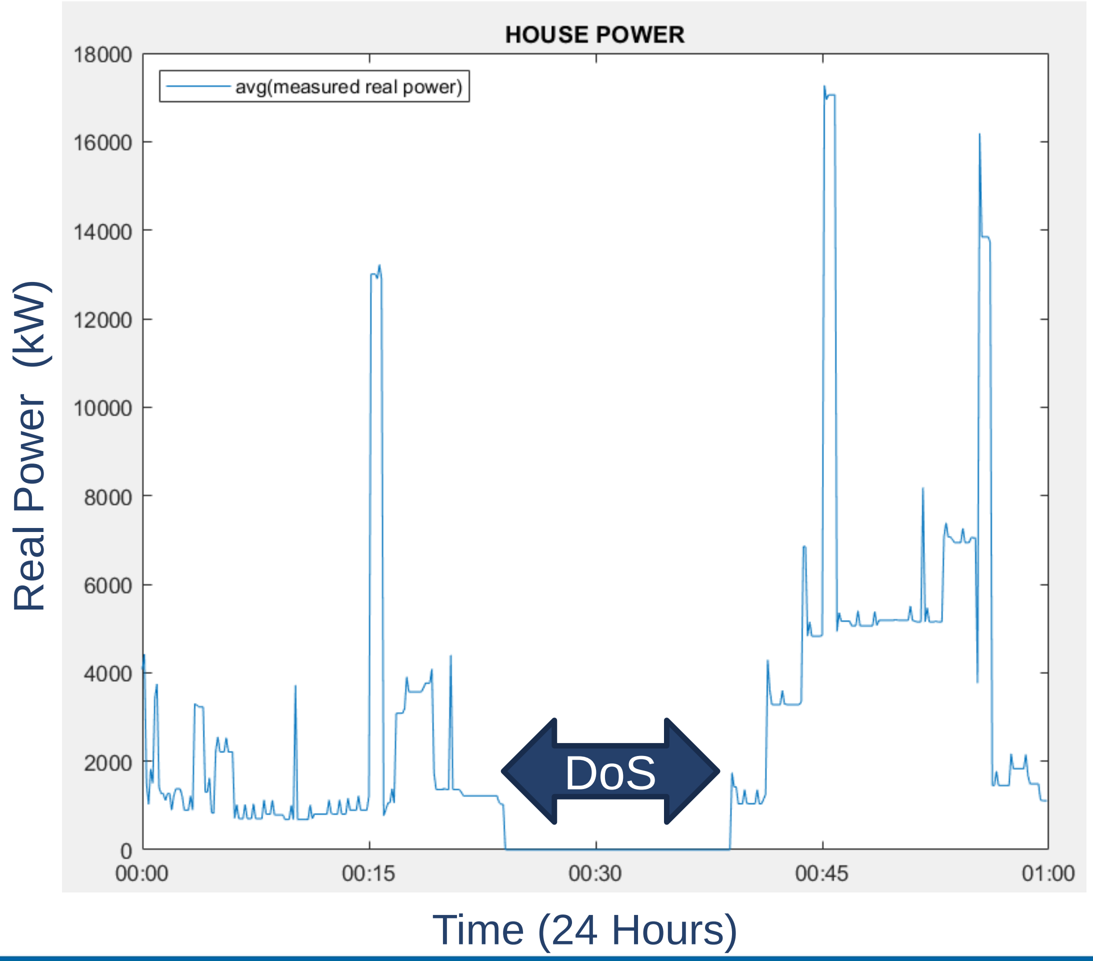
- **Cyber-Physical Attack Impact:**
  - **Coordination between several devices can form stealthy attacks and destabilization/damage to grid hardware**



