Cybersecurity for DER Networks: Situational Awareness and Attack Surface Reduction

Manimaran Govindarasu
Dept. of Electrical and Computer Engineering
Iowa State University

Collaborators:
Moataz Abdelkhalek
Gelli Ravikumar
Iowa State University
Outline of the Talk

- DER Cyber Attack Surface

- Cybersecurity Situational Awareness
  - ML-based Anomaly Detection
  - ML-based Alert Correlation
  - Real-time Visualization

- Attack Surface Reduction using MTD

- Conclusions
**Distributed Energy Resources (DER)**

- **DER**: Solar PVs, wind farms, energy storage, electric vehicles (EVs)
- DER deployment is continuously growing …
- Forms microgrids and integration into distribution grid
- **Real-time morning and control** with latency constraints
- Decentralized monitoring and control architecture
- Distributed communication architecture
- **IoT**: Utilizes public networks & cloud infrastructures
- Edge devices/controllers have limited capabilities
- Large attack surface and is growing …
DER Cybersecurity Threats

Real Cyber incidents on Industrial Control Systems (ICS)

- **Stuxnet**: The world’s first publicly known digital weapon causing cyber-physical damage.
  - **2010**

- **Duqu**: Advanced and complex malware used to target specific organizations, including ICS manufacturers.
  - **2011**

- **Havex**: An ICS-focused malware campaign.
  - **2013**

- **Shamoon**: Malware used to target large energy companies in the Middle East, including Saudi Aramco and RasGas.
  - **2012**

- **Black Energy**: Malware that targeted human-machine interfaces (HMIs) in ICSs.
  - **2014**

- **Ukraine Power Grid Attack No. 1**: The first known successful cyber-attack on a country’s power grid.
  - **2015**

- **Ukraine Power Grid Attack No. 2**: Cyber-attackers tripped breakers in 30 substations, turning off electricity to 225,000 customers in a second attack.
  - **2016**

- **LockerGoga**: Attack halted global aluminum manufacture Norsk Hydro.
  - **2017**

- **Triton / Trisis**: Malware specifically designed to target Schneider Electric safety systems - hits mostly in the Middle East.
  - **2018**

- **OLDSMAR Water Hack**: Remote attackers contaminated sodium hydroxide levels in drinking water.
  - **2020**

- **Colonial Pipeline Attack**: Fuel distributor attacked by ransomware causing several days of shutdown and market disruption.
  - **2021**

- **JBS Foods Attack**: Ransomware attack shut down world’s largest meat supplier.
  - **2021**

- **TSMC**: Chipmaker TSMC hit with computer virus and forced to shut down several of its factories.
  - **2016**
DER Networks Attack Surface

Cyber Situational Awareness & Control (Cloud)
- IADS Master
  - Correlation Engine
  - Real-Time Situational Awareness

Distribution Grid Control Center
- DER/Microgrid Control Applications
  - DMS
  - OMS
  - GIS
  - CIS

Utility WAN or Internet
- Management & Control Layer Security
- Communication Layer Attacks
- DER Stealthy Attacks
- Communication Layer Attacks
- Physical Layer Attacks

Tier-1
- EID
- Control Signals
- Modbus/
  - DNP3/
  - IEEE 2030.5

Tier-2
- EID
- Configurations
- Alerts
- Control
- Measurements

IADS Sensor
- DMS / DRAS
- Utility Aggregator
- 3rd Party Aggregator / DRAS

DER Client
- DER Client
- Loads
- Modbus/
  - DNP3/
  - IEEE 2030.5
Modbus DER Communication Protocol

- One of the most common automation communication protocols for DER devices.
  - Serial, over Ethernet, over TCP/IP
- Client/Server Communication model.
- Server initiate queries, Clients send responses of requested data or apply action.
- Susceptible to various IT-OT attacks -- originally clear text protocol
- No mutual authentication and Access Controls

Most used Open-source communications protocol in SCADA and DER systems in the US.
  - Serial, over Ethernet, over TCP/IP
- Control larger, more complex processes
- Detect and correct problems quickly
- Eliminate bottlenecks and inefficiencies
- Susceptible to various IT-OT attacks -- originally clear text protocol
- No mutual authentication and Access Controls
### DER Communication Protocols - Cybersecurity Features

