Cyber-Physical Systems Security of Smart Grid

Manimaran Govindarasu
Iowa State University

gmani@iastate.edu

http://powercyber.ece.iastate.edu

Presented at ISRCS 2012, Aug. 15, 2012
Smart Grid: A Cyber-Physical System

Source: http://cnslab.snu.ac.kr/twiki/bin/view/Main/Research
Recognizes that critical infrastructures are vulnerable to cyber attacks from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and other malicious intruders.
Consequences vs. Likelihood – High Impact Low Frequency (HILF) events

NERC Cyber Attack Task Force – High-Impact Low-Frequency Event
Power Grid Cyber Security Roadblocks

- Legacy systems
- Geographically disperse
- Insecure remote connections
- Long system deployments
- Threats/Attacks evolve rapidly

- Adoption of std. technologies with known vulnerabilities
- Connectivity of control systems to other networks
- No “fail-closed” security mechanisms
- Widespread availability of technical info & tools
Attacks - Cyber - Control - Physical

Attacks
- Deny of service
- Malware
- Phishing
- Memory mgmt.
- Authentication

Network
- Spoofing
- MITM
- Routing attacks
- Physical

Cyber Resources
- Devices
  - SCADA Servers
  - Historian
  - HMI
  - Field Devices
- Networks
  - Routing protocols
  - Physical medium
  - Communication protocols

Control
(Power Applications)
- Generation
  - Automatic Voltage Regulator
  - Governor Control
  - Protection
- Transmission
  - VAR Compensation
  - State Estimation
  - Protection
- Distribution
  - Fault Isolation
  - Load Shedding
  - Protection

Physical System Impact
- Stability
- Loss of Load
- Contingency Analysis
- Economics
## Smart Grid Security = Info + Infra + Appln. Security

### Information Security
- **Information Protection**
  - Confidentiality
  - Integrity
  - Availability
  - Authentication
  - Non-repudiation

### Infrastructure Security
- **Infrastructure protection**
  - Routers
  - DNS servers
  - Links
  - Internet protocols
  - Service availability

### Applications Security
- **Generation Control apps.**
- **Transmission Control apps.**
- **Distribution Control apps.**
- **System Monitoring functions**
- **Protection functions**
- **Real-Time Energy Markets**

### MEANS
- **Encryption/Decryption**
- **Digital signature**
- **Message Auth.Codes**
- **Public Key Infrastructure**

### NEEDS
- **Firewalls**
- **IDS/IPS**
- **Authentication Protocols**
- **Secure Protocols**
- **Secure Servers**
- **IPSEC, DNSSEC**

### MEANS
- **Attack-Resilient Control Algos**
  - Anomaly detection
  - Intrusion Tolerance
- **Model-based Algorithms**
- **Risk modeling and mitigation**
- **Attack-Resilient Protection**

---

**Cyber Attacks: Deter, Prevent, Detect, Mitigate, Attribution; be Resilient**

---

**IEEE PES Power & Energy Society**

**PSERC Future Grid Initiative Webinar Series**

February 7, 2012
Research Focus

**Topic 1: Defense against Coordinated Attacks**
- Risk modeling of coordinated cyber attacks
- Risk mitigation algorithms

**Topic 2: Cyber Security of WAPMC**
- Attack-Resilient control algorithm (AGC)
- Domain-specific Intrusion Detection/Tolerance
Topic 1: Risk modeling coordinated attacks

Risk = Threat x Vulnerability x Impacts

- Risk Assessment & Risk Mitigation (GAO CIP Report, 2010)
- Security Investment Analysis

Diagram:
- Real-Time Monitoring
- Threat & Vulnerability Analysis
- Impact Analysis
- Defense measures

Risk Levels:
- High risk
- Low risk
Risk modeling (1)

Hierarchical relationship **system, scenario, and access point** vulnerability

\[ V_S = \max(V(I)) \]

\[ V(I) = \{V(i_1), V(i_2), \ldots, V(i_K)\} \]

\[ V(i) = \sum_{j \in S} \pi_j \times \gamma_j \]

\( \pi_j \) **Probability of intrusion** thro access point \( j \)

\( \gamma_j \) **Impact** due to compromise of substation \( j \)
Risk Modeling (2) – Coordinated Cyber Attacks

Attacker can control:  **Space:** where to attack?  **Time:** when to attack?

**Evaluating $\gamma$ – Impact Estimation**

• Coordinated Attack Groups-
  ✓ Gen + Gen
  ✓ Gen + Trans
  ✓ Trans + Trans

• Optimal power flow simulation
• $\gamma =$ load shedding for OPF solution

**Results**

$\bigcirc$ $\gamma = 363$ MW
$\bigcirc$ $\gamma = 163$ MW
$\bigcirc$ $\gamma = 110$ MW
TOPIC 2: Cyber Security of Wide-Area Monitoring, Protection and Control

Attack-Resilient Control Algorithms

• Man-in-the-middle attacks
• Data integrity attacks
• Denial of service attacks
• Replay attacks
• Timing attacks ...