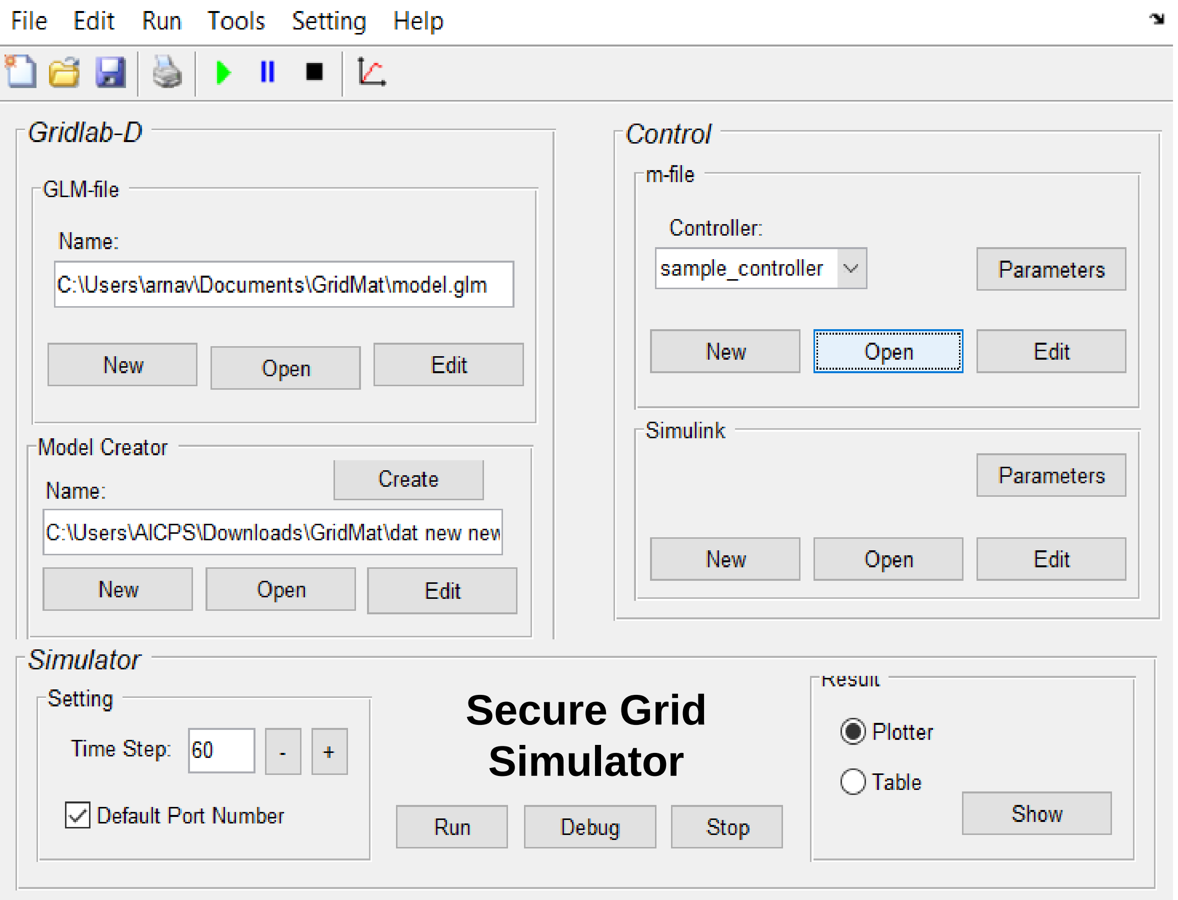


Example – DoS Attack from Compromised Smart Meter

- Use Case:
  - Smart Meters have capability to remotely disconnect customers
  - Smart Meters are part of the Advanced Metering Infrastructure (AMI) and have a 2-way communication link with the network
- Attack Model:
  - Power DoS Attack: Attacker could use compromised meter to directly disconnect customer’s power.
  - Communication DoS Attack: Multiple compromised meters can flood the network with bad data.
- Direct Impact:
  - Availability of power is compromised. Loss of service.
  - Data integrity is lost and/or communication network is disabled.
- **Cyber-Physical Attack Impact:**
  - **Coordination between compromised meters can cause localized blackouts**
  - **Strategic bad data injection with multiple compromised meters can hide the attack from monitoring systems (stealthy attack)**
  - **Coordinated on/off oscillations can potentially damage physical equipment**



