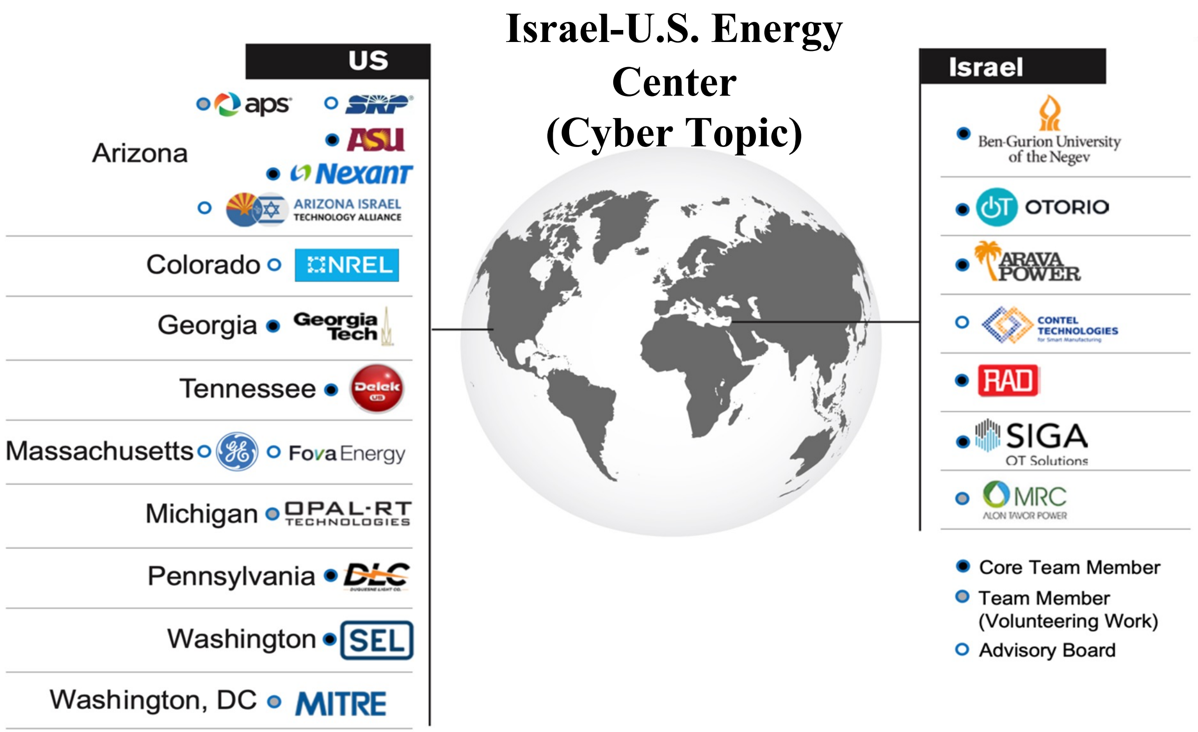
Comprehensive Cybersecurity Technology for Critical Power Infrastructure AI-Based Centralized Defense and Edge Resilience



Israel-U.S. Energy Center (Cyber Topic)

Prepared for

Itai Ganzer and **Ofer Goldhirsh**

Israel Innovation Authority

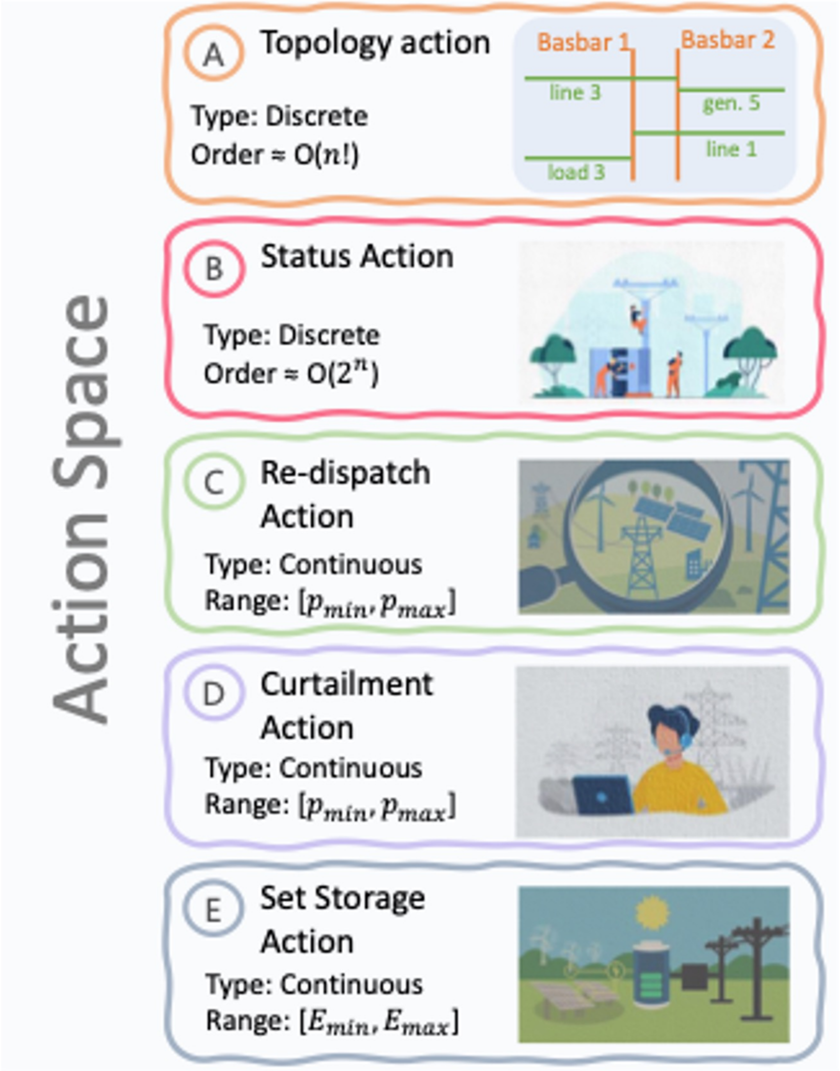
Avi Shavit and **Eynan Lichterman**

Israel Ministry of Energy

Heterogeneous Reinforcement Learning for Defending Power Grids and Commercialization

- Students: Mohammadamin Moradi, Zheng-Meng Zhai
- PI: Dr. Y.-C. Lai
- Academic Collaborator: Lead PI Yang Weng
- Industrial Collaborator: John Dirkman

Power Grids: Large and Diverse Action Space



Action Space

A Topology action

Type: Discrete

Order ≈ O(n!)

