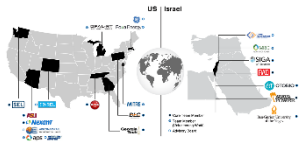
Task 11: AI Based Intrusion Detection

Ying-Cheng Lai

Arizona State University

1/24/2022

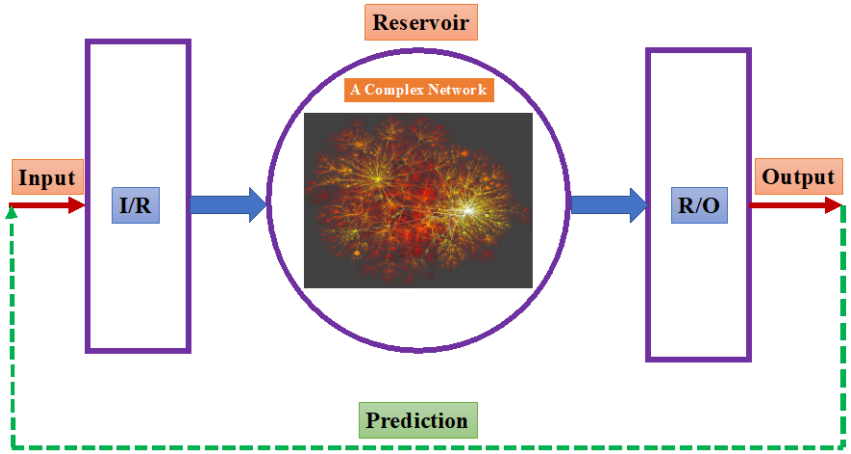
Task Overview



- **Main Objective**: to develop a network nonlinear dynamics and machine-learning based framework to detect external perturbations that can potentially cause catastrophic damages to a distributed electrical power network.
- **Cascading Failures**: catastrophic for power networks with heterogeneous energy sources.
- **Research Focus**: identifying the type of perturbations or intrusion that will result in cascading failures and developing real-time detection schemes based on digital twins.
- **Digital Twin for Electrical Power Systems**: recurrent neural-network based machine-learning architecture as required by the intrinsic nonlinear dynamics of the power systems.
- **Training Data**: from real-world power systems - possibly through enterprise Operational Technology (OT) management tools and Industrial Control System (ICS) tools.
- **Anticipated Outcome**: enabling a systematic identification of all types of possible attack (intrusion) scenarios that can potentially lead to cascading failures, resulting in a “library” of such intrusion types.

