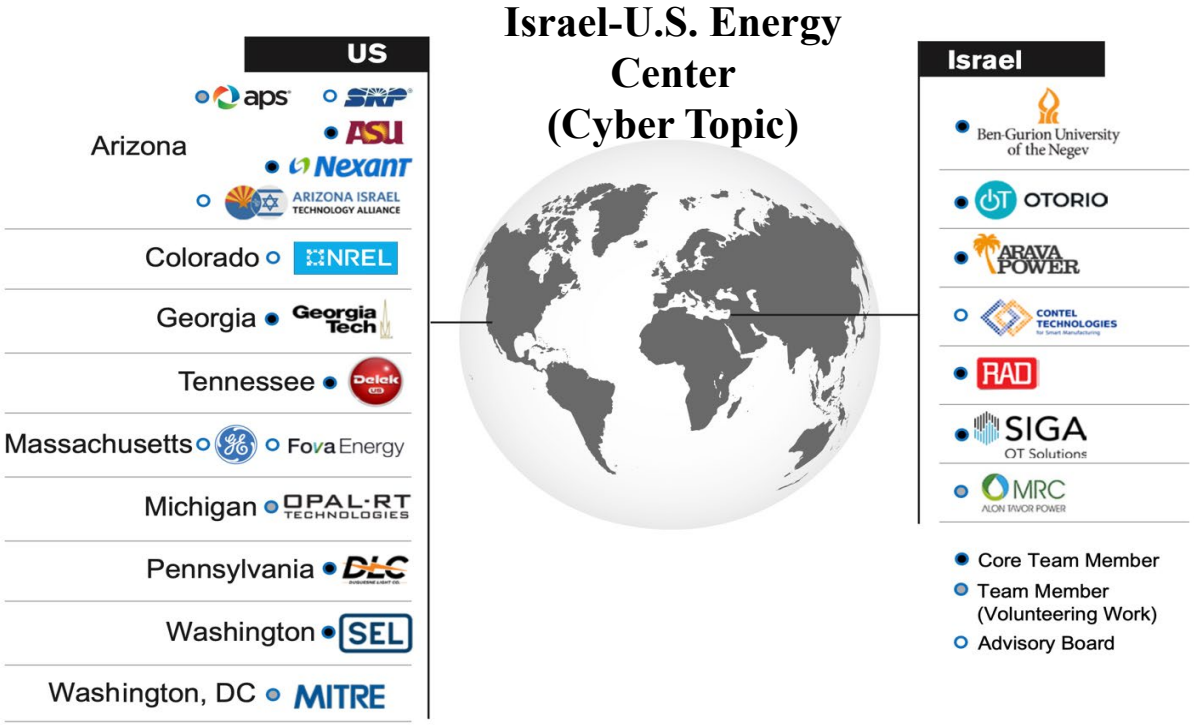
Comprehensive Cybersecurity Technology for Critical Power Infrastructure AI-Based Centralized Defense and Edge Resilience



Prepared for

Itai Ganzer and **Ofer Goldhirsh**

Israel Innovation Authority

Avi Shavit and **Eynan Lichterman**

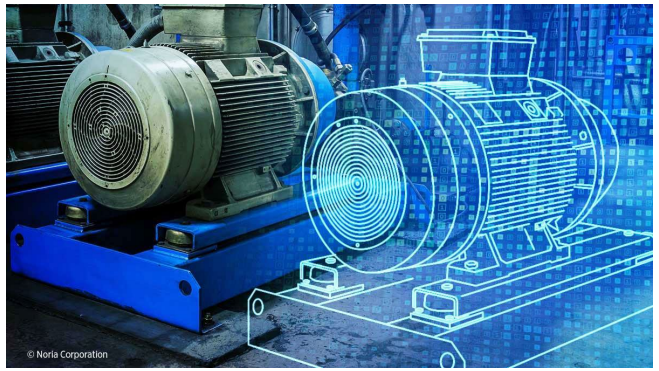
Israel Ministry of Energy

Task 11: AI Based Attack Detection

- Students: Ling-Wei Kong (graduating soon), Mohammadamin Moradi, and Zheng-Meng Zhai (new)
- Task Lead: Dr. Y.-C. Lai

