AI for Cybersecurity in Photovoltaic Systems

Presenter: Qinghua Li
Associate Professor and the 21st Century Research Leadership Chair
Dept. of Electrical Engineering and Computer Science
University of Arkansas

Project: Multilevel Cybersecurity for Photovoltaic Systems (DE-EE0009026)
Principal Investigator: H. Alan Mantooth, University of Arkansas, mantooth@uark.edu
Subawardees: NREL, UGA, UIC, TAMUK, TPI, Ozarks Electric, GE Research, ANL
Project Overview

- **Inverter-level security**
  - Digital twin and hot patching
  - Vulnerability mitigation
  - Attack detection
  - Supply chain security

- **System-level security**
  - Model- and ML-based attack detection
  - Blockchain-based security
AI in the Project

Data-driven Cyberattack Detection

- A comprehensive comparison of data-driven cyber-attack detection methods

Neural Network
- Artificial Neural Network (ANN)
- Convolution Neural Network (CNN)
- Long Short-Term Memory (LSTM)

Input Data
- Type 1: Waveform
- Type 2: μPMU
- Type 3: figure of merit, such as μPMU, THD, unbalanced degree

AI in the Project

Data-driven Cyberattack Detection

- A comprehensive comparison of data-driven cyber-attack detection methods

Conclusion:
- Well-designed Figures of Merit outperform the Waveform and PMU data in terms of efficiency and accuracy.
- CNN shows superior performance surpassing ANN and LSTM.
- This method cannot detect novel attacks that are not included in the training set.

Data-driven cyber-attack detection using physics-guided time-frequency features

Data-driven Cyberattack Detection

- Data-driven cyber-attack detection using physics-guided time-frequency features

Innovative Features to Address New Attacks

Testing Results when New Attacks occur

AI in the Project
Data-driven Cyberattack Detection

● A transfer learning technique for cyber-attack detection in PV farms

- Research problem - how to reduce the data needs and time of training machine learning models for a new solar farm?
- Two solar farm attack models are built to generate the dataset
  - Solar farm #1: 400 kVA in a small-scale power grid.
  - Solar farm #2: 910 kVA connected to the IEEE 37-node distributed grid.
- Transfer learning is used

AI in the Project

Data-driven Cyberattack Detection

A transfer learning technique for cyber-attack detection in PV farms

Performance comparison between transferred model and the newly trained model

<table>
<thead>
<tr>
<th>Training samples</th>
<th>F1 (transferred model)</th>
<th>F1 (newly trained model)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10%</td>
<td>0.757</td>
<td>0.673</td>
</tr>
<tr>
<td>20%</td>
<td>0.805</td>
<td>0.698</td>
</tr>
<tr>
<td>40%</td>
<td>0.912</td>
<td>0.822</td>
</tr>
<tr>
<td>60%</td>
<td>0.952</td>
<td>0.894</td>
</tr>
<tr>
<td>80%</td>
<td>0.979</td>
<td>0.982</td>
</tr>
<tr>
<td>100%</td>
<td>0.978</td>
<td>0.989</td>
</tr>
</tbody>
</table>

Transferred model achieves 95.2% accuracy (F1 score) using 60% training dataset.

- Transfer learning requires much lower amount of dataset and training time compared with newly-trained model.

**AI in the Project**

**Firmware Malware Detection for Smart Inverters**

- The DTL method takes a pre-trained model from a type of image dataset, freeze a portion of the layers, and then fine-tune the last few layers on the newly obtained dataset.

![A commercial smart inverter architecture](image)

AI in the Project
Firmware Malware Detection for Smart Inverters

- The basis DL model experiment
  - 100 benign files and 100 malware

- The proposed DTL model experiment
  - IoT device (Raspberry Pi 4B)
  - 1 benign file and 5 malware

Experiment setup on an emulated smart inverter security testbed

Training and validation accuracy of the DTL model

What We Learned

• ML is a promising technique in PV system cybersecurity
• No ML model works for all
• Lack of data – transfer learning might help
  • Transfer across domains
  • Transfer within PV systems
• Physics-informed feature selection could be leveraged
• Cyber attacks and physical faults should be considered together
Acknowledgment

• This material is based upon work supported by the Department of Energy under Award No. DE-EE0009026.

• Some content in the slides is shared from Drs. Alan Mantooth, Jin Ye, Taesic Kim, and Chris Farnell.