Overview

1. Introduction
2. Cybersecurity challenges and opportunities
3. AI for Cybersecurity
4. Ongoing AI Research at NREL
5. Cyber Range for AI Research
6. Challenges Leveraging AI for Cybersecurity
17 U.S. Department of Energy National Laboratories

“Government owned, contractor operated”
NREL at-a-Glance

Workforce, including
- 219 postdoctoral researchers
- 60 graduate students
- 81 undergraduate students

World-class
facilities, renowned technology experts

More than
900

Partnerships
with industry, academia, and government

Campus
operates as a living laboratory
NREL Science Drives Innovation

Renewable Power
- Solar
- Wind
- Water
- Geothermal

Sustainable Transportation
- Bioenergy
- Vehicle Technologies
- Hydrogen

Energy Efficiency
- Buildings
- Advanced Manufacturing
- Government Energy Management

Energy Systems Integration
- Grid Integration
- Hybrid Systems
- Energy Security and Resilience
Cybersecurity Challenges and AI Research Opportunities
Future Grid Challenges

Features of future grid
- Distributed Authority
- Interconnected Communications
- Hierarchal and Coordinated Operation
- Autonomous Operation
- Scale of number of devices
- Diversity of vendors and devices

Cybersecurity challenges
- Distributed attack surface
- Many attacker pivot options
- Cascading impacts and failures
- Trust in autonomous decisions
- Larger attack surface
- Supply chain risks
AI Research Opportunities

• **Distributed Attack Surface:**
  • AI for threat correlation across entities and geographies

• **Multiple Attack Entry Points:**
  • Hybrid Intrusion Detection for Energy System

• **Scale of number of devices:**
  • AI for attack anticipation using large datasets
AI Research Opportunities

- **Cascading Impacts and Failures:**
  - Physics informed machine learning for attack detection at control layer

- **Supply Chain:**
  - AI for characterizing device behavior and trust scores

- **Autonomous Decision Making:**
  - Online real-time learning in adversarial environments
AI for Cybersecurity
Hybrid Intrusion Detection for Energy System

Known attack signatures from cyber logs

- **Signature-based IDS**

- **Model-based IDS**

  Rules based on spatiotemporal behavior of power system

**Learning-based IDS**

Classification of cyber-physical anomalies
Hybrid Intrusion Detection for Energy System

Attack Vectors

IT based attacks
• Network scanning
• Denial of Service
• IP spoofing

OT based attacks
• Malicious tripping (MITM)
• Pulse attack
• Ramp attack

<table>
<thead>
<tr>
<th>IDSs</th>
<th>IT Attacks</th>
<th>OT Attacks</th>
<th>Line Faults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network-based IDS</td>
<td>100%</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Model-based IDS</td>
<td>×</td>
<td>98.624%</td>
<td>×</td>
</tr>
<tr>
<td>Hybrid IDS (Network+Model+Learning)</td>
<td>100%</td>
<td>98.624%</td>
<td>97.9%</td>
</tr>
</tbody>
</table>

DDoS Attack Detection on SDN

• Well-tuned gradient-boosted decision tree for automated detection of DoS and DDoS attacks
• Optimal machine learning classifiers with general protocol case algorithm accuracy > 97%

Table 5: RF vs. XGB Performance Comparison.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Accuracy</th>
<th>Precision</th>
<th>Recall</th>
<th>ROC AUC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random Forest</td>
<td>97.15 ± 0.04</td>
<td>95.57 ± 0.07</td>
<td>97.17 ± 0.08</td>
<td>0.99</td>
</tr>
<tr>
<td>XGBoost</td>
<td>97.66</td>
<td>95.33</td>
<td>98.81</td>
<td>0.99</td>
</tr>
</tbody>
</table>

Ongoing AI Research at NREL
Autoencoders provide two means of anomaly detection: latent space distance measurement and reconstruction errors.

NREL has experience using autoencoders to detect physical system anomalies, for example in wind plant flow physics.
Deep reinforcement learning (DRL) solves a critical load restoration (CLR) problem in distribution system following major outages or attacks.

DRL controller restores load despite uncertainty in generation ability, network or user actions.

DRL controller is less susceptible to generation forecast errors than model predictive control (MPC).
Adversarial Training

- Generative Adversarial Networks (GANS) train two competing neural networks: **generator** and **discriminator**
- Discriminator identifies fake/anomalous samples and generator produces new samples (fallback action/synthetic data)
- Adversarial attacks can use similar gradient information to identify weaknesses in NN’s

Super Resolution

GANS

Stengel, Glaws, Hettinger, and King, Proc. of the Natl Acad. Sciences, 2020

Conditional GANS

Hassanaly et al, under review in JCP, 2021.
Cyber Range for AI Research
NREL’s **Cyber Range** is a broadly capable hybrid private cloud solution for research involving operation and security for both telecommunication networks and physical systems.

With hardware-, controller-, and human-in-the-loop integration, NREL’s Cyber Range offers a realistic, interactive dynamic environment and provides visualizations of the **digital and physical systems for real-time awareness, historical analysis, and future planning and operation.**
Distribution Utility Emulation Environment

Distribution Utility
Electrical Nodes: 375K
No. of Customers: 134K
No. of Dist. Xmers: 11K

AMI Aggregator
AMI Environment
DER Comms Engine
GIS Visualization
OT Environment
Control Center
Utility WAN VM
Substations and Field Devices

Cyber Energy Emulation Platform
ARIES Research Platform – At-Scale
Challenges Leveraging AI
Challenges Leveraging AI

- Imbalanced data
- Data pollution
- Data bias
- Edge data important for resilience
- Realtime streaming of data and updated learning
  - How fast can updates be observed
  - What are the resource requirements
- Defining precise terminologies for technology adoption