B Status Action

Type: Discrete

Order ≈ O(2^n)

C Re-dispatch Action

Type: Continuous

Range: [p_{min}, p_{max}]

D Curtailment Action

Type: Continuous

Range: [p_{min}, p_{max}]

E Set Storage Action

Type: Continuous

Range: [E_{min}, E_{max}]

Discrete actions:

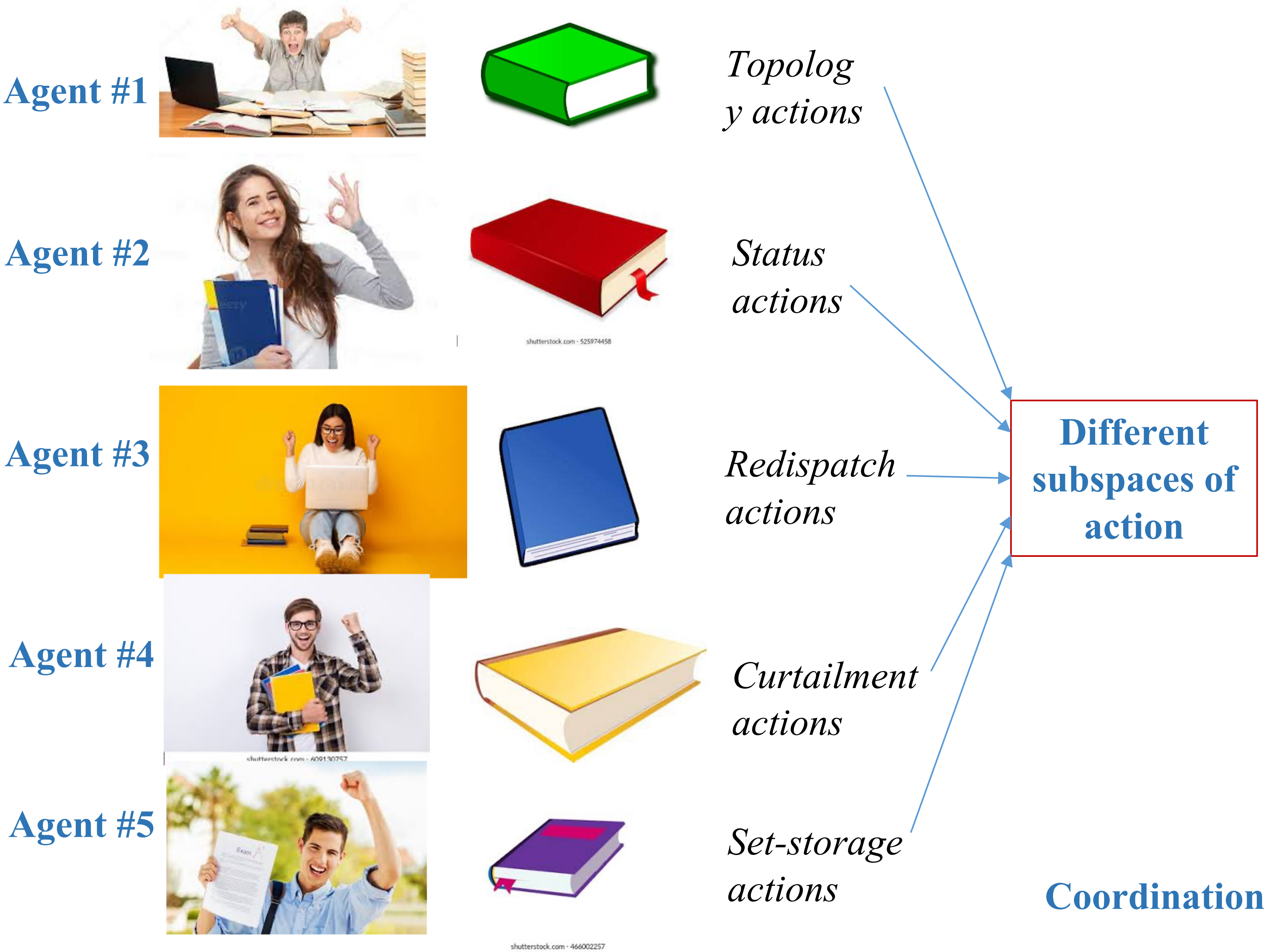
- *Topology actions*: changing the topology of certain substations (TG)
- *Status actions*: transmission or power line switching (PLS)

Continuous actions:

- *Redispatch actions*: changing the operating schedule of power plants
- *Curtailment actions*: limiting the production of renewable generators
- *Set-storage actions*: changing the role of some storage units from loads to generators or vice versa

Example: IEEE 118-Bus system: about 12 million possible actions

Reinforcement Learning CPS Control Analogy



Agent #1

Topolog y actions

Agent #2

Status actions

Agent #3

Redispatch actions

Agent #4

Curtailment actions

Agent #5

Set-storage actions

Different subspaces of action

shutterstock.com · 525974458
shutterstock.com · 609130757
Exam
shutterstock.com · 466002257

Test includes questions from the 5 books (Grid under attack)

RL Environment

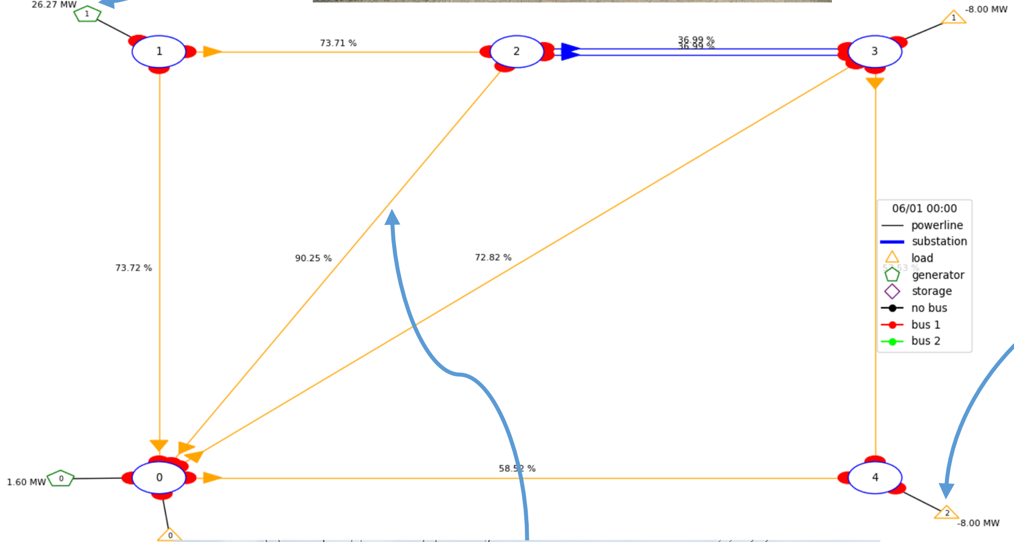
Goal: maximizing reward or grid survival

