Known Secure Sensor Measurements for Resilient Infrastructure

Dumidu Wijayasekara
Prof. Milos Manic
Virginia Commonwealth University – Richmond, VA

VIRGINIA COMMONWEALTH UNIVERSITY
Modern Heuristics Research Group
http://mhrg.vcu.edu

Introduction

- Data integrity attacks:
  - Compromised communication infrastructure
  - Critical sensor data manipulated and misrepresented
  - Operator deceived
- Intelligent manipulation of data can lead to:
  - Significant damages (equipment and resources)
  - Can affect non-directly related resources
  - Additional security breaches
- Power grid especially vulnerable to such attacks:
  - Well places attack can misrepresent loads and or production
  - This can lead to significant blackouts and damage to critical and expensive resources
  - Residual repercussions to other entities (e.g.. Industry)

Known Secure Sensor Measurements

- KSSM-Concept of sending a subset of redundant sensor values that are known to be secure, along with the plain text sensor values.
- The known and secure sensor measurements can be used to estimate the overall system health and state.
  - Sensor data fusion and intelligent decision systems used
- This is then used to verify that the plain text sensor information is correct:
  - Mismatch indicates system/data falsification
- Advantages:
  - Not all sensors have to be secured: lowered cost
  - Communication infrastructure is not overwhelmed
  - Able to detect attacks
- Randomly change the set of secured sensors periodically

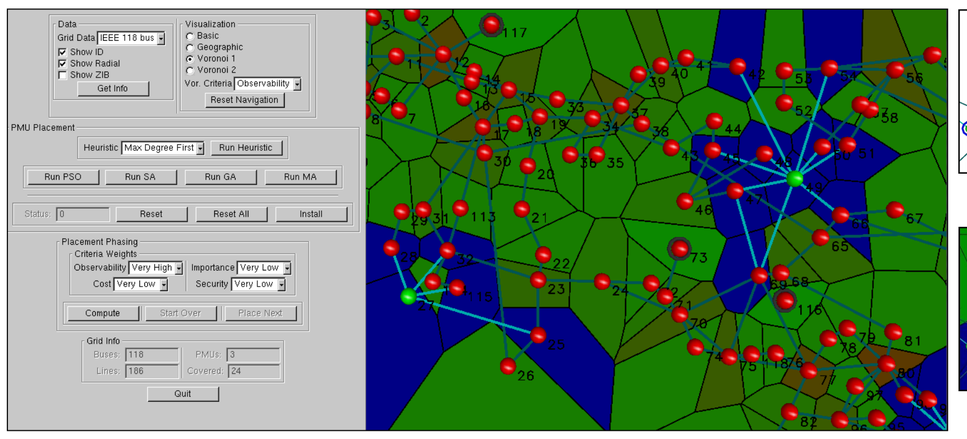
Power Grid: Phasor Measurement Units (PMUs)

- Phasor Measurement Units (PMUs):
  - Widely used in the industry
  - Enables secure communication
  - High initial overhead and communication
  - Difficulty in retrofitting
  - Essential component in smart grid initiative

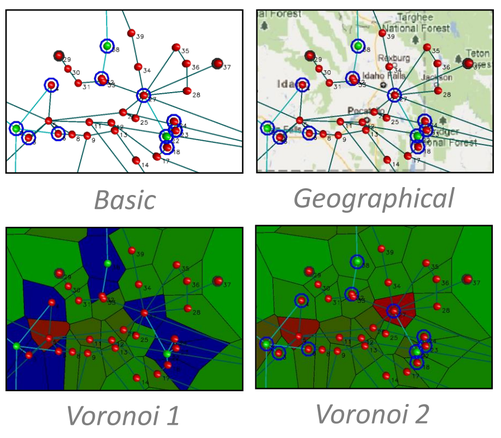
- Optimal PMU Placement (OPP) problem:
  - Find the minimal set of power buses to place PMUs for complete observability of the grid
- Further requirements of PMU Placement:
  - Finding the most optimal set of buses given other criteria such as cost and importance
  - What is the security impact of a PMU