User Interface



Secure Grid Simulator

GLM-file Name: C:\Users\arnav\Documents\GridMat\model.glm

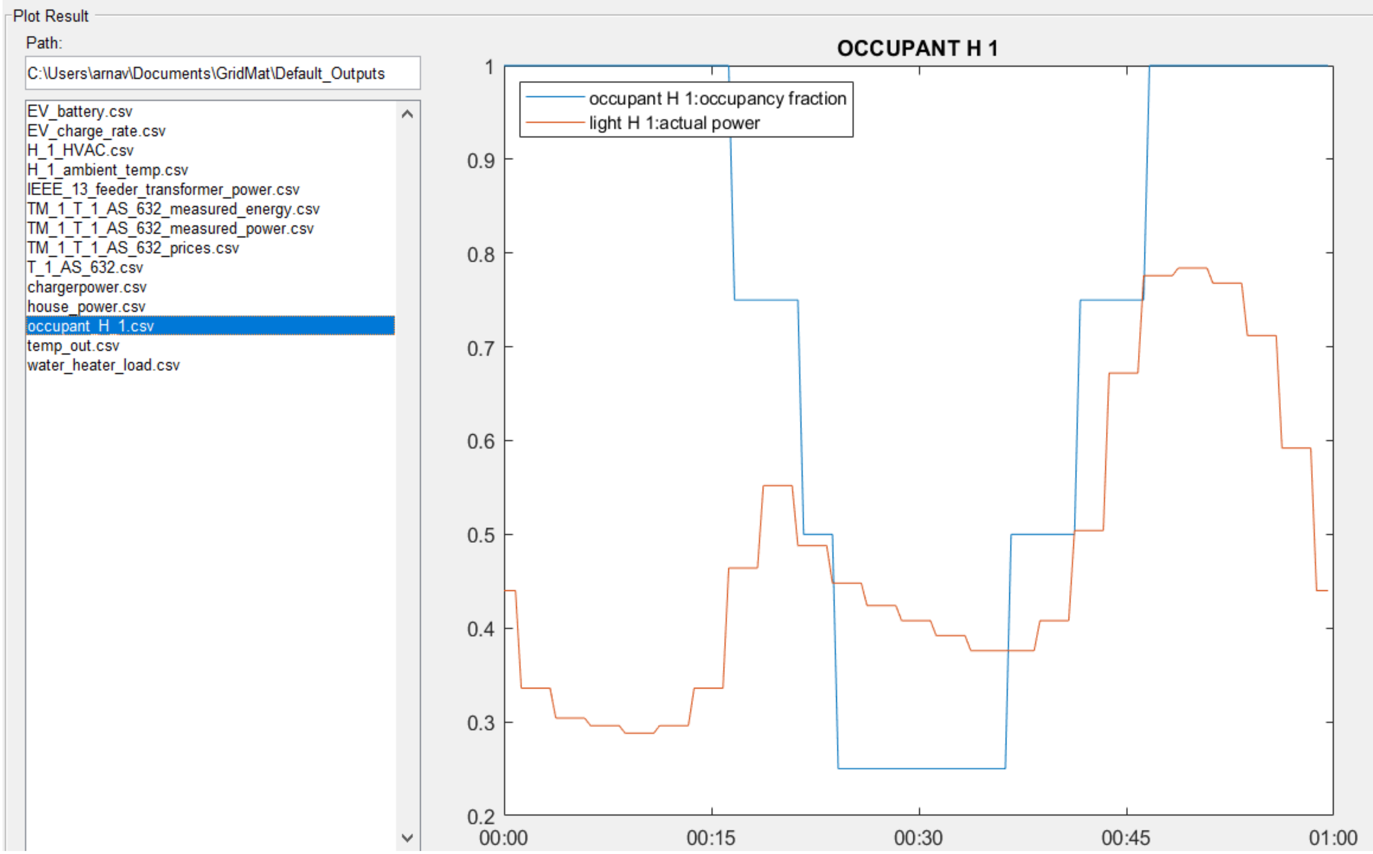
Model Creator Name: C:\Users\AICPS\Downloads\GridMat\dat new new