• Frequency control
• Voltage control
• Transient stability

Cyber-Physical Control in Power Grid
WAMPAC architecture

Power system

PMU

Protection elements

VAR control elements (SVC, FACTS)

High Speed Communication Network

WAP Controller
Logic processing, Arming control, Decisions, Alarms

Plant

Sensors

Actuators

Cyber attack points

Delay
Control Systems Attack Model

**Generic Control System Model**

- **Control Center**
- **Analyses & Computation**
- **Actuators**
- **Machine/Device**
- **Sensors**
- **Data Acquisition**

**Types of Attacks**

- Data integrity
- Replay
- Denial of service
- De-synchronization and timing-based

Figure adopted from - Yu-Hu. Huang, Alvaro A. Cardenas, et al, “Understanding the Physical and Economic Consequences of Attacks on Control Systems”
Automatic Generation Control (AGC)

AGC Features

• Maintains frequency at 60 Hz

• Supply = Demand

• Maintain power exchange at scheduled value

• Ensures economic generation

[Figure from NERC Balancing and Frequency Control
www.nerc.com ]
Automatic Generation Control

Frequency Control

Attack: Modify tie-line flow and frequency measurements
Impact: Abnormal operating frequency conditions

Siddharth Sridhar and G. Manimaran – “Data Integrity Attacks and Impacts on SCADA Control System” – PES GM 2010
Balancing Authorities in the U.S.

Source: NERC
AGC – Attack Vector

Area Control Error

\[ ACE = \Delta P_{\text{net}} + \beta \Delta f \]

\[ \Delta P_{\text{net}} = \text{Scheduled Flow} - \text{Actual Flow} \]

\[ \Delta f = 60 \text{ Hz} - \text{Measured Frequency} \]

Attack: Modify tie-line flow and frequency measurements

Impact: Unhealthy operating frequency conditions
AGC – attack impacts (sample result)

**Attack Impact – Perceived Load at the Control Center**

![Graph showing Attack Impact - Perceived Load at the Control Center](image)
AGC – attack impacts (sample result)

*Attack Impact – Resulting System Frequency*
Attack Resilient Control (ARC)

\[ \text{Attack Resilient Control} = \text{Domain-specific Anomaly Detection} + \text{Model-based Mitigation} \]
• **Forecasts** – Load and wind forecasts
• **Situational Awareness** – System topology, geographic location, market operation
• **Attack Templates** – Attack vectors, signatures, potential impacts
• **System Data** – Machine data, control systems
• **System Resources** – Generation reserves, VAR reserves, available transmission capacity
ARC for AGC

Key

$ACE_R$ – ACE obtained from real-time measurements

$ACE_F$ – ACE obtained from forecast
CPS Testbed-based Evaluation

Information/Control Layer

EMS, SAS, RTUs, IEDs
Routing infrastructure, Network protocols, Routers, Firewalls
Defenses

Communication Layer

Power System Simulators (RTDS, Power factory)

Physical Layer

Cyber attacks
Iowa State’s **PowerCyber** Testbed

- **Control center EMS**
- **WAN (ISEAGE)**
- **Physical RTU, IED**
- **Virtual RTU, IED**
- **Power System Simulation/Emulation**

**Physical components**

**Emulated components**

**Simulated components**

- DNP3
- OPC
- IEC 61850
- DNP3
- OPC
- OPC

**Software Tools**

- DigSilent PowerFactory
- RTDS
ISU PowerCyber Testbed - Configuration
Security Evaluations

Vulnerability assessment
- Protocol vulnerabilities
- Firewall/VPN vulnerabilities
- Substation automation vulnerabilities
- Control center vulnerabilities

Impact Analysis
- System performance
- System stability

Attack-defense studies
- Denial of Sensor measurement (Substation → Control center)
- Denial of Control (Control center → Substation)
- Cyber-Physical Defense Evaluation
Conclusion

**Topic 1: Cyber Security of Wide-Area Control**
- How to design Attack-Resilient algorithms?
- Domain-specific Intrusion Detection

**Topic 2: Defense against Coordinated Attacks**
- How to model Risk due to coordinated cyber attacks
- Risk mitigation algorithms

Testbed-based Evaluation Studies
Research Challenges

1. Cyber Physical Systems Security
2. Risk Modeling and Mitigation
3. Transform: FROM Fault-Resilient Grid of today TO Attack-Resilient Grid of tomorrow
4. Defense against HILF cyber events
5. Trust management & Attack Attribution
6. DMS and AMI Security
7. Datasets and Validations
THANK YOU