One Product

Chaos ARTICLE scitation.org/journal/cha



Reservoir computing as digital twins for nonlinear dynamical systems

Cite as: Chaos **33**, 033111 (2023); doi: 10.1063/5.0138661
Submitted: 13 December 2022 · Accepted: 13 February 2023 ·
Published Online: 7 March 2023

View Online Export Citation CrossMark

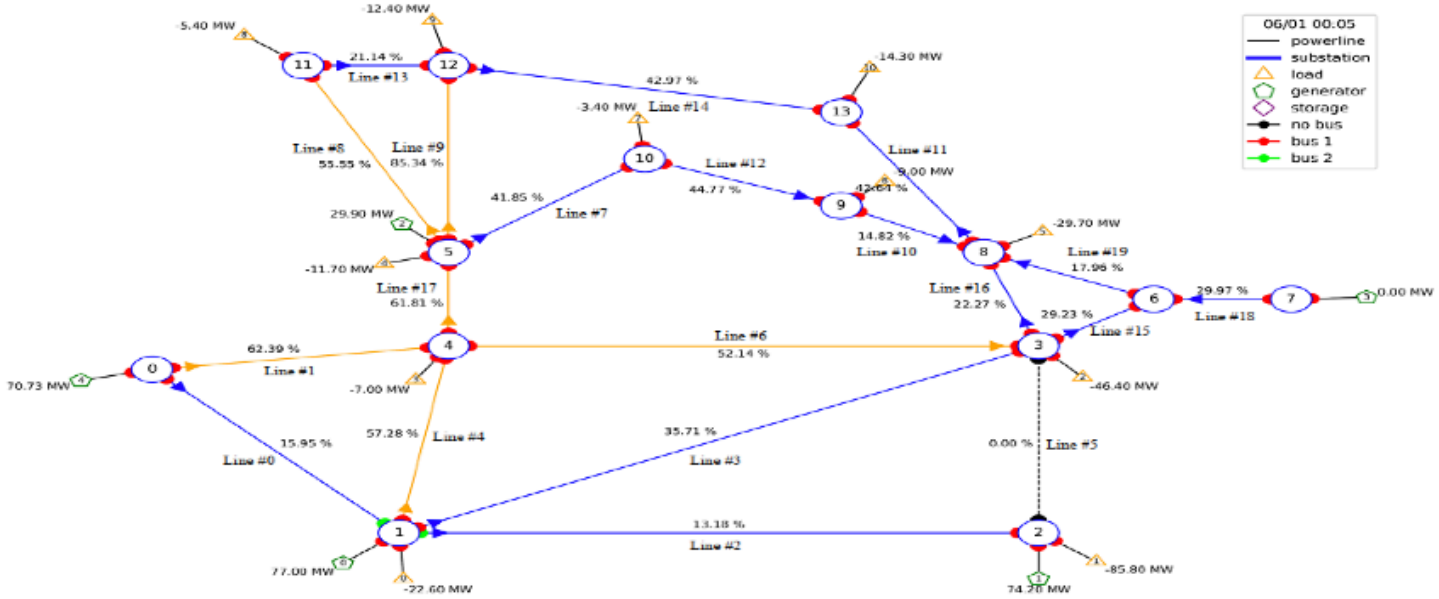
Ling-Wei Kong,[1] Yang Weng,[1] Bryan Glaz,[2] Mulugeta Haile,[2] and Ying-Cheng Lai[1,3,a)]