Controller: sample_controller

Time Step: 60

☑ Default Port Number

● Plotter
○ Table



Path: C:\Users\arnav\Documents\GridMat\Default_Outputs

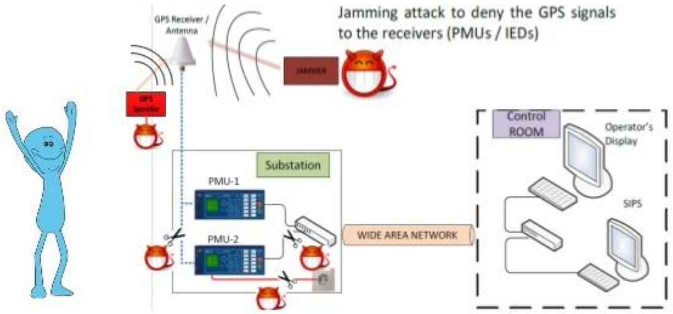
EV_battery.csv
EV_charge_rate.csv
H_1_HVAC.csv
H_1_ambient_temp.csv
IEEE_13_feeder_transformer_power.csv
TM_1_T_1_AS_632_measured_energy.csv
TM_1_T_1_AS_632_measured_power.csv
TM_1_T_1_AS_632_prices.csv
T_1_AS_632.csv
chargerpower.csv
house_power.csv
occupant_H_1.csv
temp_out.csv
water_heater_load.csv

Self-Secured Control with Anomaly Detection and Recovery in BMS of DER’s*

*Accepted to be published in the IEEE/ACM Design Automation and Test in Europe (**DATE'19**), Florence, Italy, March, 2019. **It acknowledges UCOP Grant LFR-18-548175**

Motivational Example of a Compromised System:

- **Case 1: Unreliable sensor data**
  - Example: GPS vulnerabilities in PMU could open grid to hacks.



* https://www.slideshare.net

- **Case 2: Attack on the physical system of the controller**
  - Example: A battery may be replaced with a low-quality alternative and cause the whole CPS to catch on fire since the BMS is unaware of the alteration of the physical system.

* https://insideevs.com/tesla-princess-car-battery-fire-video

- **Case 3: Biased machine learned models in the controllers can give wrong decisions**
  - Example: An image classifier model in an autonomous driving control may detect a ”STOP” sign as a ”Speed Limit” sign.

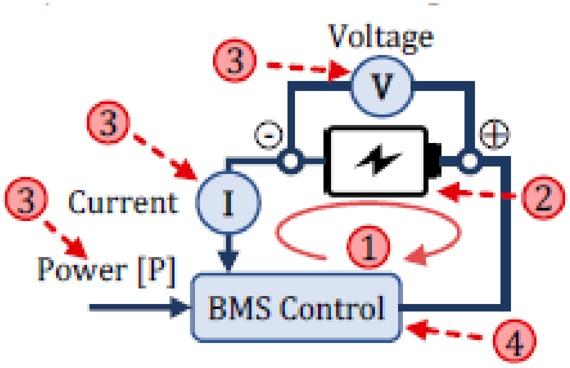
REAL
ATTACKED

Attack Model on BMS

- **Physical System Attack**
  - *Middle-man-attack*: Replace or alter the cells with the counterfeit ones without the BMS being aware of the alteration.
  - *Consequences*: Counterfeit physical system may not operate properly resulting in unstable states, e.g. fast draining battery cells or cells catching on fire.

- **Sensor Attack (DoS)**
  - Compromised voltage sensor of a battery may cause the BMS to over charge or over discharge the battery resulting in shorter battery lifetime or in the worst case explosion.

