Cyber Physical Security of the Smart Grid

Siu Jun Yen, A/P Sanjib Kumar Panda

Motivation

- Paris agreement: To reduce emission intensity by 36% from 2005 levels by 2030.
- Implementation of smart grid will be one of the key measures to achieve goal, as well as improving efficiency, reliability, and resiliency of the electricity grid.
- Incorporating communication and information on top of the existing grid.
- However, with the increased accessibility into the system, this leads to higher susceptibility to attacks.
- Furthermore, past events have shown that cyber attacks are very advanced and can occur anywhere within the system which could lead to extensive damages to the system operators, consumers and regulators.

Stuxnet 2010

Dragonfly 2013

Black energy 2015

Triton 2017

Past Cyber Attack Events

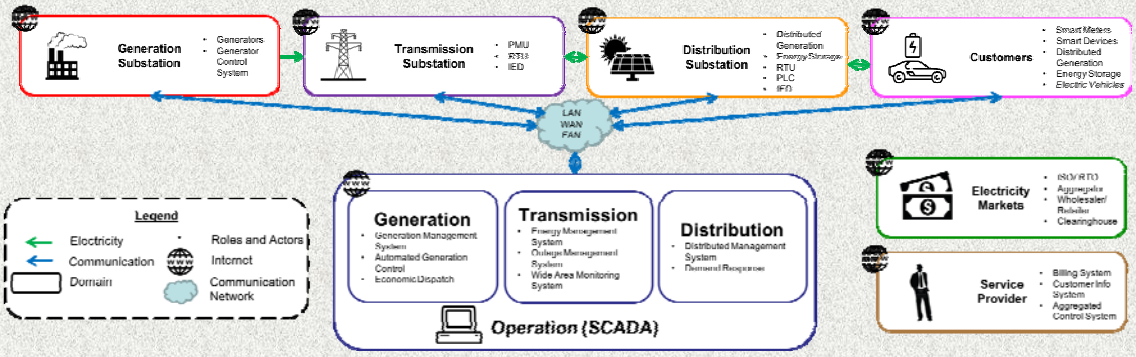

Fig. Smart Grid Architecture

Objectives

- Making use of a security framework to allow conceptualization of the cyber physical security study in a broader context.

Approach

Identification

- Understand how the system works
- Perform risk assessment to identify potential security concerns
  - Attackers intent
  - Access points
  - Impacts on assets

Fig. Automatic Generation Control

Protection

- Against information and cyber attacks
- Develop attack resilient system design
  - Traditional methods (Encryption, authentication)
  - State of the art solutions (Load forecasting, system hardening)

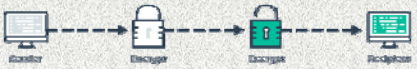

Fig. Encryption

Detection

Signature	• Detects attack when behavior of system matches with a signature pattern in the library • Might not be effective in detecting new threats
Anomaly	• Detects attack when the monitored data deviates from the normal behavior • Might suffer from high false positive
Specification	• Similar to anomaly, but has a set of pre-defined behaviors • Low false positive rate but the strength depends of the accuracy and efficiency of the selected specifications

Mitigation

- Assess if there is a breach of system
- Identify methods to contain the effects of the attacks
- Perform digital forensics to prevent similar occurrence
  - Based on past data, narrow down source of attack
  - Learn what is compromised
  - Suggest protection layers

Fig. Digital Forensic

National Institute of Standards and Technology (NIST) Cyber Security Framework

Conclusion and Future Work

- In the literature, Lack of proper use of framework for the cyber physical security of the smart grid
- Furthermore, past events have shown that attacks are sophiscated and many attacks are yet to be discovered
- Hence, there is a need for developing attack resilient smart grid
- Applying the cyber physical security framework for security assessment on each domain of the smart grid

"This research project is funded by the National Research Foundation Singapore under its Campus for Research Excellence and Technological Enterprise (CREATE) programme."