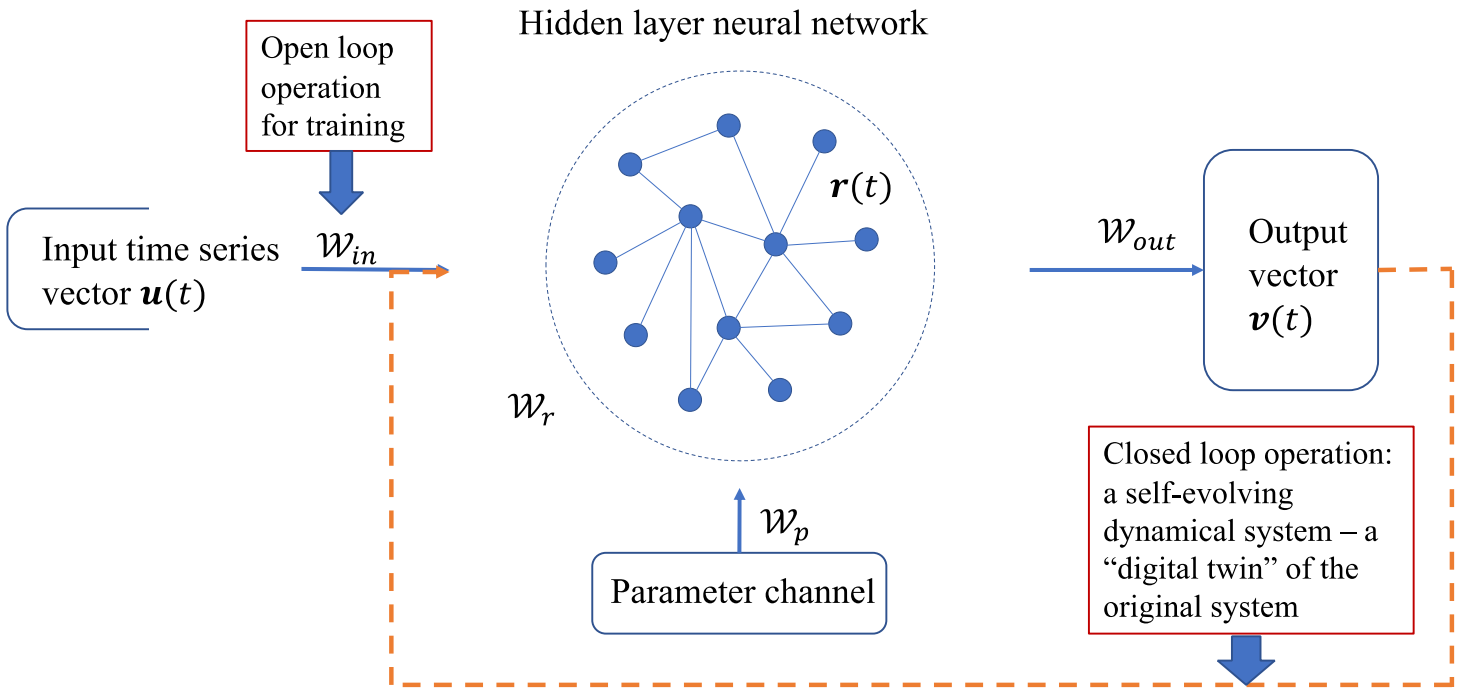
Technical Content (1)

Reservoir computing: general architecture



- H. Jaeger and H. Haas, Harnessing nonlinearity: Predicting chaotic systems and saving energy in wireless communication, *Science* **304**, 78 (2004);
- J. Pathak, B. Hunt, M. Girvan, Z. Lu, and E. Ott, Model-Free Prediction of Large Spatiotemporally Chaotic Systems from Data: A Reservoir Computing Approach, *Phys. Rev. Lett.* **120**, 024102 (2018);
- J. Jiang and Y.-C. Lai, Model-free prediction of spatiotemporal dynamical systems with recurrent neural networks: Role of network spectral radius, *Phys. Rev. Research* **1**, 033056 (2019).