[1] BMS Control loop
[2] Physical Attack
[3] Sensor Attack
[4] Vulnerable Model



Methodology: Machine Learning Architecture for Self Secured Control

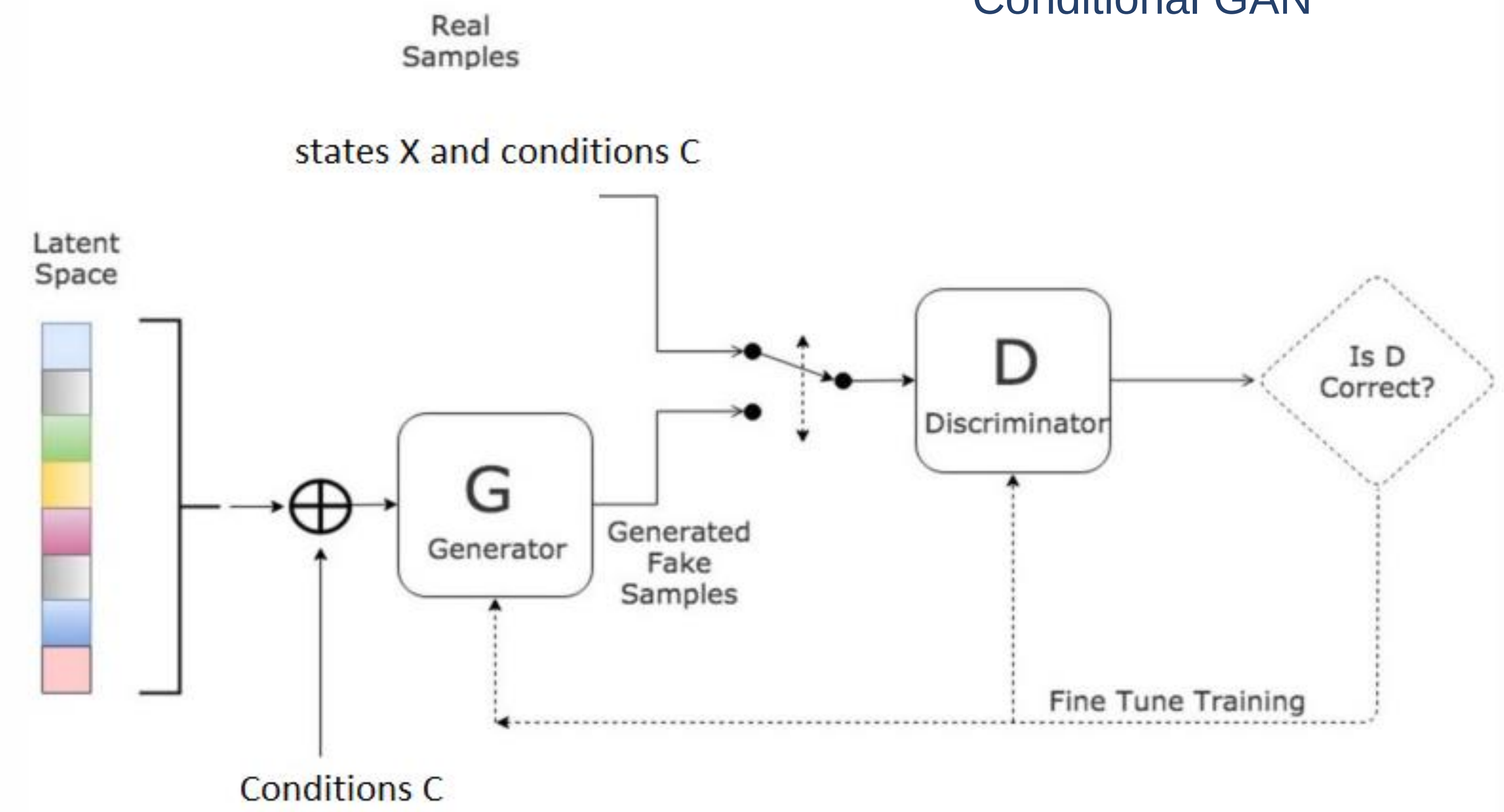
- **First Phase: Train-Only Phase**

➢ ***Discriminator*** will tell the difference between real and fake states based upon some conditions C.

➢ ***Generator*** will generate fake states closely related with the real states based upon similar conditions C.

➢ So the model will get better.