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices Support</td>
<td>DER, Power Systems Devices</td>
<td>DER, Smart Grid devices</td>
<td>Utility, Grid Devices</td>
<td>Utility, Grid, ICS devices</td>
</tr>
<tr>
<td>Encryption Capability</td>
<td>Non-Native</td>
<td>Yes</td>
<td>BITW</td>
<td>BITW</td>
</tr>
<tr>
<td>Encryption Required</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Supported Transport Protocols</td>
<td>N/A</td>
<td>TCP or UDP</td>
<td>Serial or TCP</td>
<td>Serial or TCP</td>
</tr>
<tr>
<td>Supported Networks</td>
<td>N/A</td>
<td>IPv4, IPv6</td>
<td>IPv4</td>
<td>IPv4, IPv6</td>
</tr>
<tr>
<td>Authentication Support</td>
<td>Non-Native</td>
<td>Yes</td>
<td>Optional</td>
<td>Non-Native</td>
</tr>
<tr>
<td>Type of Communication Protocol</td>
<td>IEC 61850-90-7 contains functions for power converter-based DER systems</td>
<td>Communication protocol for device integration with the Smart Grid</td>
<td>Communication protocol for real-time monitoring and control</td>
<td>Communication protocol for real-time monitoring and control</td>
</tr>
<tr>
<td>Type of Information Model</td>
<td>IEC 61850-90-7</td>
<td>CSIP</td>
<td>DNP3 Application Note</td>
<td>SunSpec and MESA are information models for Modbus</td>
</tr>
<tr>
<td>Type of Security Requirements</td>
<td>IEC 62351 Series</td>
<td>IEEE 2030.5 + CSIP</td>
<td>IEEE 1815</td>
<td>There are no security requirements for Modbus communications</td>
</tr>
<tr>
<td>Type of Data Transmitted</td>
<td>DER settings, control modes, and measurements</td>
<td>DER measurement and control data</td>
<td>Data objects with defined attributes and priority levels</td>
<td>DER measurement and control data</td>
</tr>
<tr>
<td>Aggregation Support</td>
<td>Utility or aggregators can collect data</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

A Cybersecurity Lifecycle Model

**CPS Security for the Power Grid**

- **Enabling Technologies**
  - Synchrophasors
  - Cloud Computing
  - Software Defined Networking

- **Testbeds**
  - Datasets & models
  - Federation, Open access

- **Science of Security**
  - Game theory
  - Moving Target Defense
  - Stochastic Optimization
  - Control theory
  - Machine Learning

- **Detection**

- **Attribution**
  - Forensic tools and techniques

- **Resilience**
  - Cyber-Physical Attack resilience
  - Dynamic, System Reconfiguration

- **Mitigation**
  - CPS Model-based Approaches

- **Prevention**
  - Risk Assessment & Mitigation
    - Attack Surface Reduction, MTD: Moving Target Defense

- **Deterrence**
  - Offensive capabilities

**Intrusion & Anomaly Detection**

1. **Develop Real-Time Cybersecurity Situational Awareness Architecture and Algorithms for DER Networks**
   
   - ML-based anomaly detection models (ML-ADS) tailored for DER communication networks, with a focus on Modbus and DNP3 protocols.
   
   - The models should accurately identify intrusions and anomalies from normal events.
   
   - The models should be able to detect both known and unknown attacks with high detection accuracy while satisfying real-time latency constraints.

2. **Develop Attack Surface Reduction Techniques for DER networks**

   - Network-based solution complementing end-system solutions
   
   - Effectiveness and feasibility for real-time implementation
Our Research Framework – An IoT-based Architecture for DER Cybersecurity
Proposed ML-based Anomaly Detection for DER

- Data Acquisition and Analysis
- DER DNP3 (Normal/Attack) Traffic Augmentation
- Attack Categorization
- Dataset Balancing
- Trained Model Exportation/Storage
- ML Classification Model (Training/Testing)
- Data Preparation
- Data Formatting
- Data Normalization
- Feature Extraction and Selection
- Model Evaluation and Selection

Models:
- Gaussian Naive Bayes (NB)
- Logistic Regression (LR)
- Decision Trees (DT)
- Gradient Boosting (GB)
- Random Forests (RF)
- Artificial Neural Network (ANN)
- Support Vector Machines (SVM)
## Data Acquisition -- Datasets for ML models