Multi Criteria Based Staging of PMUs

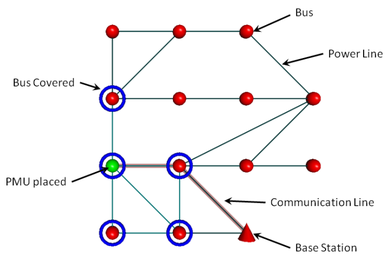
- Multi-criteria decision making problem:
  - Various stake holders, incentives, constraints and requirements
- Example criteria:
  - *Observability*: Based on number of incident buses
  - *Security*: Based on the presence of sparse data integrity attacks
  - *Cost*: Estimated installation cost
  - *Importance*: Relative importance of power bus
- Presented solution utilizes a *Fuzzy Linguistic Weighted Average* based method along with *Evolutionary Algorithms* to provide a dynamic framework for PMU staging



Graphical User Interface



- Tool enables selection and changing of criteria to visualize the importance of each bus/PMU
- Real-time visualization of covered/uncovered buses along with risk
- Visualization of staging of PMUs and gained observability and other requirements

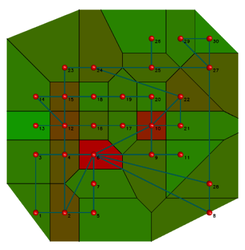


Legend

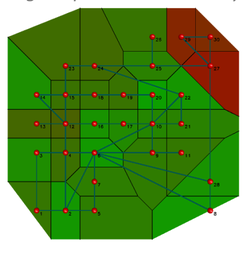
Brief Experimental Results

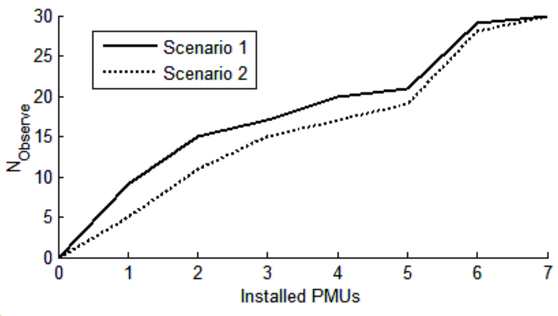
- Able to find the optimal set of buses to place PMUs
- Shows ranking of buses according to the preset criteria
- Multi criteria optimization

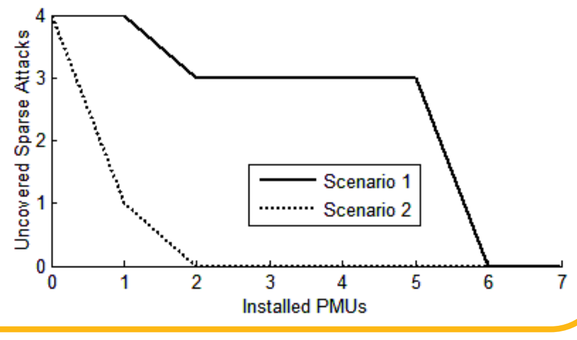
Scenario 1:
Low importance to security



Scenario 2:
High importance to security







Conclusions and Future Work

- KSSM concept for resilience against data integrity attacks
- PMUs help realize the KSSM architecture in power grids
- Multi-criteria decision engine for placement of PMUs in the grid
- Even if all buses have PMUs installed the framework can be used to identify critical assets.
- Randomly select a set of as “trusted” PMUs to achieve full KSSM capability

O. Linda, D. Wijayasekara, M. Manic, M. McQueen, "Optimal Placement of Phasor Measurement Units in Power Grids Using Memetic Algorithms," in Proc. IEEE International Symposium on Industrial Electronics, ISIE 2014, Istanbul, Turkey, June 1-4, 2014.
O. Linda, A. Giani, M. Manic, M. McQueen, "Multi-Criteria Based Staging of Optimal PMU Placement using Fuzzy Weighted Average," in Proc. of IEEE International Symposium on Industrial Electronics, IEEE ISIE 2013, Taipei, Taiwan, May 28-31, 2013.