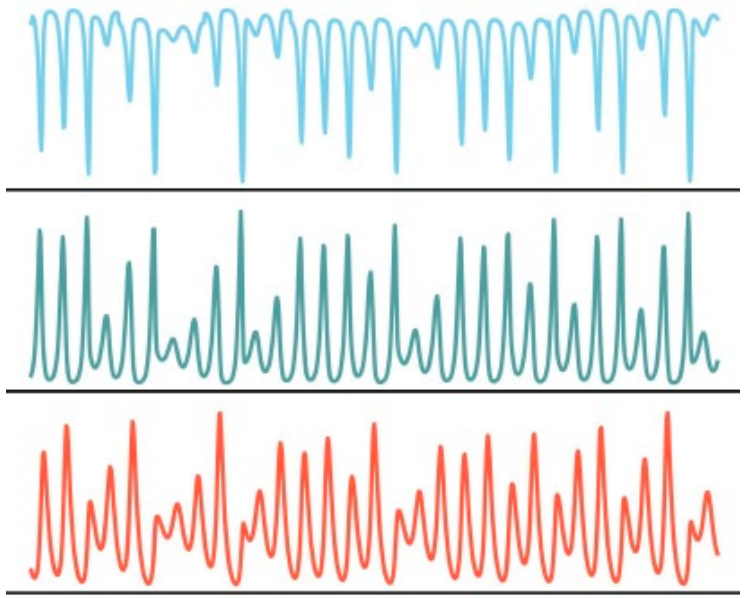
AFFILIATIONS

[1]School of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, Arizona 85287, USA
[2]Vehicle Technology Directorate, CCDC Army Research Laboratory, 2800 Powder Mill Road, Adelphi, Maryland 20783-1138, USA
[3]Department of Physics, Arizona State University, Tempe, Arizona 85287, USA

[a)]**Author to whom correspondence should be addressed:** Ying-Cheng.Lai@asu.edu

Problem Statement





- Attack causes K - an intrinsic parameter of the power grid, to vary with time
- Example of $K(t)$: number of lines whose currents exceeds a threshold

$$K(t) = ?$$

Inverse Problem

K = Constant: Parameter Identification

- **Least squares fitting** – e.g., E. W. Weisstein, Least squares fitting, https://mathworld.wolfram.com/ (2002)
- **Maximum likelihood estimation** – e.g., J.-X. Pan and K.-T. Fang, Maximum likelihood estimation, pp. 77-158 in Growth Curve Models and Statistical Diagnostics (Springer, 2002)
- **Bayesian estimation** – e.g., A. J. Haug, Bayesian Estimation and Tracking: A Practical Guide (John Wiley & Sons, 2012)
- **Genetic algorithm** – e.g., L. Yao and W. A. Sethares, Nonlinear parameter estimation via the genetic algorithm, IEEE Trans. Signal Proc. **42**, 927 (1994)
- **Neural networks** – e.g., P. Guo, M. R. Lyu, and C. L. P. Chen, Regularization parameter estimation for feedforward neural networks, IEEE Trans. Sys. Man Cyber. B **33**, 35 (2003)
- **Markov chain Monte Carlo** – e.g., F. Yandun, M. Torres-Torriti, and F. Auat Cheein, Markov chain Monte Carlo parameter estimation for nonzero slip models of wheeled mobile robots: A skid steer case study, J. Mech. Robot. **13** (2021)
- **Kalman filter** – e.g., G. Evensen, The ensemble Kalman filter for combined state and parameter estimation, IEEE Cont. Sys. Mag. **29**, 83 (2009); L. Ljung, Asymptotic behavior of the extended Kalman filter as a parameter estimator for linear systems, IEEE Trans. Auto. Cont. **24**, 36 (1979).