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
<th>Realistic Normal/Attack Traffic</th>
<th>Labeled Data</th>
<th>Attack Types</th>
<th>CPS Traffic</th>
<th>Full Packet Capture</th>
</tr>
</thead>
<tbody>
<tr>
<td>KDD CUP 99</td>
<td>1999</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>DARPA’2000</td>
<td>2000</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>NSL - KDD</td>
<td>2009</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>ISCKIDS2012</td>
<td>2012</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>CIC-IDS2017</td>
<td>2017</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>CSE-CIC-IDS2018</td>
<td>2018</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Bot-IoT</td>
<td>2018</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>WUSTLIOT2018</td>
<td>2018</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Electra</td>
<td>2019</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>IoT-23</td>
<td>2020</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Source: CSE–CIC–IDS2018 Dataset
Data Augmentation

- No DER specific Datasets available
- Inaccurate training will result in high false-positive and false-negative rates.
- **Generated realistic DER traffic and Attack using ISU CPS–DER Security Testbed**
  - various DER stealthy attacks such as port scanning,
  - DoS attacks, Modbus stealthy injection attacks,
  - DNP3 stealthy injection attacks, etc.
- Denial of Service attacks

\[ P_{depletion}(t) = 1 - (1 - P_B(t))(1 - P_M(t)) \]

- Sample Pseudo Modbus Data–integrity Attack
### Attack Categorization and Balancing

<table>
<thead>
<tr>
<th>Traffic Source</th>
<th>Attack Type</th>
<th>Attack Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Dataset</td>
<td>DDoS attack-LOIC-UDP</td>
<td>DOS</td>
</tr>
<tr>
<td>Original Dataset</td>
<td>DoS attacks-SlowHTTP</td>
<td>DOS</td>
</tr>
<tr>
<td>Original Dataset</td>
<td>DoS attacks-Slowloris</td>
<td>DOS</td>
</tr>
<tr>
<td>Original Dataset</td>
<td>DoS attacks-Hulk</td>
<td>DOS</td>
</tr>
<tr>
<td>Original Dataset</td>
<td>DoS attacks-GoldenEye</td>
<td>DOS</td>
</tr>
<tr>
<td>Original Dataset</td>
<td>DDoS attack-HOIC</td>
<td>DOS</td>
</tr>
<tr>
<td>Original Dataset</td>
<td>DDoS attacks-LOIC-HTTP</td>
<td>DOS</td>
</tr>
<tr>
<td>Original Dataset</td>
<td>SSH-Bruteforce</td>
<td>RA</td>
</tr>
<tr>
<td>Original Dataset</td>
<td>FTP-Bruteforce</td>
<td>RA</td>
</tr>
<tr>
<td>Original Dataset</td>
<td>Brute Force-Web</td>
<td>RA</td>
</tr>
<tr>
<td>Original Dataset</td>
<td>Brute Force-XSS</td>
<td>RA</td>
</tr>
<tr>
<td>Original Dataset</td>
<td>SQL Injection</td>
<td>RT</td>
</tr>
<tr>
<td>Original Dataset</td>
<td>Infiltration</td>
<td>Scanning</td>
</tr>
<tr>
<td>Original Dataset</td>
<td>Bot</td>
<td>RA</td>
</tr>
<tr>
<td>Augmented DER Traffic</td>
<td>DER Reconnaissance</td>
<td>Scanning</td>
</tr>
<tr>
<td>Augmented DER Traffic</td>
<td>DER Bruteforce</td>
<td>RA</td>
</tr>
<tr>
<td>Augmented DER Traffic</td>
<td>DER Traffic Flooding</td>
<td>DOS</td>
</tr>
<tr>
<td>Augmented DER Traffic</td>
<td>DER Remote Exploitation</td>
<td>RT</td>
</tr>
<tr>
<td>Augmented DER Traffic</td>
<td>DER Stealth Attacks</td>
<td>DER Stealth</td>
</tr>
</tbody>
</table>

### Diagram

The diagram illustrates the comparison between the number of attack flows in the Original IDS Dataset and the Augmented DER Traffic (Normal/Attacks). The bars show a significant increase in the number of attacks, particularly in the DoS category. The legend indicates the types of attacks and categories, with colors distinguishing between the Original IDS Dataset and Augmented DER Traffic.
Feature Extraction and Selection - Modbus

