Cyber-Physical Attacks Recovery in Smart Grids: Security, Resiliency, and Interdependency

Dr. Wei Sun, Assistant Professor & Director of Siemens Digital Grid Lab
Department of Electrical & Computer Engineering, University of Central Florida, Orlando, FL
sun@ucf.edu, http://www.eecs.ucf.edu/~weisun/

Project Overview

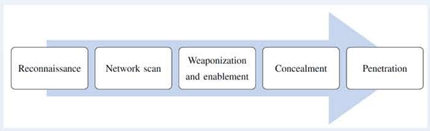
This project aims to develop **adaptive and resilient restoration** strategies to recover cyber-physical systems from cyber attacks and the resulting damage, ultimately self-healing from cyber attacks. It introduces two new types of **multistage** and **multiwave** cyber attacks, and the developed recovery strategies could provide us insights and recommendations on threat monitoring and cyber attack defense.

The project **objectives** are to: 1) **assess** threats and **quantify** the impact of cyber attacks on physical systems; 2) develop **adaptive and resilient restoration** strategies in order to recover from multistage and multiwave cyber attacks in smart grids; 3) provide **security improvements** for stakeholders (e.g., policy makers, regulatory agencies, device manufactures, utility companies, and system operators) in smart grids; and 4) make **recommendations** about allocating human and security resources to recover from cyber security incidents or safety-related events.

The proposed research will advance the knowledge of **interdependent critical infrastructure recovery** after cyber attacks, and provide recommendations to improve system security and resiliency.

Multistage Cyber-Physical Attacks

Definition: a number of **dynamically interrelated attacks**, which the next step of attack depends on the successful completion of the attack in previous step.



In smart grids, vulnerabilities exist in

- communication devices and infrastructure (e.g., sensors and smart meters, PMUs, AMI, utility data centers),
- and network communication protocols (e.g., IEC 61850, DNP3, C37.118).

General Model and An Example in Smart Grid:

Stage 1: Obtain the connection in the enterprise network

- gather information and send a phishing email of software update
- the infected program will be downloaded and malware will be installed
- scan network and identify the vulnerable machine as the target

Stage 2: Exploit the vulnerability in SCADA network

- download Metasploit and exploit shellshock vulnerability to access the data server
- establish a shell connection from PC to data server and download the attack tool

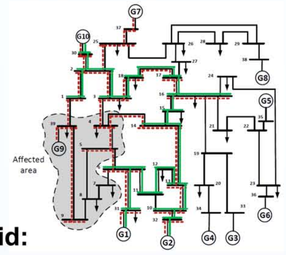
Stage 3: Launch attacks on physical power systems

- By using the ARP spoofing, attackers launches the MITM attack on the IEC 61850 SCADA commands between the IEC 61850 client and relays and PMUs

Multiwave Cyber-Physical Attacks

Definition: **spatial and temporal coordinated attacks**, which attackers compromise cyber system and strategically launch consecutive attacks at selective devices in cyber-physical systems and at different times.

Example: during power system restoration, an attack happens at *t*=11, trips generator G9 together with the outage of transmission lines (1-39), (3-4), (4-5), (4-14), (39-9), and (5-6)



General Model and An Example in Smart Grid:

Model 1: Time-selective multiwave attacks

- disguise part of obtained network access or compromised devices
- strategically choose the time of next attacks

Model 2: Location-selective multiwave attacks

- target at non-critical nodes and cause cascading failures through multiple steps of consecutive attacks

Model 3: Horizontal-spatial multiwave attacks

- evaluate the spatial characteristics of cascading failure propagation and launch attacks in one network

Model 4: Vertical-spatial multiwave attacks

- evaluate the spatial characteristics of cascading failure propagation from the joint effect of interdependency among networks and failures in CPS

Restoration from Multistage and Multiwave Cyber-Physical Attacks

Restoration from Multistage Cyber-Physical Attacks

Step 1: Determine the system status and identify the stage of attacks

- If at stage 1, identify suspicious connections or compromised PCs
- If at stage 2, security checks to scan entire SCADA network
- If at stage 3, physical systems are under attack with damages, evaluate system damage to identify the available resources for restoration

Step 2: Develop the restoration strategies for each attack scenario

- For stage 1, **cyber intrusion detection and recovery**, w/o CPS coupling
- For stage 2, cyber system recovery with the simplified physical system analysis
- For stage 3, restoration strategy considering the **interdependency** between CPS, e.g. restoration of interdependent power and communication systems