*Conditional GAN



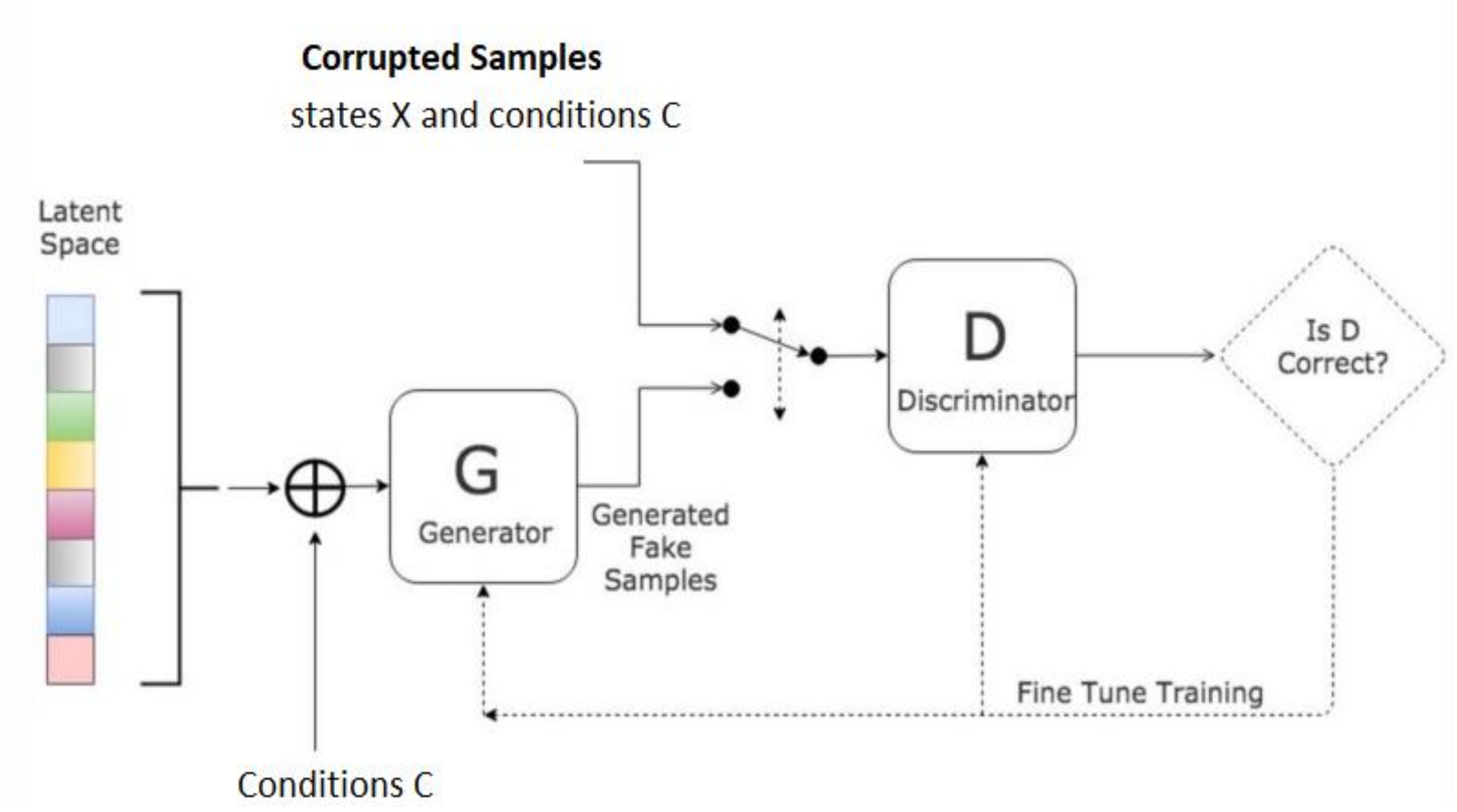
Methodology: Machine Learning Architecture for Self Secured Control

- **Second Phase: Detect-n-Predict Phase**

- ***Anomaly detection: Discriminator*** *can give a probability of detecting anomaly* for given state X and conditions C.

- ***Recovering Prediction: Generator*** will generate fake states closely related with the real states based upon similar conditions C.

*Conditional GAN



Experimental Setup:

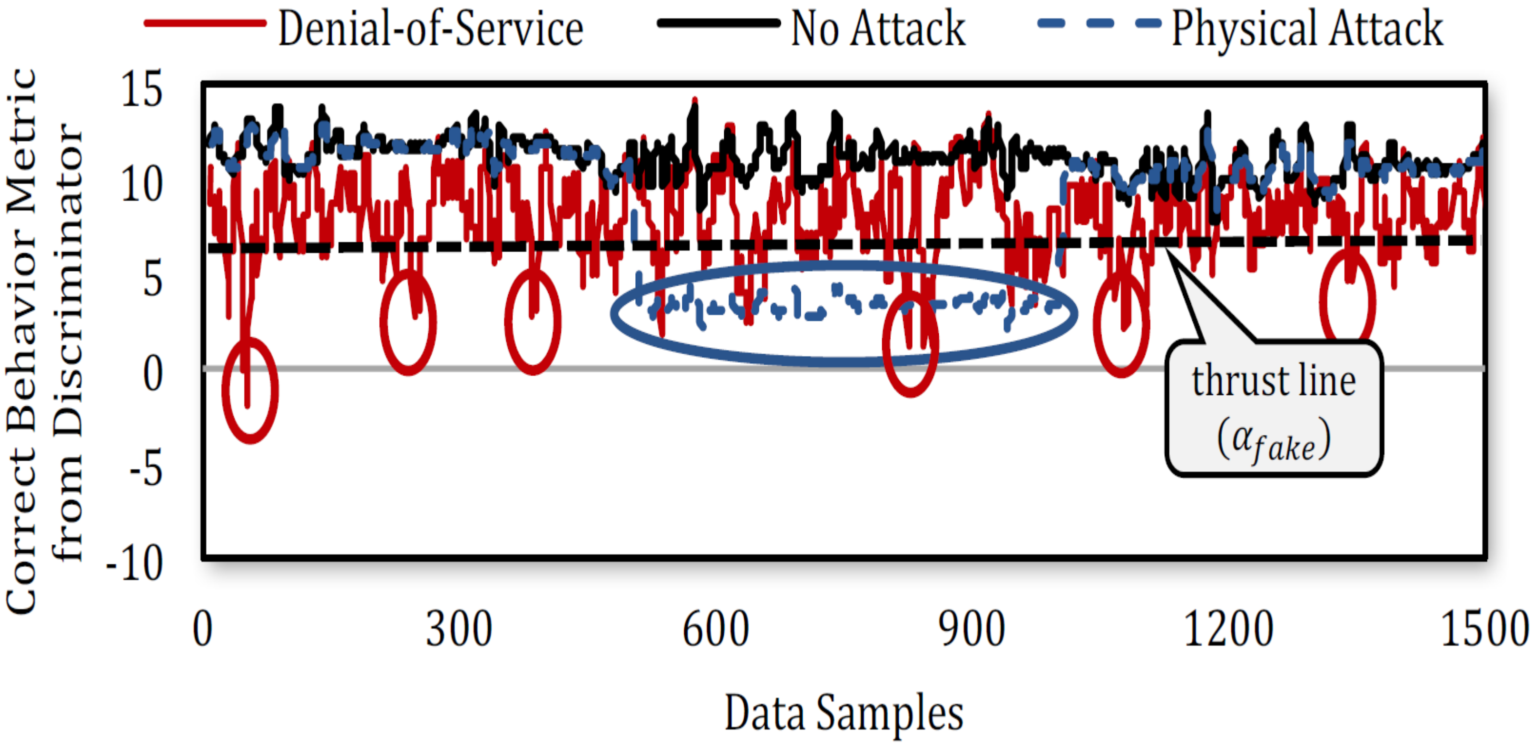
- The battery, sensors, and actuators are modeled in MATLAB.
- Lithium-ion battery cell 18650 has been used for the experiment.
- A Nissan Leaf S EV has been driven on a standard driving cycle NEDC and ECE as case studies.
- The training and prediction of the CGAN has been implemented using TensorFlow.
- The control algorithms of the self-secured BMS is running in python and communicating with MATLAB.

Results

- **Anomaly Detection**:

- 83% of the DoS attacks are detected.