- Statistical Feature Extraction
  - 84 OT/IT based features
- Dimensionality Feature Reduction
  - Pearson’s and Chi-Squared correlation
  - 42 selected features

<table>
<thead>
<tr>
<th>IT Features</th>
<th>OT Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>FlowID</td>
<td>DER Flow Duration</td>
</tr>
<tr>
<td>Source IP</td>
<td>Length of DER Protocol Payload</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Number of DER Protocol Requests</td>
</tr>
<tr>
<td>Source Port</td>
<td>DER Protocol Payload Values Mean</td>
</tr>
<tr>
<td>Destination Port</td>
<td>DER Protocol Payload Values Standard Deviation</td>
</tr>
<tr>
<td>Protocol</td>
<td>Mean Total Flow Time</td>
</tr>
</tbody>
</table>
Performance Evaluation - ML-ADS Modbus

Divided Datasets into 70% Training and Validation, and 30% Testing (containing unknown attacks patterns)
Feature Extraction and Selection – DNP3

- Statistical Feature Extraction
  - 92 OT/IT based features

- Dimensionality Feature Reduction
  - Principal Component Analysis (PCA), Pearson’s and Chi-Squared correlation
  - 47 selected features

<table>
<thead>
<tr>
<th>IT Features</th>
<th>OT Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Bytes/s</td>
<td>DER Flow Duration</td>
</tr>
<tr>
<td>Src &amp; Dst IP</td>
<td>DER DNP3 Payload Length</td>
</tr>
<tr>
<td>Src &amp; Dst Port</td>
<td>DER DNP3 Requests/s</td>
</tr>
<tr>
<td>Traffic Set Flags</td>
<td>DER DNP3 Payload Values Mean &amp; Std Dev</td>
</tr>
<tr>
<td>Packet Length</td>
<td>DER DNP3 Payload Function Codes</td>
</tr>
<tr>
<td>Protocol</td>
<td>DER DNP3 IIN Flags</td>
</tr>
</tbody>
</table>
Performance Evaluation - ML-ADS DNP3

Divided Datasets into 70% Training and Validation, and 30% Testing (containing unknown attacks patterns)

<table>
<thead>
<tr>
<th>ML Algorithm</th>
<th>NB</th>
<th>DT</th>
<th>RF</th>
<th>SVM</th>
<th>LR</th>
<th>GB</th>
<th>ANN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training Accuracy</td>
<td>66.07</td>
<td>99.52</td>
<td>98.49</td>
<td>82.61</td>
<td>82.9</td>
<td>99.43</td>
<td>98.67</td>
</tr>
<tr>
<td>Testing Accuracy</td>
<td>66.48</td>
<td>99.24</td>
<td>98.03</td>
<td>83.27</td>
<td>83.39</td>
<td>99.15</td>
<td>98.43</td>
</tr>
<tr>
<td>Training Latency (μs)</td>
<td>4.91</td>
<td>26.13</td>
<td>220.36</td>
<td>687.6</td>
<td>251.87</td>
<td>2166.65</td>
<td>4107.54</td>
</tr>
<tr>
<td>Testing Latency (μs)</td>
<td>3.58</td>
<td>1.9</td>
<td>55.49</td>
<td>634.29</td>
<td>0.52</td>
<td>9.91</td>
<td>75.31</td>
</tr>
</tbody>
</table>
Our Research Framework – An IoT-based Architecture for DER Cybersecurity
One of the main drawbacks for distributed ADS systems is:
- Low-level representation of attacks.
- High false-positives
- Large number of alerts

Alert analysis is a challenging task

Alert Correlation:
- Transforms raw alerts into a more meaningful wider insight of the attack scenarios.
- Cyber situational Awareness into the DER incidents
- Reduce total volume of alerts
- Reduce false-positive alerts
Proposed Alert Correlation framework for DER Networks

Distributed Correlation Sensors

IADS Sensor Alerts

Alert Normalization → Alert Aggregation → Alert Confidence

Cloud Correlation Engine

Similarity-based scenario correlation → Statistical-based incident correlation → Severity calculation and recommendation strategies

Encrypted Channel

WAN

System Logs

DER Situational Security Dashboards

Correlated Intrusions

Adjustable Time-Window

Total Log Count Over Time
Alert Confidence (Verification)