Coordination: Temporal Graph Convolutional Network

Power Grid on Grid2op Platform

Generator station

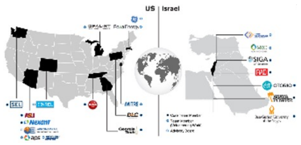
Load: a Small Town

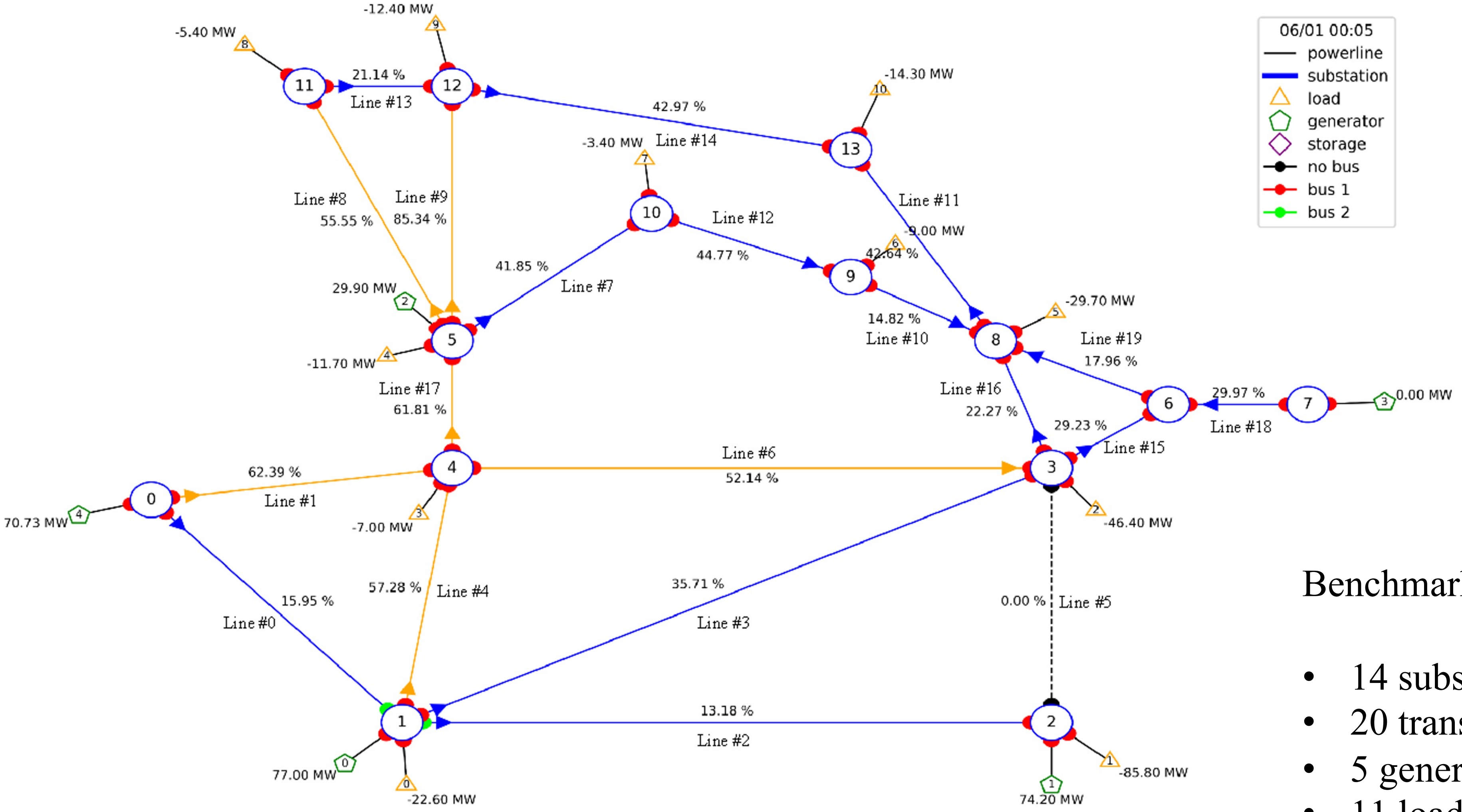


Substation (Bus)

Transmission lines

A Power Grid Network

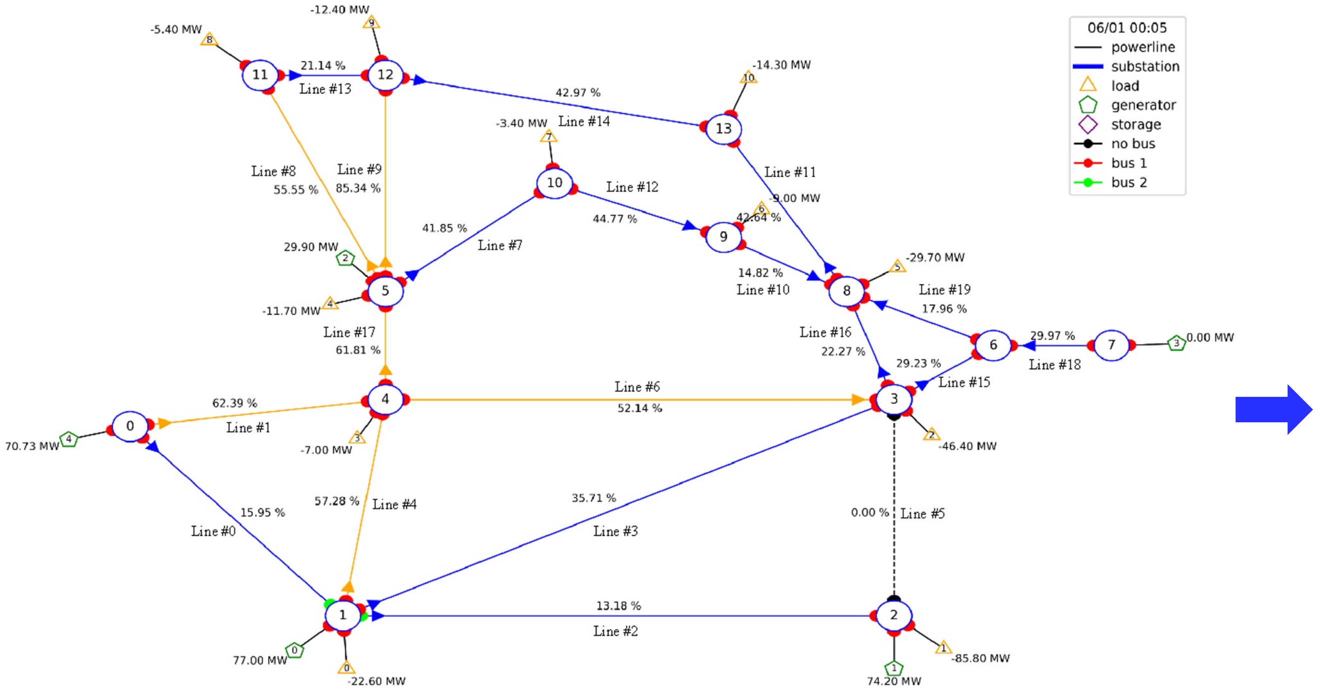


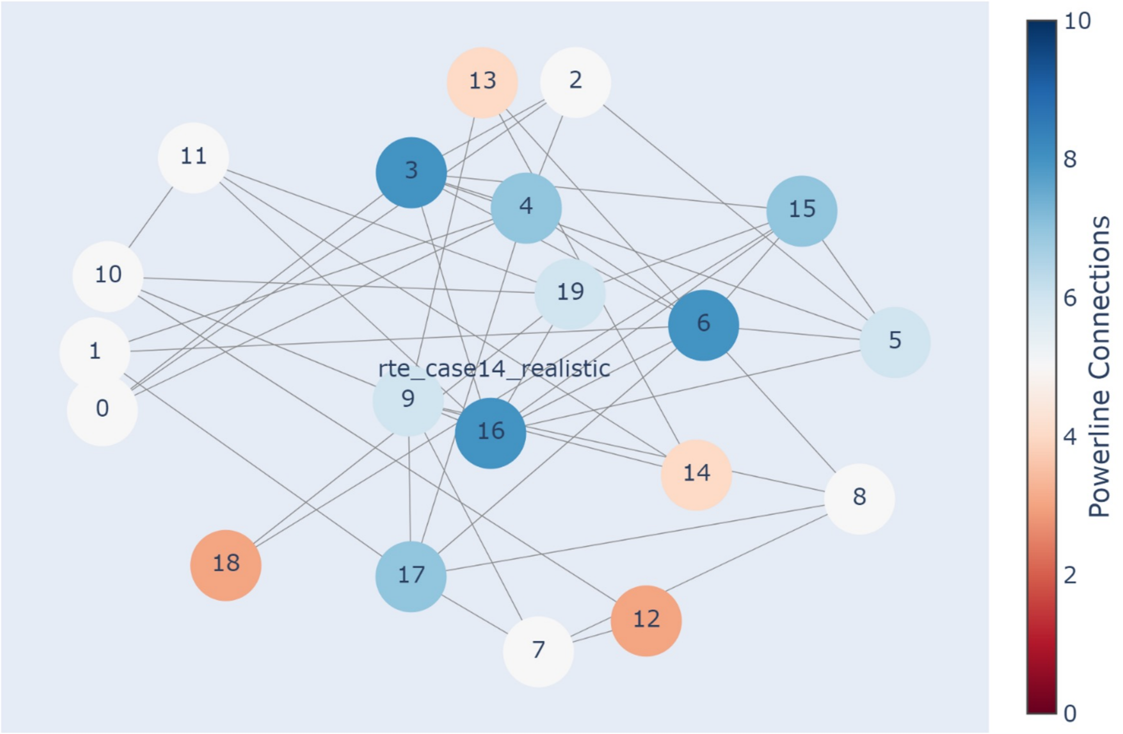


Benchmark RTE 14 Bus System:

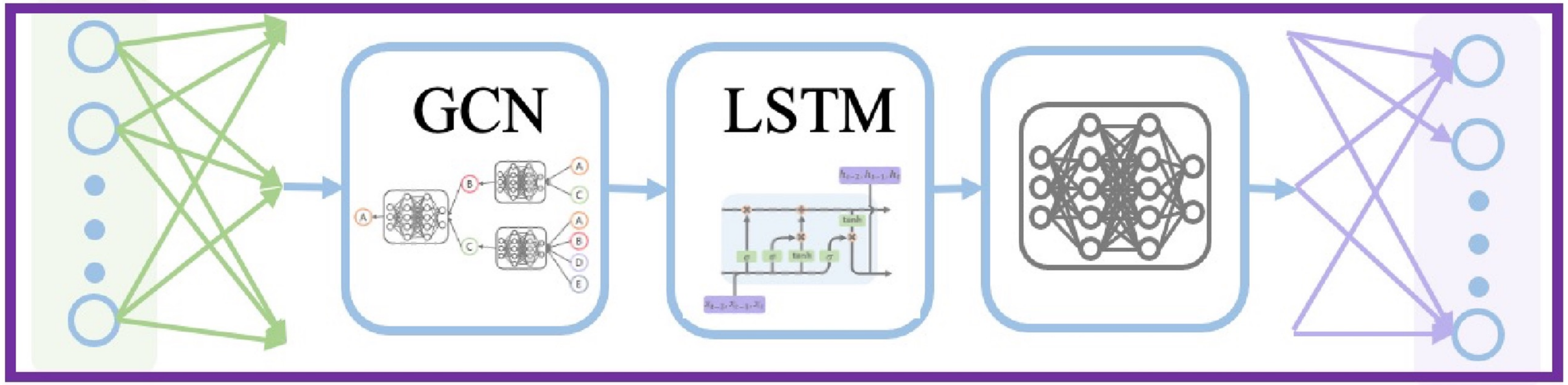
- 14 substations
- 20 transmission lines
- 5 generattors
- 11 loads

Line Graph of Power Grid Network



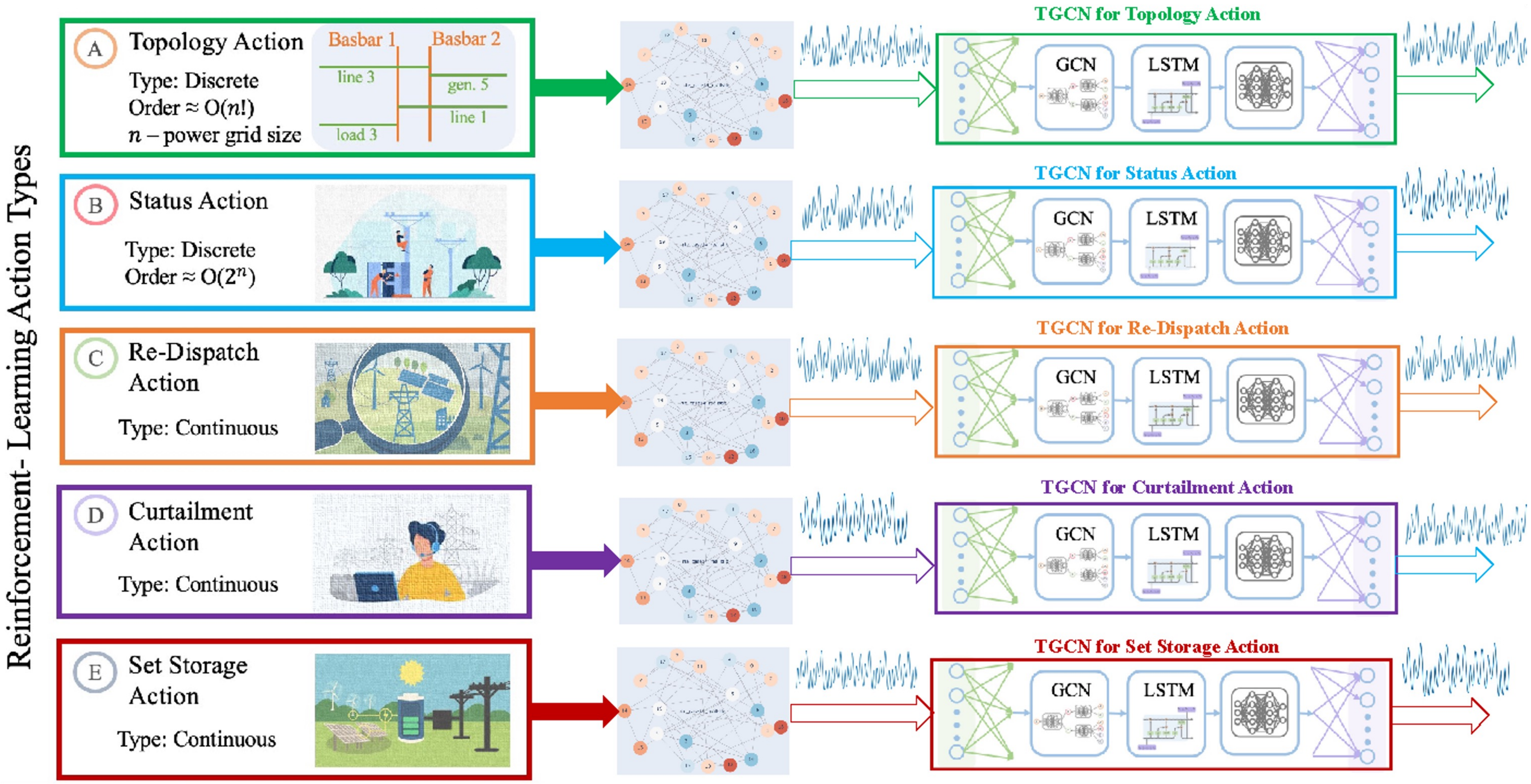


Temporal Graph Convolutional Neural Network (TGCN)



- TGCN: action specific (e.g., **five different TGCNs depending on the action types**)
- Input: currents from all nodes in the line graph
- Output: currents from all nodes in the line graph
- Training data: Grid2op simulations

Heterogeneous TGCN Framework



Reinforcement- Learning Action Types

A Topology Action
Type: Discrete
Order ≈ O(n!)
n – power grid size

B Status Action
Type: Discrete
Order ≈ O(2^n)