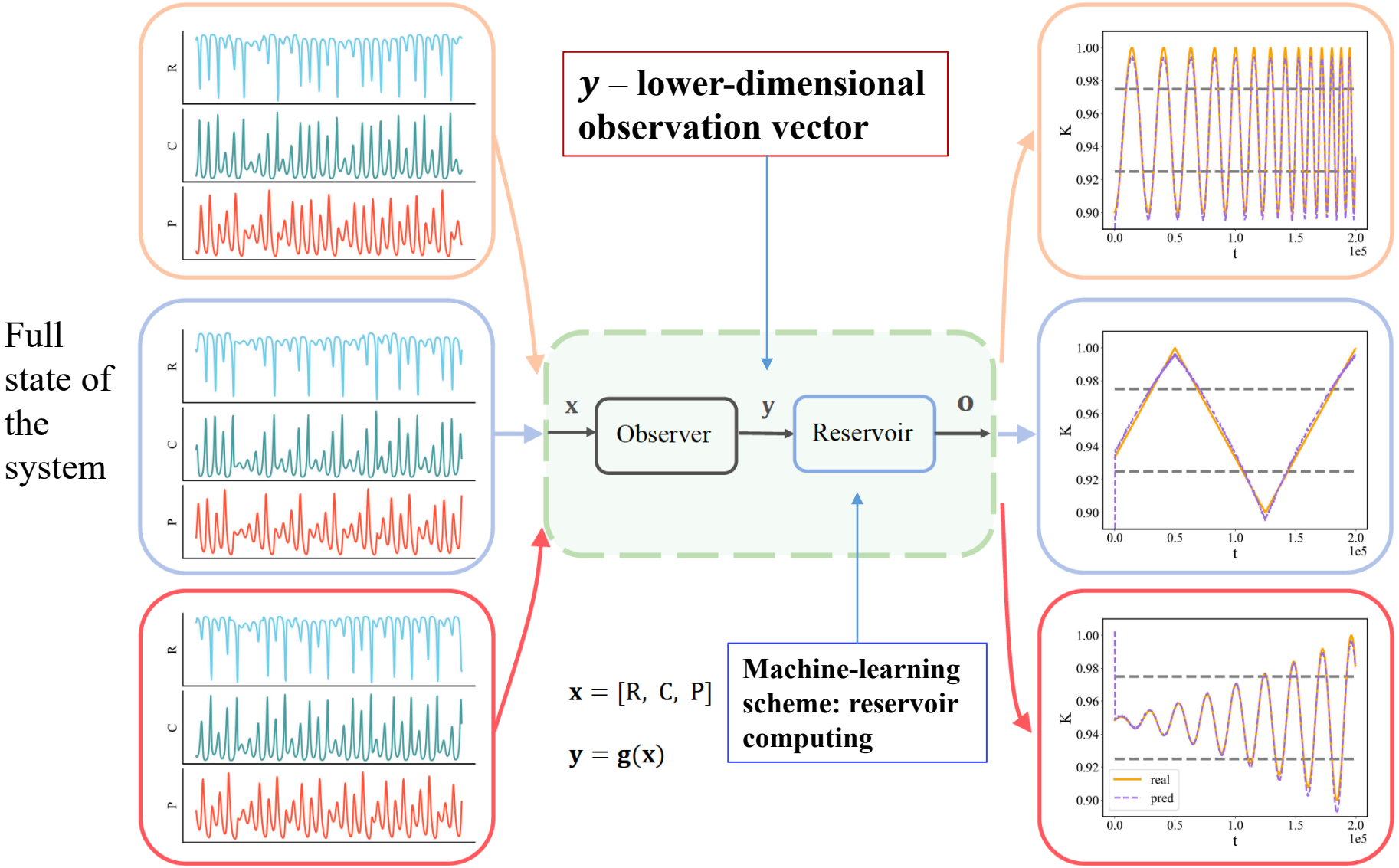
Time-Varying Parameter K(t): Parameter Tracking

Machine-learning methods:

- Y. Chen and Y. Zhou, Machine learning based decision making for time varying systems: Parameter estimation and performance optimization, Knowledge-Based Sys. **190**, 105479 (2020).
- Y. Zhang, Neural network algorithm with reinforcement learning for parameters extraction of photovoltaic models, IEEE Trans. Neural Net. Learning Sys. (2021).
- A. B. Abdusalomov, F. Safarov, M. Rakhimov, B. Turaev, and T. K. Whangbo, Improved feature parameter extraction from speech signals using machine learning algorithm, Sensors **22**, 8122 (2022).
- J. Hannink, T. Kautz, C. F. Pasluosta, K.-G. Gabmann, J. Klucken, and B. M. Eskofier, Sensor-based gait parameter extraction with deep convolutional neural networks, IEEE J. Biomed. Health Info. **21**, 85 (2016).
- X. Chen, Y. Tian, T. Zhang, and J. Gao, Differential evolution based manifold gaussian process machine learning for microwave filter's parameter extraction, IEEE Access **8**, 146450 (2020).
- M.-Y. Kao, F. Chavez, S. Khandelwal, and C. Hu, Deep learning-based BSIM-CMG parameter extraction for 10-nm finfet, IEEE Trans. Elec. Dev. **69**, 4765 (2022).