<table>
<thead>
<tr>
<th>Alert Type</th>
<th>Time Stamp</th>
<th>Operator</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>IDS Alert</th>
<th>IDS Rule ID</th>
<th>Target Register Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>WARNING</td>
<td>Sep 16, 2020 14:56:03.503279000 Central Standard Time</td>
<td>Operator_1</td>
<td>192.168.1.100</td>
<td>192.168.1.103</td>
<td>Modbus write single coil</td>
<td>9000003</td>
<td>3 5</td>
</tr>
<tr>
<td>WARNING</td>
<td>Sep 16, 2020 14:59:12.582314100 Central Standard Time</td>
<td>Operator_1</td>
<td>192.168.1.100</td>
<td>192.168.1.103</td>
<td>Modbus read single coil</td>
<td>9000002</td>
<td>3 Null</td>
</tr>
<tr>
<td>Malicious</td>
<td>Sep 16, 2020 15:05:50.121131000 Central Standard Time</td>
<td>Null</td>
<td>192.168.1.100</td>
<td>192.168.1.103</td>
<td>Modbus write single coil</td>
<td>9000003</td>
<td>3 0</td>
</tr>
<tr>
<td>WARNING</td>
<td>Sep 16, 2020 15:11:45.392545000 Central Standard Time</td>
<td>Operator_1</td>
<td>192.168.1.100</td>
<td>192.168.1.103</td>
<td>Modbus read single coil</td>
<td>9000002</td>
<td>3 Null</td>
</tr>
</tbody>
</table>
Similarity-based Correlation

- Attack Thread Reconstruction and Attack Session Reconstruction

<table>
<thead>
<tr>
<th>Time</th>
<th>Source (Attacker)</th>
<th>Destination (EID)</th>
<th>ADS Alert Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/17/2020 00:45</td>
<td>10.0.0.100</td>
<td>10.0.0.2</td>
<td>A</td>
</tr>
<tr>
<td>06/17/2020 00:50</td>
<td>10.0.0.100</td>
<td>10.0.0.3</td>
<td>B</td>
</tr>
<tr>
<td>06/17/2020 00:55</td>
<td>10.0.0.100</td>
<td>10.0.0.4</td>
<td>C</td>
</tr>
<tr>
<td>06/17/2020 02:00</td>
<td>10.0.0.2</td>
<td>10.0.0.5</td>
<td>D</td>
</tr>
<tr>
<td>06/17/2020 02:05</td>
<td>10.0.0.3</td>
<td>10.0.0.5</td>
<td>D</td>
</tr>
<tr>
<td>06/17/2020 02:10</td>
<td>10.0.0.4</td>
<td>10.0.0.5</td>
<td>D</td>
</tr>
</tbody>
</table>
## ML Statistical-based Correlation Feature Extraction

<table>
<thead>
<tr>
<th>Classification Feature</th>
<th>Attack Session 1</th>
<th>Attack Session 2</th>
<th>Attack Session 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Type</td>
<td>Distributed Denial of Service Attack</td>
<td>Worm Attack</td>
<td>Remote Hacking Attack</td>
</tr>
<tr>
<td>Attack Technique Rate of Change</td>
<td>Low</td>
<td>Low / None</td>
<td>High</td>
</tr>
<tr>
<td>Source IP Rate of Change</td>
<td>High</td>
<td>Low / None</td>
<td>Low</td>
</tr>
<tr>
<td>Dest. IP Rate of Change</td>
<td>Low / None</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Dest. Port Rate of Change</td>
<td>Unknown</td>
<td>Low / None</td>
<td>Medium</td>
</tr>
<tr>
<td>Time Rate of Alerts</td>
<td>Very High</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>Type of Events</td>
<td>DoS</td>
<td>Scan Remote-Access</td>
<td>Reconnaissance Scan Remote-Access Privilege Level</td>
</tr>
</tbody>
</table>

Initially Correlated Alerts

- Historical intrusion alerts
- Alert correlation likelihood
- Feature Extraction
- Dynamic threshold

Incident Correlation
ML Statistical-based Alert Correlation - Correlation Trees

Mean of Protocols <= 0.005
- gini = 0.8
- samples = 8040
- value = [1629, 1596, 1631, 1582, 1602]
- class = Hacking