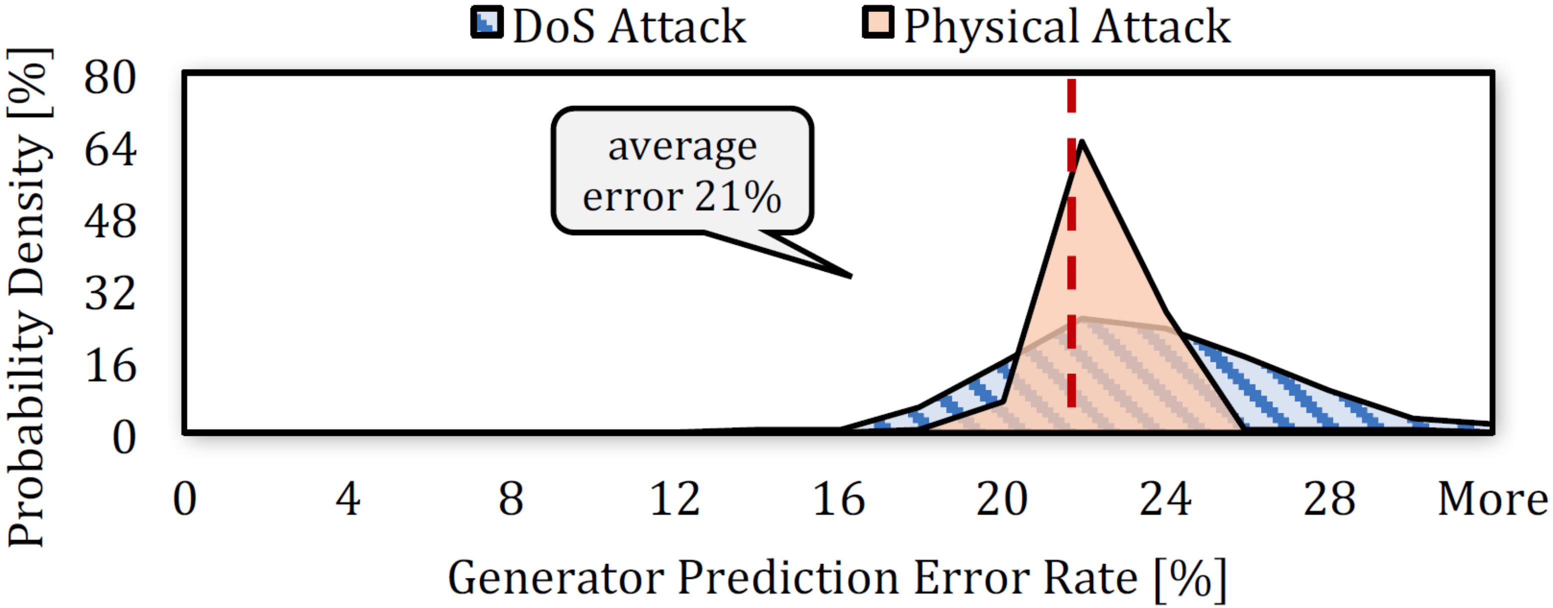
- 65% of the Physical attacks are detected.



Results

- **Prediction Recovering Error**

➢ Average prediction error resulted from the generator is about 21%.



Future Works:

❑ Continue further development of Secure-Grid-Simulator to handle Distributed Coordinated attacks on Smart Grid.

❑ Development of new architecture for Self Healing of the DER’s and their controllers from physical attacks.

❑ Combine Physics based modelling of the smart grid with the machine learning to make it robust.

Deliverables:

- M. A. Al Faruque et al., "Self Secured Control with Anomaly Detection and Recovery in Automotive Cyber-Physical Systems", *IEEE/ACM Design Automation and Test in Europe (DATE'19)*, Florence, Italy, March 2019 (Accepted).

References:

1. Mo, Yilin, et al. "Cyber–physical security of a smart grid infrastructure." *Proceedings of the IEEE* 100.1 (2012): 195-209.
2. Shahidehpour, Mohammad, William F. Tinney, and Yong Fu. "Impact of security on power systems operation." *Proceedings of the IEEE* 93.11 (2005): 2013-2025.
3. Fang, Xi, et al. "Smart grid—The new and improved power grid: A survey." *IEEE communications surveys & tutorials* 14.4 (2012): 944-980.
4. Al Faruque, Mohammad Abdullah, and Fereidoun Ahourai. "GridMat: Matlab toolbox for GridLAB-D to analyze grid impact and validate residential microgrid level energy management algorithms." *Innovative Smart Grid Technologies Conference (ISGT), 2014 IEEE PES*. IEEE, 2014.
5. Lu, Jiakang, et al. "The smart thermostat: using occupancy sensors to save energy in homes." *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*. ACM, 2010.

THANKS FOR YOUR ATTENTION !

Any Questions