C Re-Dispatch Action
Type: Continuous

D Curtailment Action
Type: Continuous

E Set Storage Action
Type: Continuous

TGCN for Topology Action

TGCN for Status Action

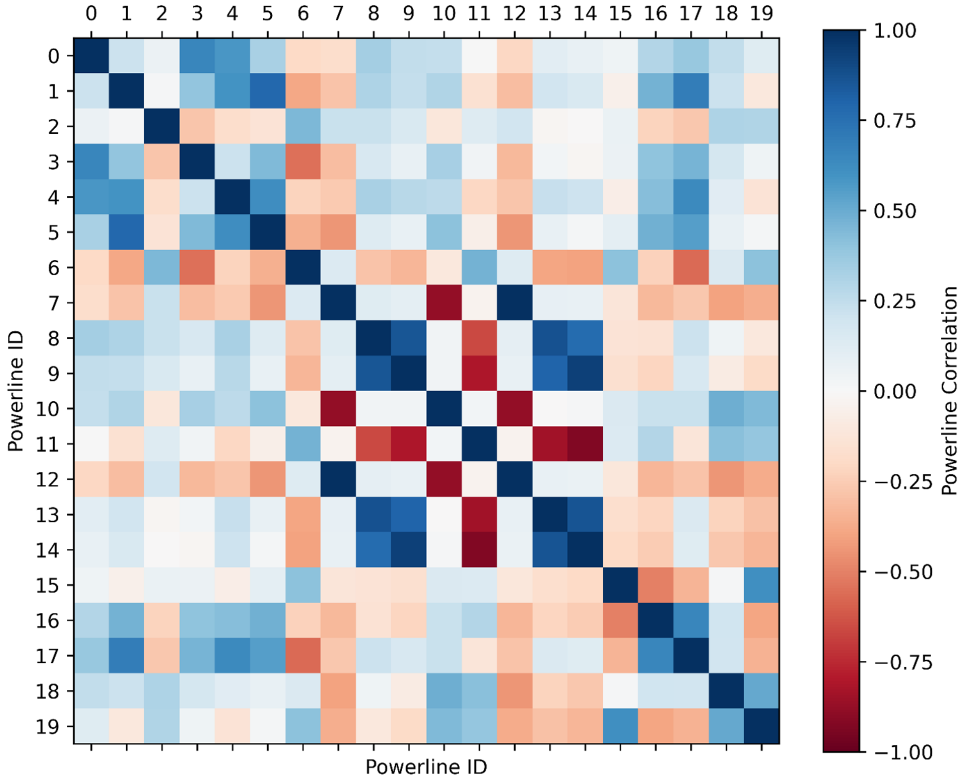
TGCN for Re-Dispatch Action

TGCN for Curtailment Action

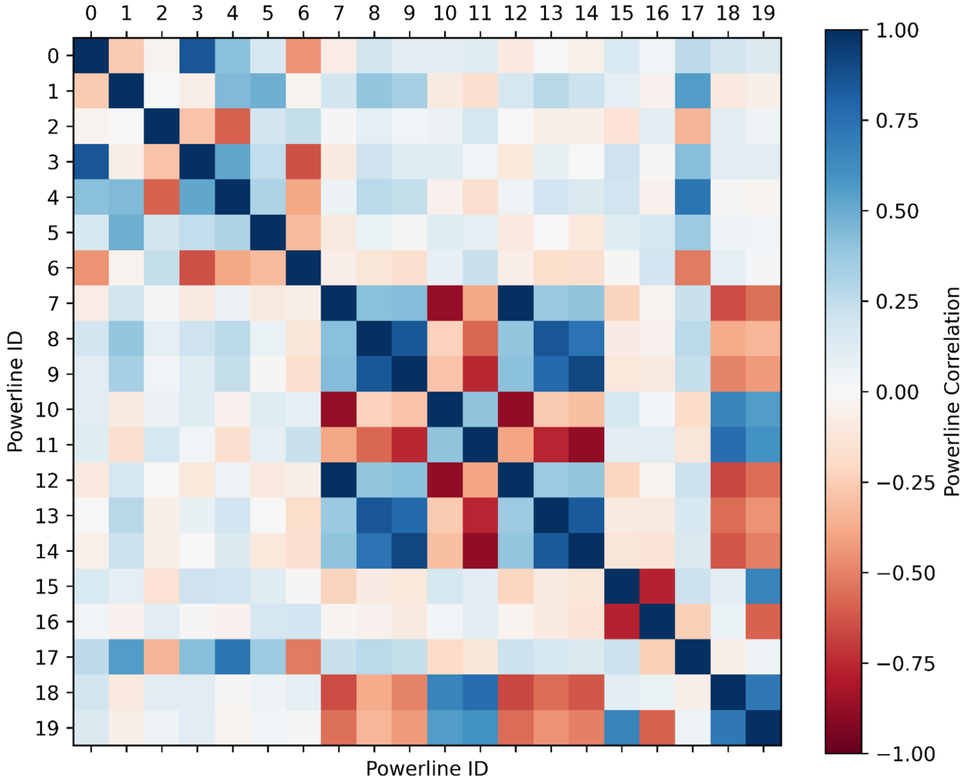
TGCN for Set Storage Action

Correlation of Line Current Flow under Attack

PLS Agent

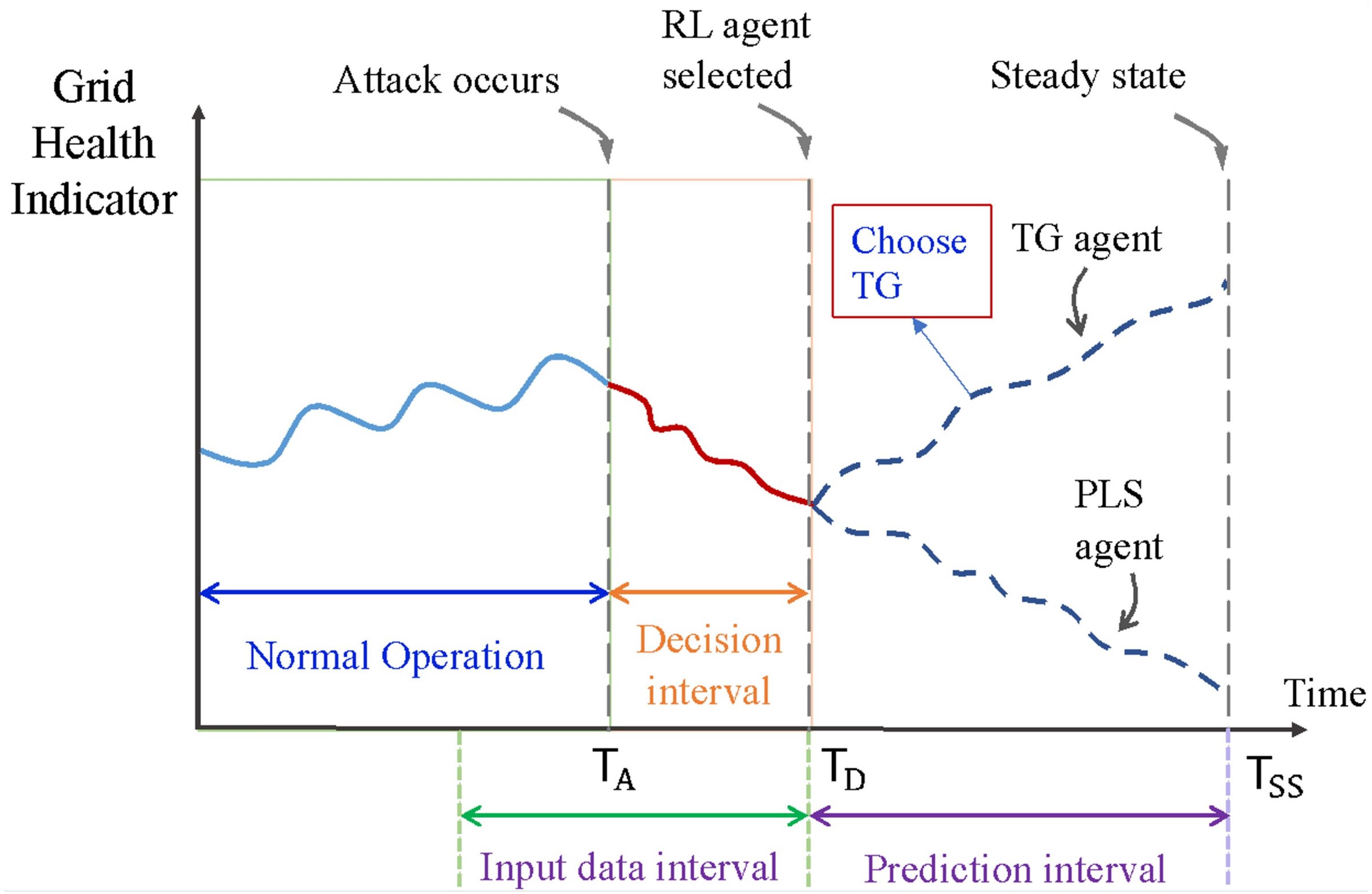


TG Agent



Correlations are neither too small nor too large, justifying TGCN

TGCN Aided RL for Optimal Agent Selection Under Attack

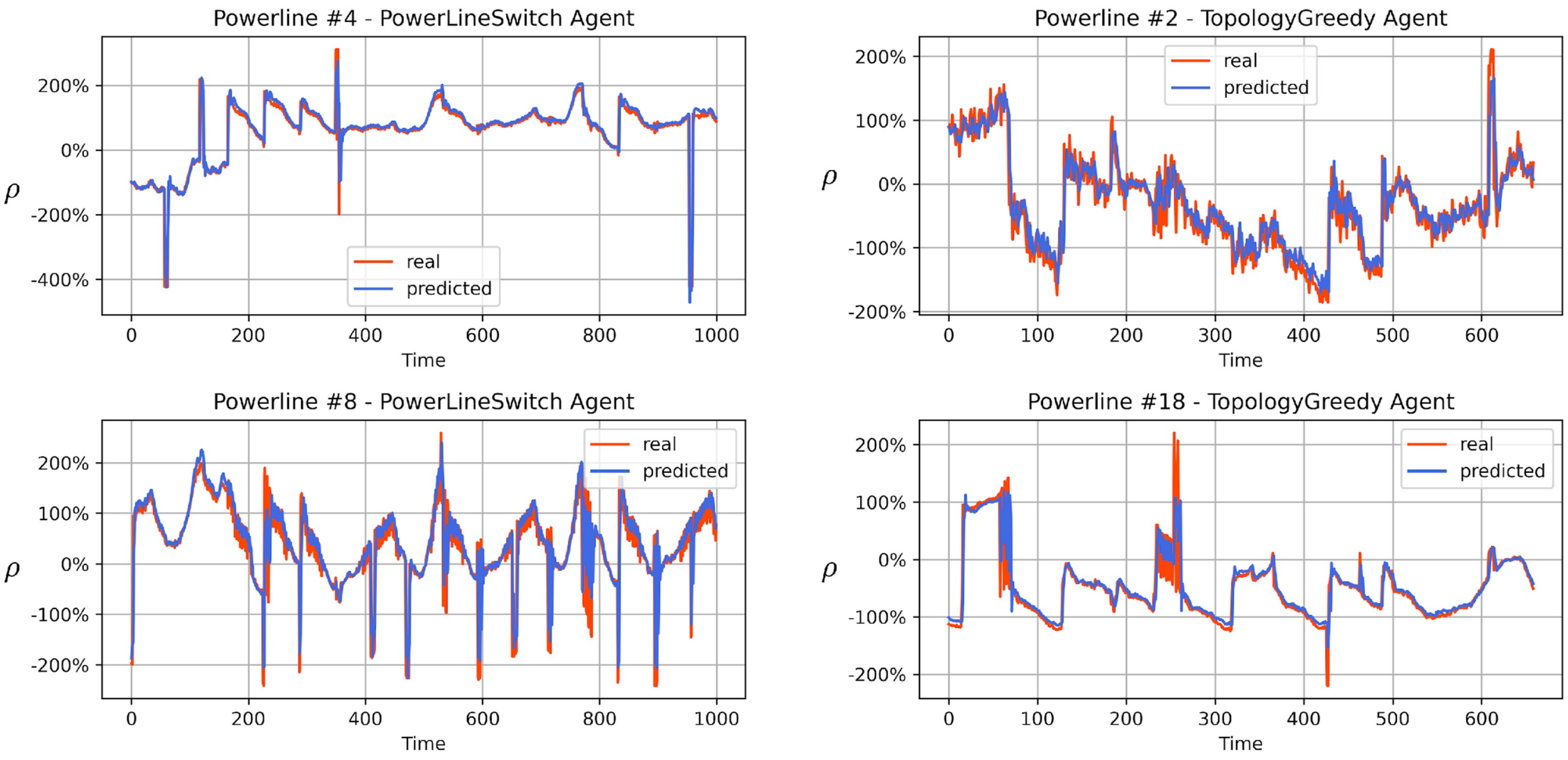


$$\varrho \equiv \frac{\textit{Line Current}}{\textit{Line Thermal Capacity}}$$

$N_>$ - number of lines in the network with ϱ greater than a threshold

$$\text{Reward} \equiv \frac{1}{1+N_>}$$

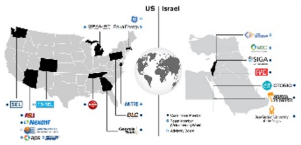
Examples of TGCN Prediction

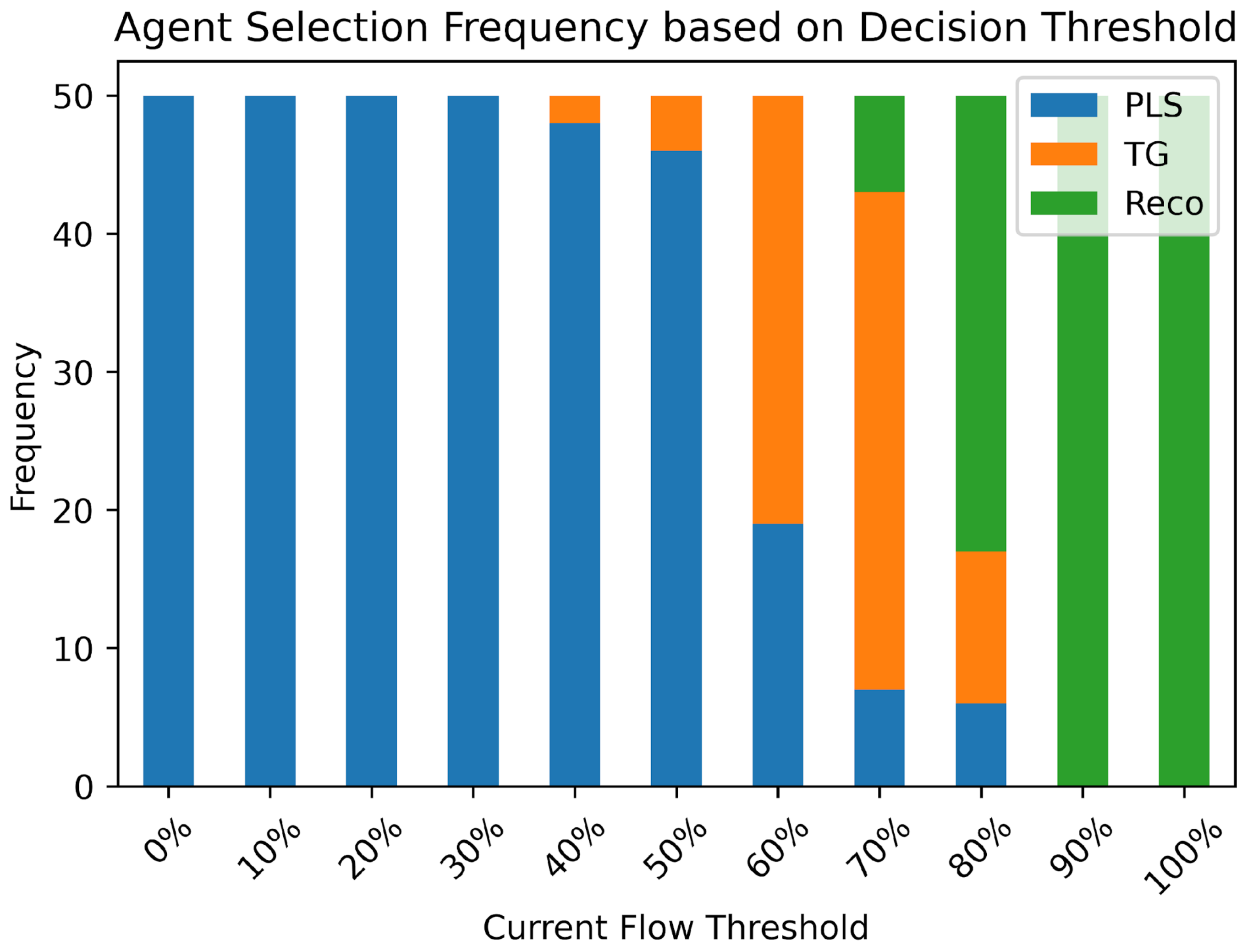


(a)

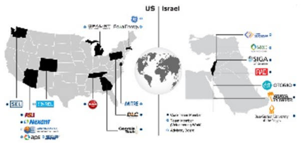
(b)

Selection of Controller Based on TGCN Prediction





Ongoing Commercialization Efforts

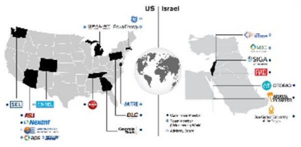


The ASU Task 16 team is working with John Dirkman’s team at *Resource Innovations Nexant* to implement the principle and methodologies of reinforcement learning control of cyber physical systems into the existing industrial software tools.

RI Team: John Dirkman, Guanji Hou, Narsi Vempati, Roozbeh Emami