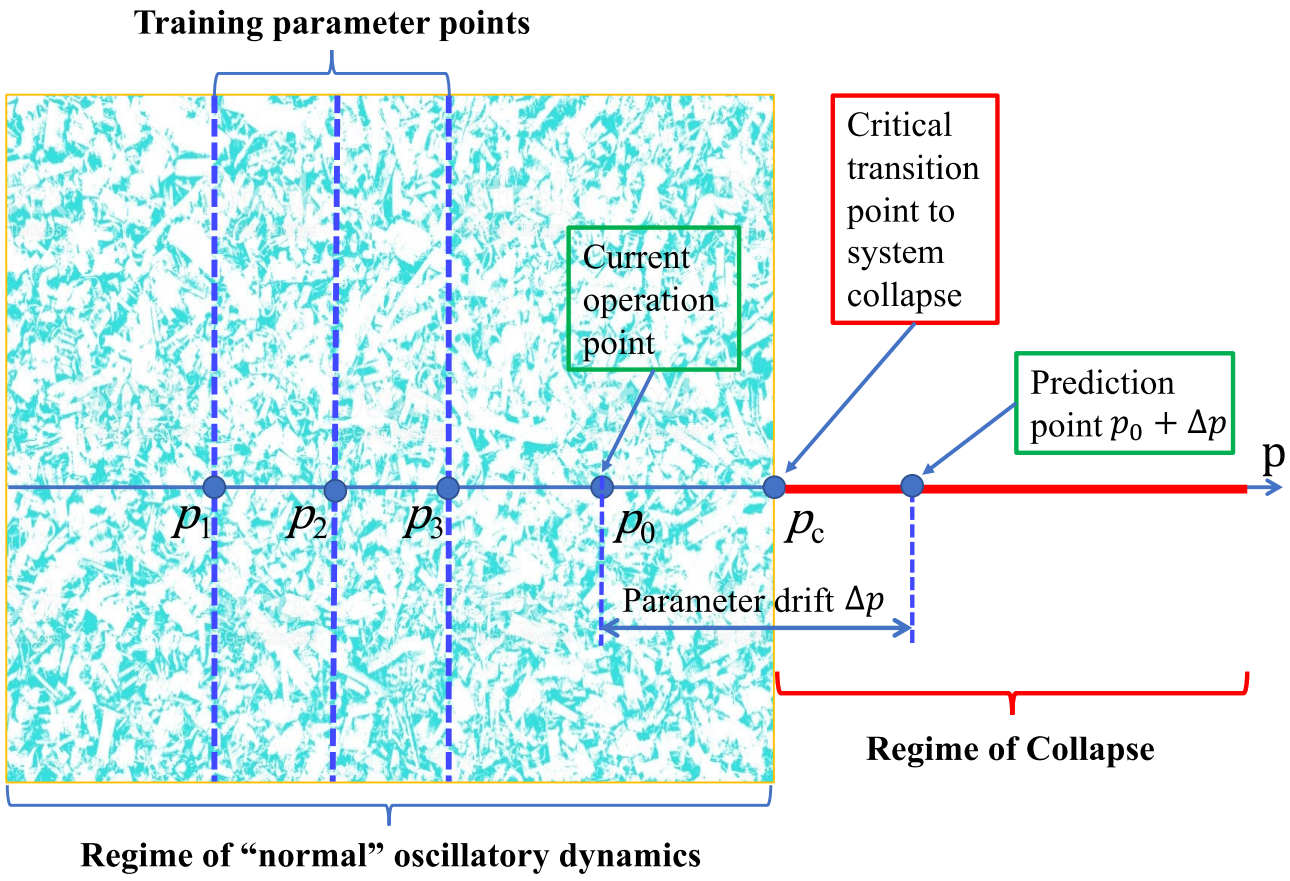
ASU Design: Creation of recurrent neural-network based digital twin



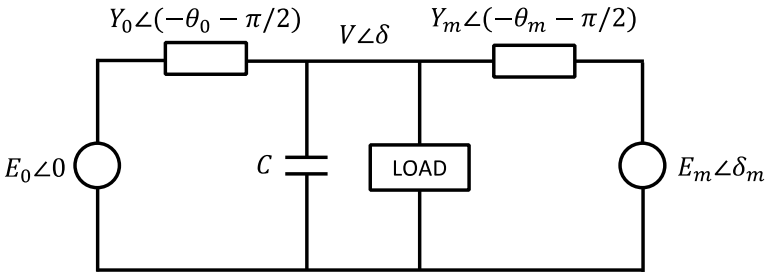
L.-W. Kong, H.-W. Fan, C. Grebogi, and Y.-C. Lai, "Machine learning prediction of critical transition and system collapse," *Physical Review Research* **3**, 013090, 1-14 (2021)