Time Rate <= 0.75
- gini = 0.75
- samples = 6411
- value = [0, 1596, 1631, 1582, 1602]
- class = Hacking

Number of Sensor IDs <= 0.001
- gini = 0.5
- samples = 3184
- value = [0, 0, 0, 1582, 1602]
- class = Malware

Number of Destination Ports <= 0.067
- gini = 0.5
- samples = 3227
- value = [0, 1596, 1631, 0, 0]
- class = Hacking

Number of Destination IPs <= 0.641
- gini = 0.07
- samples = 1656
- value = [0, 1596, 60, 0, 0]
- class = Ping Sweep
2-Tier Testbed Architecture for DER Situational Awareness
HIL 2-tire DER Testbed Implementation for cyber situational awareness
Real-Time Visualization
ML-ADS Real-Time Confusion Matrix for DER Modbus Communication

<table>
<thead>
<tr>
<th></th>
<th>Actual Attack (66.57%) (133805 flows)</th>
<th>Actual Benign (33.43%) (67179 flows)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Predicted Attack</strong></td>
<td>TP (131157 flows)</td>
<td>FP (566 flows) (0.28%)</td>
</tr>
<tr>
<td><strong>Predicted Benign</strong></td>
<td>FN (2648 flows) (1.32%)</td>
<td>TN (66613 flows)</td>
</tr>
<tr>
<td></td>
<td>Recall (98.02%)</td>
<td>F1-Score (98.79%)</td>
</tr>
</tbody>
</table>

Accuracy (98.40%)
Precision (99.57%)
ML-ADS Real-Time Confusion Matrix for DER DNP3 Communication

<table>
<thead>
<tr>
<th>Predicted Attack</th>
<th>Actual Attack (31.6%) (104911 flows)</th>
<th>Actual Benign (68.4%) (227053 flows)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predicted Benign</td>
<td>TP (104373 flows)</td>
<td>FP (17 flows) (FPR 0.008%)</td>
</tr>
<tr>
<td></td>
<td>FN (538 flows) (FNR 0.51%)</td>
<td>TN (227036 flows)</td>
</tr>
<tr>
<td>Recall</td>
<td>(99.83%)</td>
<td>F1-Score (99.83%)</td>
</tr>
<tr>
<td>Precision</td>
<td>(99.84%)</td>
<td></td>
</tr>
<tr>
<td>Accuracy</td>
<td>(99.83%)</td>
<td></td>
</tr>
</tbody>
</table>
Conclusions — Cybersecurity Situational Awareness

Conclusions:

- **2-tier IoT cybersecurity situational awareness architecture** – design and testbed-based implementation

- **ML-based anomaly detection** for DER communication protocols (Modbus, DNP3)

- **ML-based alert correlation algorithms**

- **Demonstrated the efficacy and feasibility of the proposed IoT architecture and algorithms** for cybersecurity situational awareness – high attack detection rate, feasible latency

Future work:

- **ML-based Anomaly detection and Aler Correlation for other DER protocols** (e.g., IEEE 2030.5, IEC 61850)

- **Attack mitigation and Resiliency algorithms for DER**
Outline of the Talk

• DER Cyber Attack Surface

• Cybersecurity Situational Awareness
  • ML-based Anomaly Detection
  • ML-based Alert Correlation

• Attack Surface Reduction using SDN-enabled MTD

• Conclusions
Our Research Framework – An IoT-based Architecture for DER Cybersecurity

- Tier-1: DNP3/Modbus/IEEE 2030.5 Clients
  - Solar PV Inverter/Aggregator
  - Wind Farm Controller/Aggregator
  - Microgrid Controller
  - Battery Storage Controller
  - DER Client

- Tier-2: Alerts
  - Distributed Correlation Sensors
    - IADS Sensor Alerts
    - Alert Normalization
    - Alert Aggregation
    - Alert Confidence
  - Cloud Correlation Engine
    - Similarity-based scenario correlation
    - Statistical-based incident correlation
    - Severity calculation and recommendation strategies
  - Cloud-based ADS
    - Alert Correlation Engine
    - IADS Master
    - DER Situational Security Dashboards
Moving Target Defense (MTD) – Attack Surface Reduction

• Introduce controlled “uncertainty” in system operation without any adverse effect → confuse the adversary

Examples:

• Randomize network addresses

• Randomize network paths

• Randomize measurements & application behavior
Software-defined Networking (SDN)

