Security Analytics for Electric Grid
An Overview of Analytical Approach for Attack Detection, Defense and Vulnerability Assessment
Security Analytics for Electric Grid: Goals

- Vulnerability Assessment and Elimination
- Active defense and mitigation
- Attack detection
Security Analytics for Electric Grid: Goals

- Attack detection
- Active defense and mitigation
- Vulnerability Assessment and Elimination
Why analytics for attack detection?

➢ Rule based engine
  • Learn from attacks
  • Less false alarms
  • Cannot detect unseen attacks

➢ Analytic engine
  • Learn from normal data (and attacks)
  • Categorize seen attacks
  • Report deviated behaviors
Difficulties in attack detection

Physical Fault

Cyber attack

Anomalies
Analytical Approaches for Attack Detection

➢ Supervised or unsupervised?
  • Imbalanced classification
    ✓ Resampling: under sampling, over sampling, ensemble. Etc.
    ✓ Metrics: ROC, confusion matrix, etc.
  • Outlier detection, Novelty detection, Forecasting…
    ✓ Baselining: one class svm, autoencoder, pattern extraction
    ✓ Local outlier factor, isolation forest, etc.
    ✓ CNN/RNN/ARIMA for prediction, etc.

➢ Data sources
  • Sensor, actuator, logs, internet traffic, smart meter, …
  • Information fusion: knowledge graph
Example: Anomaly detection for transactive energy market

- **SAE Initialization (No. of Inputs; No. of SAE Layers)**
- **Updating Weights in SAE**
- **Training Data**
- **Validation Data**
- **Tuning $\epsilon_{\text{physical}}$ for Physical Anomaly**
- **Tuning $\epsilon_{\text{market}}$ for Market Anomaly caused by cyber attack**
- **Measurement Data Instances**
- **Validated SAE Model**
- **Anomaly Detected**
- **Check SCADA, PMU data**
- **Check Cyber System Data (log Files, Server Accesses, Network Traffic)**
- **$\epsilon > \epsilon_{\text{physical}}$**
- **$\epsilon > \epsilon_{\text{market}}$**
Security Analytics for Electric Grid: Goals

- Vulnerability Assessment and Elimination
- Active defense and mitigation
- Attack detection
Adaptive Control for Cyber Defense

➢ Reinforcement Learning
  • Centralized/decentralized
Example: adaptive control for voltage automatic stabilization under attacks

➢ Centralized human control
  • Slow, require human intervention
  • Vulnerable, if centralized server is hacked

➢ Distributed adaptive control
  • Fast, real time response
  • Robust, defense agents are independent
  • Complete data-driven
Security Analytics for Electric Grid: Goals

- Vulnerability Assessment and Elimination
- Active defense and mitigation
- Attack detection
Vulnerability Assessment: Critical Node Detection

➢ Critical component detection in Interdependent Power Networks
  • Mixed integer programming
  • Graph-based heuristic approach

Vulnerability Assessment: Attack Strategy Generation

➢ Machine learning for attackers: learns attack strategy which could be used to evaluate current defense policy

Microgrid
Jiaxing Pi  
Research Scientist  
CT-RDA-BAM-IBI-US  
E-mail: jiaxing.pi@siemens.com