Limitation: full-state measurements – time series of all dynamical variables of the system are required

Our Work: Machine Learning with Partial Measurements

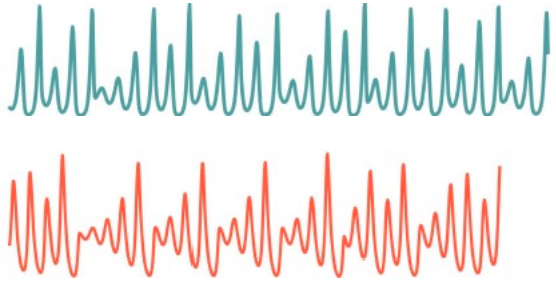


Parameter as a function of time

Zheng-Meng Zhai, Mohammadamin Moradi, Bryan Glaz, Mulugeta Haile, and Ying-Cheng Lai, "Tracking parameter variations in nonlinear dynamical systems using machine learning," preprint (2023)

Machine-Learning Strategy - Training

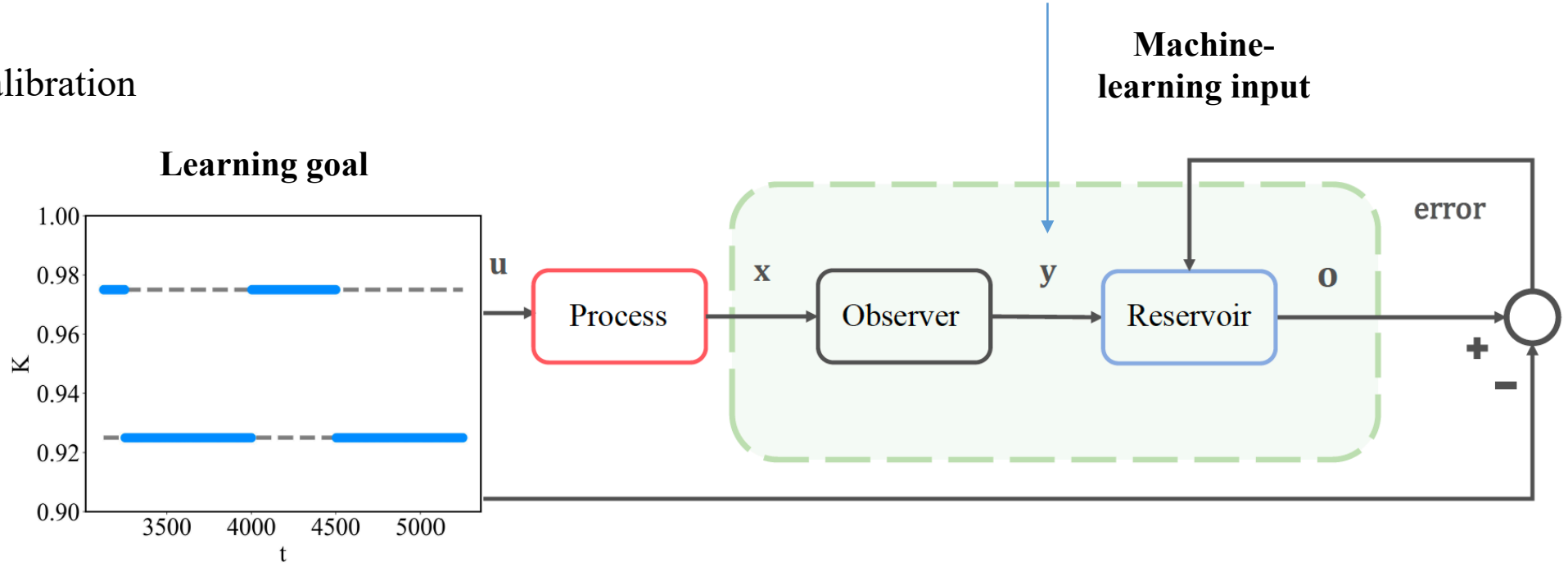
Assumption:
Observations from a small number of distinct parameter values can be collected in a well-controlled, laboratory environment



Parameter value K_1

Parameter value K_2

Training
- Laboratory calibration



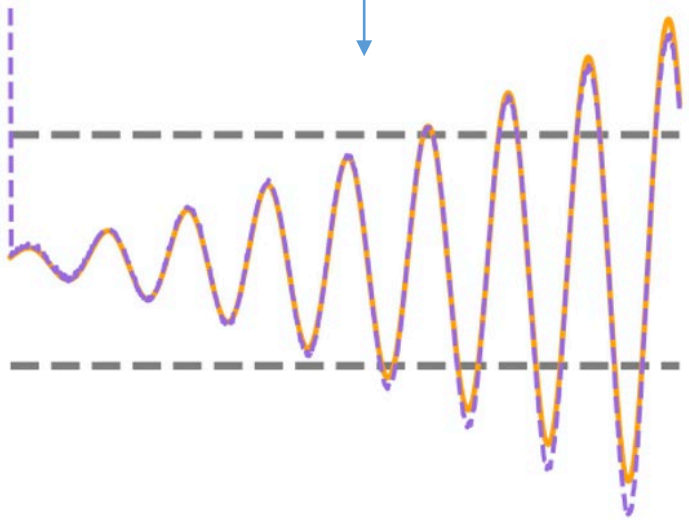
Machine-Learning Strategy: Testing or Deployment