- **SDN** is a programmable networking mechanism that *decouples control plane from data plane*.
- SDN allow for dynamic DER communication programmability for more reliable, efficient, and scalable operation.
- **SDN can enable the implementation of MTD in the DER networks.**
- SDN–enabled MTD combines the advantages of both the dynamic programmability of SDN and the randomness of MTD for cyber attack prevention and mitigation in DER environment.
SDN-enabled MTD for DER

1. Develop a **proactive security defense** mechanism for DER network using **SDN-enabled MTD** technique.

2. Show the **practicality and efficiency** of the proposed system on a close to real-world Testbed implementation.

3. The proposed mechanism should be able to **proactively reduce the effect of DoS attacks** on the DER network communication while **maintaining normal real-time** operation.
Traditional DER Communication Architecture (WAN)
SDN-enabled DER Communication Architecture (SD-WAN)
Case Study: SD-WAN MTD for DER Network

MTD Path Switching using SDN:
- Choose **Randomly** between communication channels
- Automated Switching between 3 SDN routers.

**Defender Requirement:**
- Having Redundancy Path.
- Randomness.
- MTD Switching Frequency.

**Attacker Assumptions:**
- DoS attack on only one of the communication channels.

SDN-MTD Experimental Evaluation

- Static Routing (Traditional no MTD)
- MTD Channel Hopping (Fast vs. Slow) = 9 MTD intervals
- Attack Intensity (High vs. Low) = 5 attacks
  - hping3 (DoS Tool)
- 3 SDN-enabled router

- Total Test Cases = MTD Frequency x Attack Intensity x SDN Channels = 135
- DER Packet Drop Rate
- DER Real-Time Latency

<table>
<thead>
<tr>
<th>Attack Percentage</th>
<th>Attack Volume (packet/sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0% (No Attack)</td>
<td>0</td>
</tr>
<tr>
<td>25%</td>
<td>250</td>
</tr>
<tr>
<td>50%</td>
<td>500</td>
</tr>
<tr>
<td>75%</td>
<td>750</td>
</tr>
<tr>
<td>100% (Full DoS)</td>
<td>1000</td>
</tr>
</tbody>
</table>

Increase MTD Channel Switching Interval
### Performance Evaluation (DER Packet Drop Rate vs. Attack)

<table>
<thead>
<tr>
<th>Attack Volume</th>
<th>Static</th>
<th>0.1s</th>
<th>0.3s</th>
<th>0.5s</th>
<th>1s</th>
<th>3s</th>
<th>5s</th>
<th>10s</th>
<th>15s</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>0.00%</td>
<td>0.33%</td>
<td>0.33%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.17%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>25%</td>
<td>25.00%</td>
<td>12.67%</td>
<td>12.17%</td>
<td>8.83%</td>
<td>8.33%</td>
<td>8.17%</td>
<td>7.67%</td>
<td>8.33%</td>
<td>11.33%</td>
</tr>
<tr>
<td>50%</td>
<td>50.00%</td>
<td>27.67%</td>
<td>23.33%</td>
<td>16.83%</td>
<td>16.50%</td>
<td>16.17%</td>
<td>15.83%</td>
<td>16.67%</td>
<td>24.33%</td>
</tr>
<tr>
<td>75%</td>
<td>75.00%</td>
<td>41.67%</td>
<td>34.50%</td>
<td>26.83%</td>
<td>25.17%</td>
<td>26.33%</td>
<td>24.00%</td>
<td>25.00%</td>
<td>37.33%</td>
</tr>
<tr>
<td>100%</td>
<td>100.00%</td>
<td>54.50%</td>
<td>45.17%</td>
<td>36.33%</td>
<td>33.83%</td>
<td>34.50%</td>
<td>33.83%</td>
<td>35.00%</td>
<td>49.50%</td>
</tr>
</tbody>
</table>

![Graph showing DER Packet Drop Rate vs. Attack Volume](image-url)
Performance Evaluation (Packet Drop Rate vs. MTD Freq)