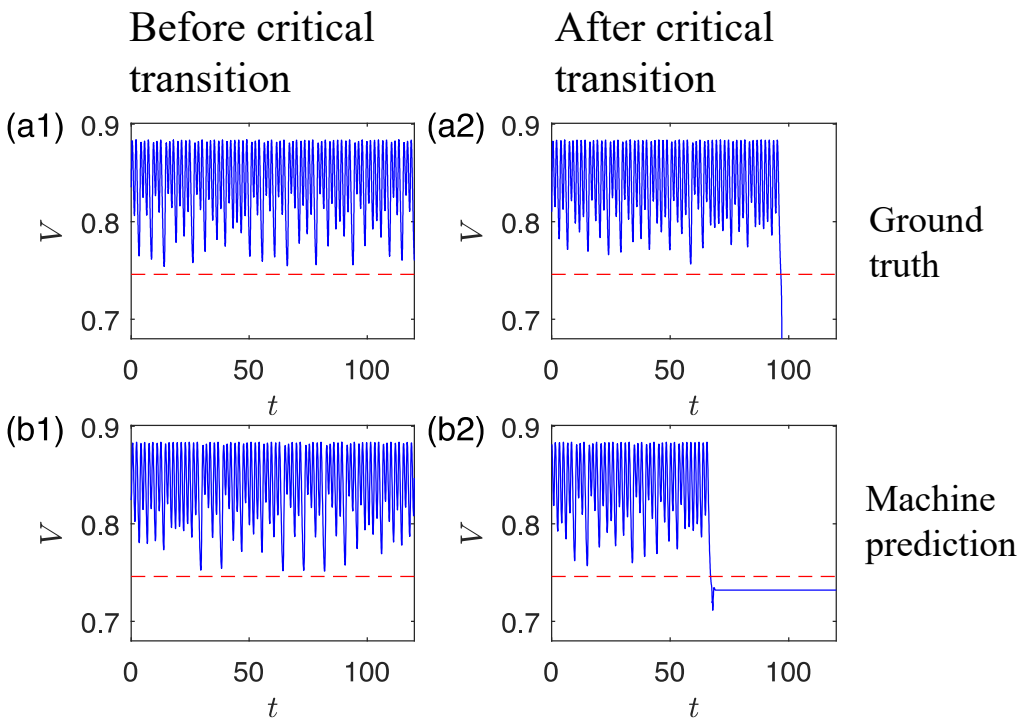
Technical Content (2)

Parameter-dependent training of digital twin

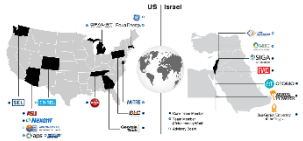


An example





Team Members and How They Interact



Team for Task 11

- Ling-Wei Kong (main), PhD candidate in ASU Electrical Engineering with experience in reservoir computing, nonlinear dynamics, and complex systems (In ASU EE for three years; eight refereed-journal papers)
- Amin Moradi (secondary), new PhD student in ASU Electrical Engineering with experience in reinforcement learning (one refereed-journal paper)
- Ying-Cheng Lai (Task lead), ASU Electrical Engineering
- Yang Weng (Consortium lead-PI), ASU Electrical Engineering
- John Dirkman, VP of Product Management and Resource Innovations of Nexant

Main student researcher

Ling-Wei Kong

FOLLOW

Arizona State University

Verified email at asu.edu - Homepage

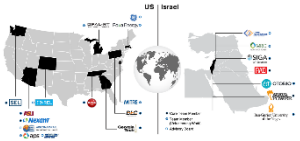
Nonlinear Dynamics Complex Networks Statistical Physics

TITLE	CITED BY	YEAR
Machine learning prediction of critical transition and system collapse LW Kong, HW Fan, C Grebogi, YC Lai Physical Review Research 3 (1), 013090	18	2021

Team interaction/collaboration

- Lai will work with the two PhD students on basic principles of digital twins and AI based intrusion detection for electrical power systems, in collaboration with Weng.
- The Task 11 team will work with Dirkman to develop software of recurrent neural-network based intrusion detection paradigm

Commercialization Plan



Past encounter with commercialization (Lai):

- In August 2020, the Air Force/MIT Artificial Intelligence Accelerator launched a public challenge to help create the artificial intelligence needed to solve the magnetic navigation problem.
- The specific call was for the signal enhancement for magnetic navigation (MagNav) challenge problem with the goal to use magnetometer readings recorded from within a cockpit and remove the aircraft magnetic noise to yield a clean magnetic signal.
- The ASU team led by Lai responded and tested three types of machine learning methods: multilayer perceptrons (MLPs), reservoir computing, and long short-term memory (LSTM) neural networks.
- In December 2020, the Air Force/MIT Artificial Intelligence Accelerator placed the ASU team as the winning team.
- The involved Air Force officers suggested to Lai to commercialize the machine-learning technique.

The ASU Task 11 team will work with Nexant to incorporate the principle and methodologies of digital twins for AI-based intrusion detection into the existing industrial Operational Technology and Industrial Control Systems management software tools.