Smart Grid Cyber Security

• The smart power grid is transforming towards a large cyber-physical system.

• The increased reliance of cyber infrastructure introduces numerous vulnerabilities in a power grid that might be manipulated by a cyber intruder with to disrupt nominal operation.

• In December 2015, the Ukrainian power grid has experienced cyber-attack in their power grid, which switched off 30 substations and left 230 thousand people without electricity.

• The Australian Energy Market Operator (AEMO) has levelled the increasing threat of cyber-attack on power grid as a matter of Australian national security.
Two Projects related to Smart Grid Cyber Security

False Data Injection Attacks on Smart Grid:
La Trobe University and RMIT University
- Demonstrates how sophisticated attacks can be carried out against a smart grid
- Analyses effect of attack using simulation
- Proposes solution to detect special types of attacks that are undetected by IT controls

Cyber Security Risk Assessment framework for Smart Grid:
Deakin University and University of Melbourne
- Developed a generalised quantitative cyber security risk assessment framework for smart power grid.
- Developed of a laboratory scale cyber-physical smart power grid test bed to assess the impact of cyber-attacks on grid operation

The developed risk assessment framework is generic and can be used by any company (GENCOS, TNSPs, DNSPs, MGO, AEMO, Retailers, etc.) operating in a power grid to assess the quantitative cyber security risk of their cyber physical infrastructure. This will help them better understand cyber vulnerabilities in their network and enable them allocate appropriate security infrastructure.
False Data Injection Attacks on Smart Grid

A/Prof. Abdun Mahmood, La Trobe University
Prof. Paul Watters, La Trobe University
Prof. Zahir Tari, RMIT University
Global Cyber Attacks Against Power Systems (Main Incidents from 2010 to 2019)

4. India (October 2019)

Cyberattack hits India's largest nuclear plant: What really happened?

TIMESOFINDIA.COM | Updated: Oct 31, 2019, 19:12 IST

HIGHLIGHTS

- On Monday night, a cybersecurity analyst sent Twitter abuzz when he made public that a cyberattack has resulted in a ‘domain controller-level access at Kudankulam Nuclear Power Plant’.
- He claimed ‘extremely mission-critical targets were hit’ and that the situation was ‘very serious’.

From left, Rosneft, the shipping company, in Chemnitz-Schöneck/Augrave.

OCSC
Oceania Cyber Security Centre
Cybersecurity Attacks in Smart Grid

### Availability attacks
- Denial of service (DoS)
- Distributed DoS (DDoS)
  
  **Target:** PMU

### Integrity attacks
- Man-in-the-middle (MITM)
- False data injection (FDI)
  
  **Target:** EMS/SCADA, AMI

### Confidentiality attacks
- Social engineering:
  - Phishing
  - Password attack
  
  **Target:** Communication protocols

### Authentication/Accountability
- Spoofing attacks:
  - MAC address spoofing
  - IP address spoofing
  
  **Target:** Communication protocols

---

![Diagram of Smart Grid with Cybersecurity Attacks](image-url)
Proposed Power System Model and Experimental Setup
Our Proposed False Data Injection Attack Detection System
A Real-Time Testbed for Cyber Security Risk Assessment and Mitigation to Ensure the Resiliency of Smart Grids

Deakin University and University of Melbourne
About us

1. Renewable Energy and Electric Vehicle Research Group, Deakin University
   - Dr. Enamul Haque
   - Dr. Sajeeb Saha
   - Dr. M. S. Rahman
   - Prof. Aman Oo

2. University of Melbourne
   - A/Prof. Tansu Alpcan
Overview of the Project:

- Development of a generalised quantitative cyber security risk assessment framework for smart power grid.
- Development of a laboratory scale cyber-physical smart power grid test bed to assess the impact of cyber-attacks on grid operation.
Defining the problem (Broader Picture)

Australian Energy Network

High Penetration of Renewables

National Energy Market (NEM)
Defining the problem (Cont.)

Automatic Generation Control Operation

Substation Automatic Control Operation

Distribution Network Control Operation

Microgrid Control Operation
Power Grid Cyber Security Risk Assessment:

- The growing threat of cyber-attack in electricity network has been acknowledged by different countries all over the world.

- In Australia, the Australian Energy Market Operator (AEMO) has levelled the increasing threat of cyber-attack on power grid as a matter of Australian national security.

- The first and foremost step while ensuring cyber-security of a power grid is to conduct a thorough cyber security risk assessment of the cyber physical infrastructure of the power grid, as it identifies cyber risks, prioritize them and helps developing strategies to mitigate them.
Power Grid Cyber Security Risk Assessment:

• There is no generic framework available for assessing cyber security risks for power grids.

• This is mainly due to the large interconnected structure of the power grid.

• Deregulated Energy Market Operation makes it even more difficult.
Risk Assessment

Definition: Likelihood of an incident x Impact of that incident
Cyber Security Risk Assessment Framework

Physical Information (Generation, Load, Topology of Network)

Communication Network Information

Step 1:

Develop a Cyber-Physical Model of the system

Identify the cyber vulnerabilities and likelihood of unauthorised access

Identify the parameters that might be manipulated due to unauthorised cyber intrusion
Cyber Security Risk Assessment Framework

Step 2:

1. Formulate an optimal load flow (OPF) problem for the system under consideration

2. Choose randomly $i^{th}$ hour of a day
   Run OPF for the system for that hour

3. Record the load flow results
Cyber Security Risk Assessment Framework

Step 3:
Define the parameters that may be manipulated as follows:
\[ X = \text{Rand}(X_{\text{min}}, X_{\text{max}}) \times F \]

\( F \) is either 0 or 1

Re-formulate an optimal load flow (OPF) problem for the system under consideration for \( i^{\text{th}} \) Hour

Record the load flow results

Step 4:
Calculate
\[ Loss = ||P' - P_A||_{L1} \]

Step 5:
Repeat Steps 2-4, \( N \) number of times

Step 6:
Expected Risk of Power Loss:
\[ E(\text{Loss}) = \frac{1}{N} \sum \text{Loss} \]
Risk Assessment of a Micro-grid

Risk of Power Loss

Cyber Physical Model of a Microgrid
Experimental Test Bed for Assessing Cyber attack Impact
Conclusion

• Cyber security of power grid is of paramount importance as it may pose threat to national security.
• Risk assessment is one of the key steps in ensuring cyber physical security of power grid. This provides a quantification of loss that may occur due to cyber intrusion, which enables the grid operator to understand the impacts of cyber threats and assign appropriate mitigation regime.
• There is no risk assessment framework to assess power grid cyber security.
• The proposed framework is generic can be used by any entity (GENCO, TNSP, DNSP, MGO, Retailers, etc.) in a power grid.