Restoration from Multiwave Cyber-Physical Attacks

Strategy 1: Resilient restoration for time-selective multiwave attacks

- The **giant component**-based restoration considering network topology, operational constraints, damage model, and resiliency measurement

Strategy 2: Adaptive restoration for location-selective multiwave attacks

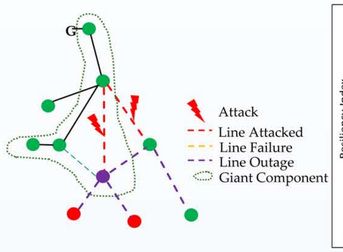
- The two-stage **adaptive** restoration decision support system with the sliding window technique for both optimal planning and optimal real-time operation

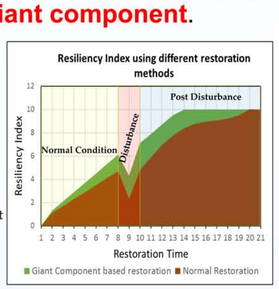
Strategy 3: Coordinated restoration for horizontal- and vertical-spatial multiwave attacks

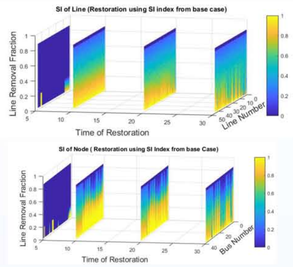
- The **coordinated** restoration between different networks in power system and across power and communication networks

Validation of Restoration Strategies

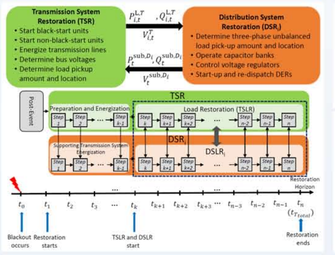
1. Networked-based Restoration: A new concept of **Resilient Restoration** to incorporate network resiliency during the restoration process against time-selective multiwave attacks. Survivability index (SI) is calculated based on the probability of survival as a **giant component**.

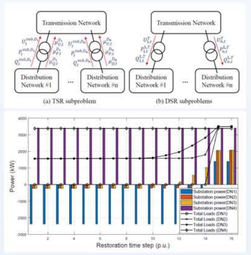


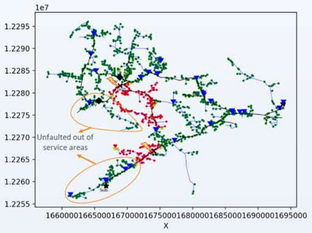




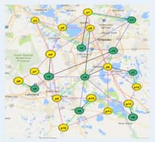
2. Integrated Transmission & Distribution Systems Restoration: Advanced **Adaptive Restoration** for location-selective multiwave attacks. A **distributed** restoration strategy using the ADMM method with the guaranteed global optimum. Real-time simulation of 100,000-node T&D systems with extremely high penetration of PVs.

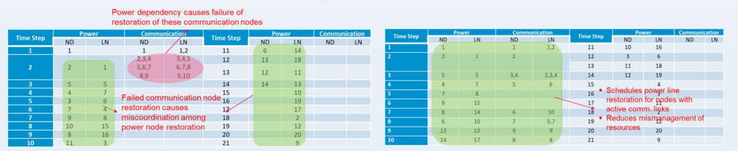






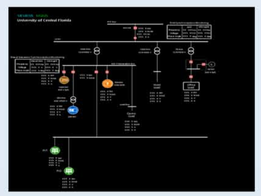
3. Co-restoration of Power and Communication Systems: **Coordinated Restoration** for horizontal- and vertical- spatial multiwave attacks.

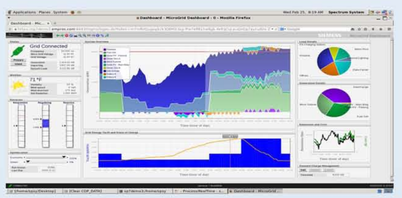


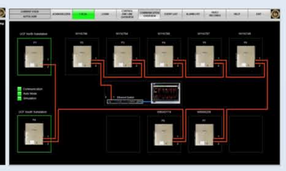


Testbed Demonstration

UCF campus grid is modeled in **Siemens Microgrid Management System (MGMS)** software, including PV, storage, EV, CHP units, etc. The switching is demonstrated in **Siemens Distribution Feeder Automation (SDFA)**.







Acknowledgements

This project is partially supported by Florida Center for Cybersecurity Collaborative Seed Award, NSF Grant ECCS-1552073, and DOE Award DE-EE0007998.