During testing or deployment:

- Parameters are no longer accessible
- Their variations are unknown
- Partial state observations are available – machine-learning inputs

Machine-learning output: **Time variations of the parameter**

Reservoir computing

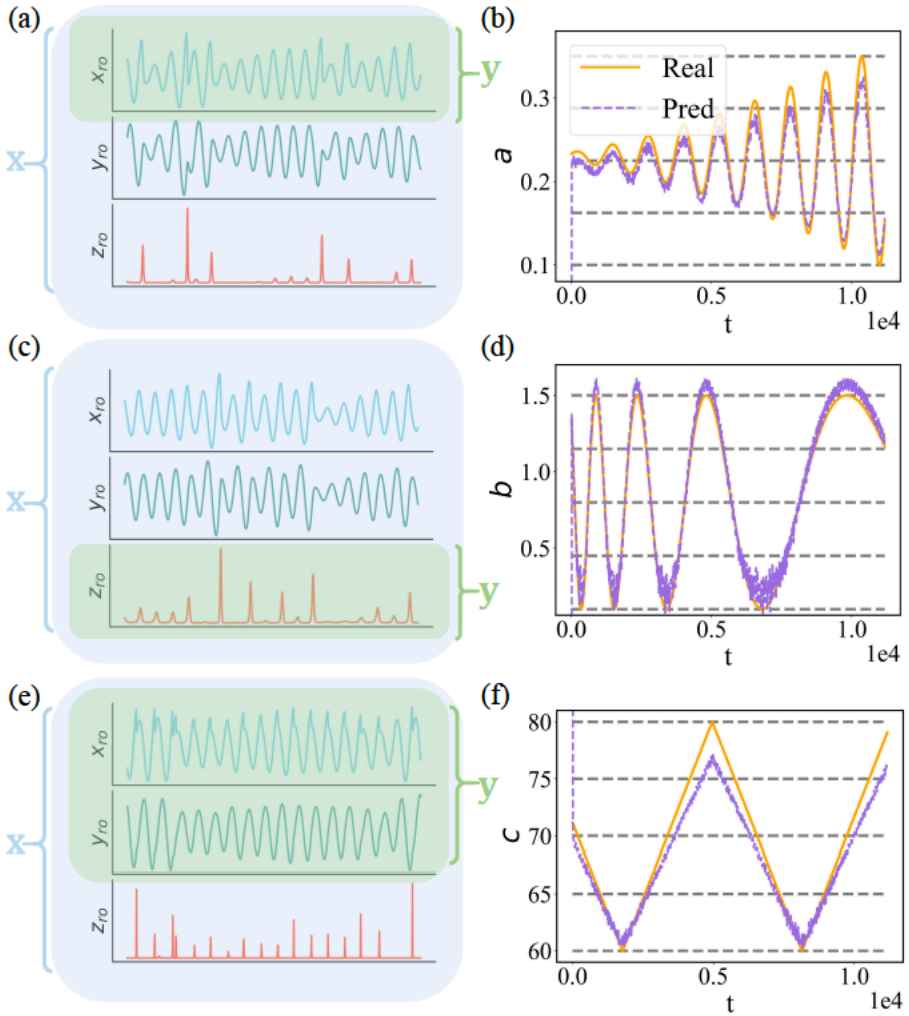


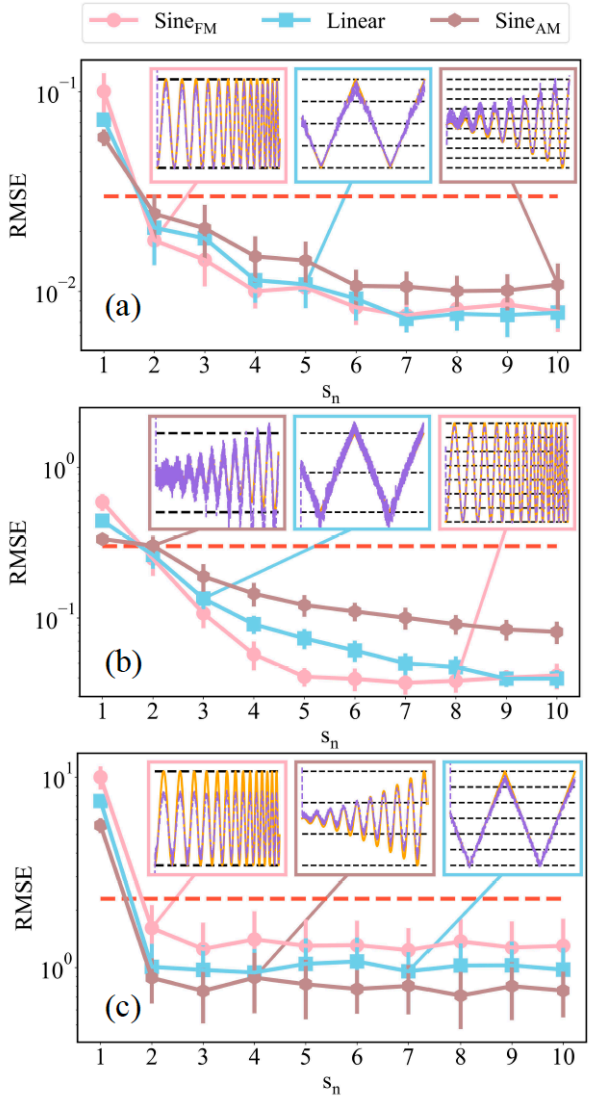
Machine-learning input

Machine-learning scheme: Adaptable Reservoir Computing – Why?

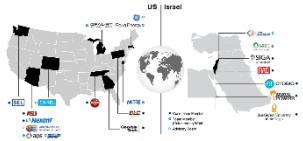
Parameter-Tracking Results: Chaotic Rossler Oscillator

$$\frac{dx_{ro}}{dt} = -y_{ro} - z_{ro}$$
$$\frac{dy_{ro}}{dt} = x_{ro} + a y_{ro}$$
$$\frac{dz_{ro}}{dt} = b + z_{ro}(x_{ro} - c)$$





Industrial Partner and Commercialization



The ASU Task 11 team is working with John Dirkman's team at *Resource Innovations Nexant* to incorporate the principle and methodologies of digital twins for AI-based intrusion detection into the existing industrial software tools.

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, Nexant Inc., 6620 Southpoint Drive South, Jacksonville, FL 32216-8098*

[3] *Department of Physics, Arizona State University, Tempe, Arizona 85287, USA*

(Dated: March 2, 2023)

The integration of computing and communication capabilities into the power grid has led to vulnerabilities enabling attackers to launch cyberattacks on the grid. Resources that can be deployed to protect a power grid are limited, rendering the need to impose preferences and priorities in optimal resource allocation. Due to the complexity of modern power grids, exploiting machine learning is desired for developing optimal preferential cybersecurity defense strategies, where choosing a suitable mathematical framework to describe the preference satisfaction and articulating a specific machine-learning method are key. We develop a reinforcement learning approach with the objective of satisfying the preferences as quantitatively described by linear temporal logic. To characterize the preferences, we exploit a probabilistic planning approach that transforms preference satisfaction into a mixed integer programming (MIP) problem, incorporate MIP into the resource allocation problem, and use reinforcement learning to obtain the optimal policy. Due to the time-varying nature of the problem, the transformation needs to be carried out and MIP is to be solved at each time step. Utilizing the benchmark W&W-6 Bus power grid network, we validate our preferential machine-learning framework to defend the system against attacks under limited resources. Although our framework is computationally intensive at the present, it provides a steppingstone toward developing more efficient machine-learning frameworks to preferentially defend large cyberphysical systems.

John's commitment on 3/1/2023:
"Regarding the manuscript on preferential cyber defense of power grids (Task 11) - as I review the manuscript I will consider the potential for commercialization."

Had a commercialization meeting with John on March 10.