ASU Team: Mohammadamin Moradi, Zheng-Meng Zhai, Ying-Cheng Lai

- **Motivation**: Reinforcement learning (RL) plays an increasing role in defending the critical infrastructures against cyberattacks. However, even for small power grids, the action space of RL is large, rendering efficient exploration by the RL agent practically unattainable.
- **Basic research**: developed RL methods solve the large action space problem in the power grid security setting by exploiting TGCNs □ a parallel but heterogeneous RL framework.
- **Idea**: Dividing the action space into smaller subspaces, each explored by a RL agent, and employing a series of TGCNs to efficiently organize the spatiotemporal action sequences by accurately predicting the performance of each individual RL agent in the event of an attack.
- **Methodology**: Selecting the top performing agent, resulting in the optimal sequence of actions.
- **Numerical demonstration**: Using TGCN to capture both the temporal and spatial dependencies of the graph structured data from IEEE 5-bus and 14-bus systems.
- **Significance**: TGCN framework □ a computationally efficient framework for generating the best course of actions to defend cyberphysical systems against attacks.

Ongoing Commercialization Efforts – Example 1



Issues addressed at the July 24 Meeting:

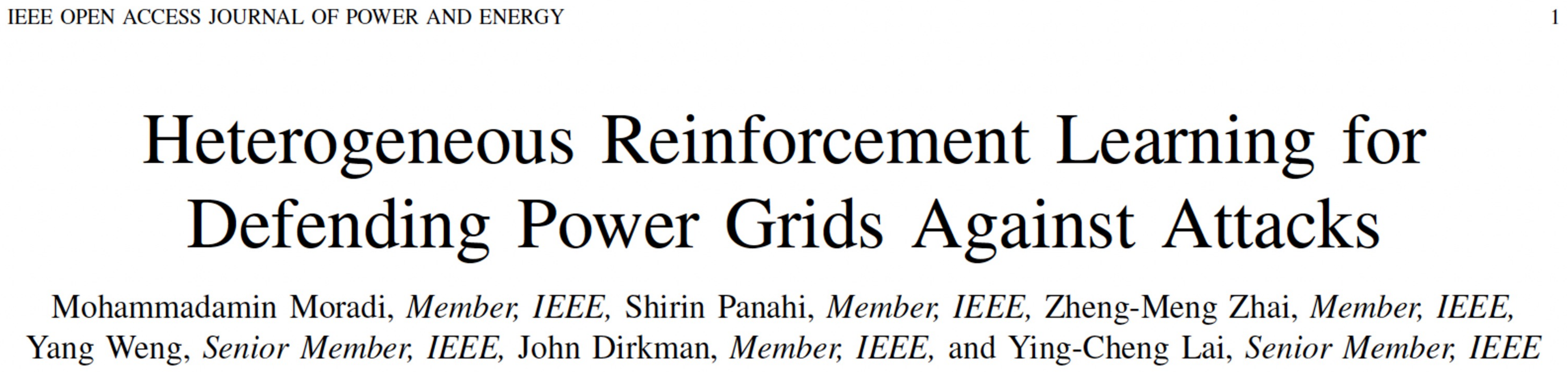
- **Agents' Response to False Detection**: Explained about how agents react to false detections.
- **Agents' Compatibility with Different Action Spaces**: Talked about the possibility of combining agents with various action spaces to improve performance.
- **Defining Custom Environments from Time Series**: Discussed the process of defining custom environments using time series data.
- **Extending Existing Data to Create Custom Environment**: Discussed about leveraging the existing data as a foundation for extending it into a custom environment.
- **Computational Burden of Environment Definition**: Raised concerns about the computational burden of defining a custom environment.
- **Feasibility of obtaining Time Series from Customers**: John Dirkman confirmed the feasibility and validity of obtaining time series data from customers.

Ongoing Commercialization Efforts – Example 2

Issues addressed at the August 8 Meeting:

- Guanji’s inquiry about the code flow, seeking a clear understanding of the overall logic and module interactions.
- A detailed explanation of inputs required for the TGCN module.
- Guanji’s questions about the roles of TensorFlow and Grid2Op in the project, emphasizing their contributions to deep learning and power grid simulation, respectively.
- Clarification provided on the roles of various agents within the project.
- A demonstration of custom environment creation flow, along with a display of chronics for predefined environments.