<table>
<thead>
<tr>
<th>Attack Volume</th>
<th>Static</th>
<th>0.1s</th>
<th>0.3s</th>
<th>0.5s</th>
<th>1s</th>
<th>3s</th>
<th>5s</th>
<th>10s</th>
<th>15s</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>0.00%</td>
<td>0.33%</td>
<td>0.33%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.17%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>25%</td>
<td>25.00%</td>
<td>12.67%</td>
<td>12.17%</td>
<td>8.83%</td>
<td>8.33%</td>
<td>8.17%</td>
<td>7.67%</td>
<td>8.33%</td>
<td>11.33%</td>
</tr>
<tr>
<td>50%</td>
<td>50.00%</td>
<td>27.67%</td>
<td>23.33%</td>
<td>16.83%</td>
<td>16.50%</td>
<td>16.17%</td>
<td>15.83%</td>
<td>16.67%</td>
<td>24.33%</td>
</tr>
<tr>
<td>75%</td>
<td>75.00%</td>
<td>41.67%</td>
<td>34.50%</td>
<td>26.83%</td>
<td>25.17%</td>
<td>26.33%</td>
<td>24.00%</td>
<td>25.00%</td>
<td>37.33%</td>
</tr>
<tr>
<td>100%</td>
<td>100.00%</td>
<td>54.50%</td>
<td>45.17%</td>
<td>36.33%</td>
<td>33.83%</td>
<td>34.50%</td>
<td>33.83%</td>
<td>35.00%</td>
<td>49.50%</td>
</tr>
</tbody>
</table>

Graph showing Packet Drop Percentage vs. MTD Switching Time (s) for different Attack Volumes and MTD Switching Frequencies.
The proposed model could maintain real-time operation (0.13s) even under full 100% DoS on the communication network.
Conclusions - SDN-MTD

• Proposed an SDN-enabled MTD solution for attack surface reduction
• Implemented and evaluated it using HIL Testbed
• SDN-enabled MTD show lower packet drop percentages with feasible latency

Future Work:
• Scalability of the SDN-enabled MTD for complex networks
• Orchestration between STD-MTD and other defense mechanisms (e.g., ADS)
CONCLUSIONS

• DER deployment is continuously growing..

• Also, Attack Surface is increasing ...

• Attack frequency and stealthy-ness have been increasing ...

• Cybersecurity Life-cycle solution is important
  • Attack Deterrence prevention, detection, mitigation, resilience, and forensics

• Presented two case studies
  • Attack Detection – Cybersecurity Situational Awareness
  • Attack Prevention – Attack surface reduction using SDN-enabled MTD

• A lot more R&D and deployment needs to be done
  • Attack prevention, mitigation, resilience
  • Testbeds, deployments, demonstrations, datasets, technology transfer, etc.
Publications

- Relevant Publications:
  - M. Abdelkhalek, and M. Govindarasu, “ML-based Alert Correlation Algorithms For DER Cyber Situational Awareness,” (under submission).

- Industry Outreach:
  - App Development & Dissemination -- "IADS Application for EID devices" development, optimization and functional testing on Docker Containers and published on DockerHub and (Phoenix Contact AppStore “deployment undersax”) for technology transfer and potential impacts
  - DER IT/OT datasets for cybersecurity experimentation – Dissemination via public portals (under development)
  - Technical presentation on IDS implementation into EID and the overall 2-tier IADS architecture to Phoenix Contact for knowledge dissemination and potential technology licensing opportunities. (Presented)
THANK YOU!

Acknowledgements:

Collaborators:
- Moataz Abdelkhalak (ISU, Cisco (now))
- Gelli Ravikumar (ISU)
- Srini Devarajan & Kunal Shah (Poundra)
- Raja Ayyanar & S. Thakar (Arizona State University)
- Burhan Hyder (ISU, PNNL (now))

Funding Support:
U.S. Department of Energy (DOE)
Solar Energy Technology Office (SETO) Award # DE-EE0008773

Project team members:
- R. Ayyanar
- V. Vittal
- Q. Lei
- Y. Weng
- M. Govindarasu
- D. Srinivasan
- B. Yang
- R. Yang
- K. Duwadi
- G. Ravikumar
- P. Chongfuangprinya
- Y. Ye
- K. Shah
- S. Thakar
- N. Korada
- Y. Si
- M. Sondharangalla
- J. Wu
- J. Yuan
- D. Moldovan
- A. Moataz
- D. Haughton
- C. Rojas
Thank you!

Questions?

Contact:
Manimaran Govindarasu
(gmani@iastate.edu)