Publications

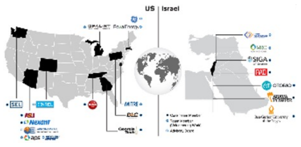
1. M. Moradi, Y. Weng, and Y.-C. Lai, “Defending smart electrical power grids against cyberattacks with deep Q-learning,” *PRX Energy* **1**, 033005, 1-13 (2022);
2. L.-W. Kong, Y. Weng, B. Glaz, M. Haile, and Y.-C. Lai, “Reservoir computing as digital twins for nonlinear dynamical systems,” *Chaos* **33**, 033111, 1-21 (2023).
3. M. Moradi, Y. Weng, J. Dirkman, and Y.-C. Lai, “Preferential cyber defense for power grids,” *PRX Energy*, in press.
4. 

IEEE OPEN ACCESS JOURNAL OF POWER AND ENERGY 1

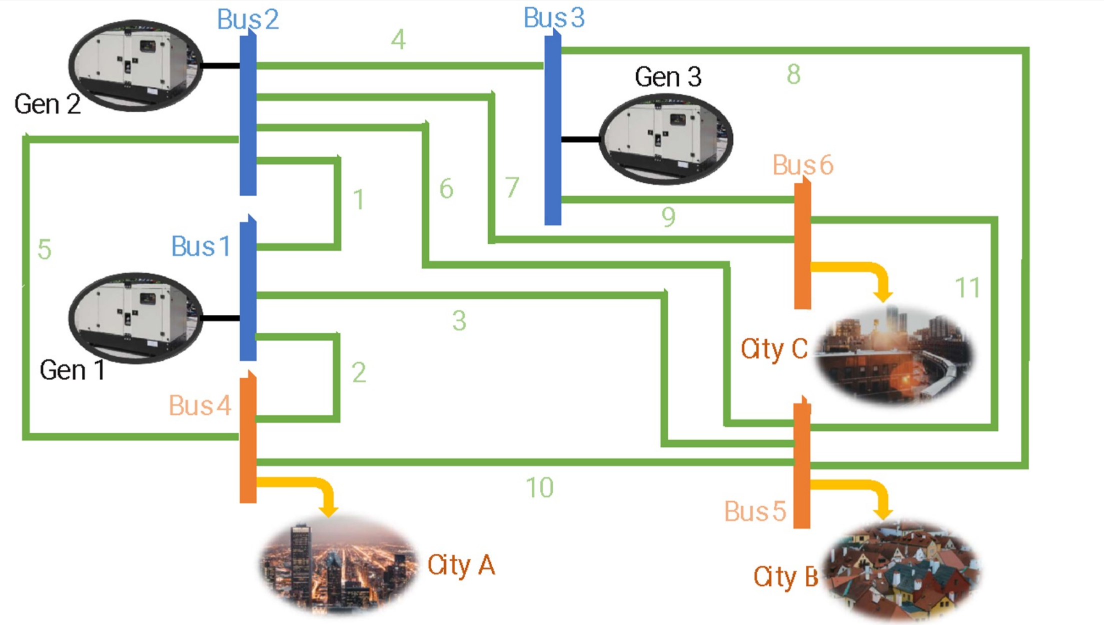
Heterogeneous Reinforcement Learning for Defending Power Grids Against Attacks

Mohammadamin Moradi, *Member, IEEE,* Shirin Panahi, *Member, IEEE,* Zheng-Meng Zhai, *Member, IEEE,* Yang Weng, *Senior Member, IEEE,* John Dirkman, *Member, IEEE,* and Ying-Cheng Lai, *Senior Member, IEEE*

Future Research (1)



- Continue to work closely with our industrial collaborators to test the heterogeneous RL/TGCN framework on real power grids using empirical data to bring the innovative cyberdefense framework closer to commercialization.



- Address the issue of limited available cyberdefense resources by incorporating preferences into heterogeneous RL/TGCN for protecting large smart power grids. This requires theoretical formulation, numerical test, and exploration for commercialization.

Preferential cyber defense for power grids

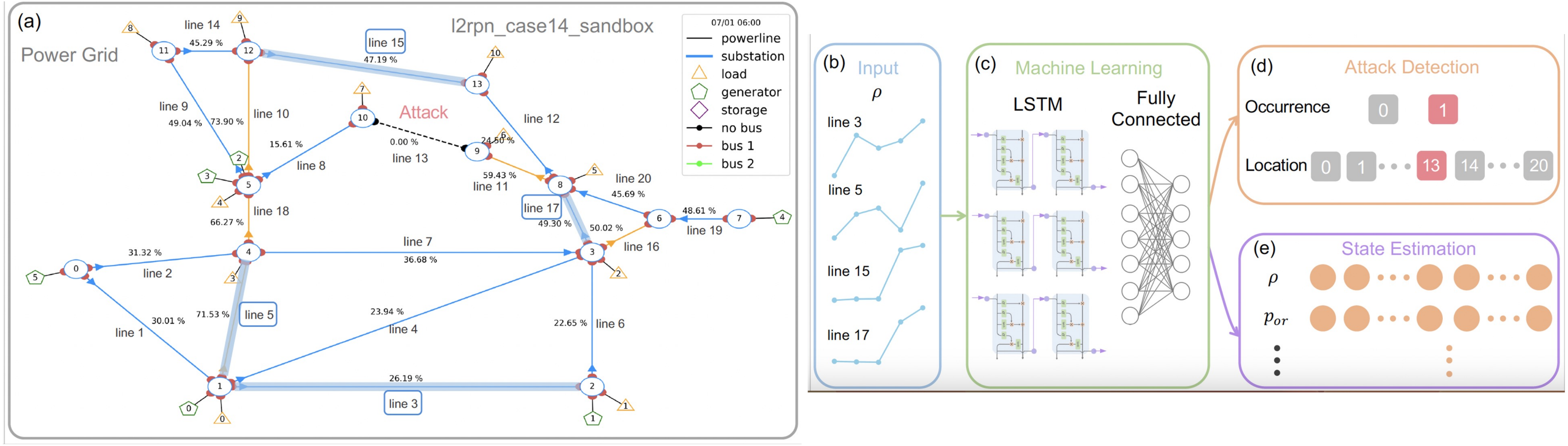
Mohammadamin Moradi,[1] Yang Weng,[1] John Dirkman,[2] and Ying-Cheng Lai[1,3,*]

[1] *School of Electrical, Computer and Energy Engineering,*
Arizona State University, Tempe, AZ 85287, USA
[2] *Resource Innovations, 719 Main Street, Half Moon Bay, CA 94019, USA*
[3] *Department of Physics, Arizona State University, Tempe, Arizona 85287, USA*
(Dated: July 27, 2023)

PRX Energy, in press

Future Research (2)

- Investigate the practical issue of partial state observation by developing an LSTM (long short-term memory) based framework for attack detection and full state estimation. Commercialization will be explored.



Future Research (3)

- ❖ Develop a comprehensive framework for probing the “uncharted” to solve the fundamental problem of exploration in machine learning, in particular RL.
- ❖ The problem is motivated by the fact that exploration plays a critical role in RL by enabling agents to discover optimal policies in unknown environments, but how this can be efficiently done remains to be a challenging problem.
- ❖ We propose an efficient approach to exploring the uncharted by leveraging automata theory and mixed integer programming, which enables the agent's behavior to be captured and the temporal or dynamic aspects of exploration to be modeled accurately for effective decision making and discovery of novel states.
- ❖ If successful, this will open a new area of research in AI and Machine Learning as applied to cyberphysical systems, with immediate applications to power grids.