Securing Smart Power Grids under Data Measurement Cyber Threats

PIs: Sara Eftekharnejad, Syracuse University

Brian Johnson, James Alves-Foss, University of Idaho

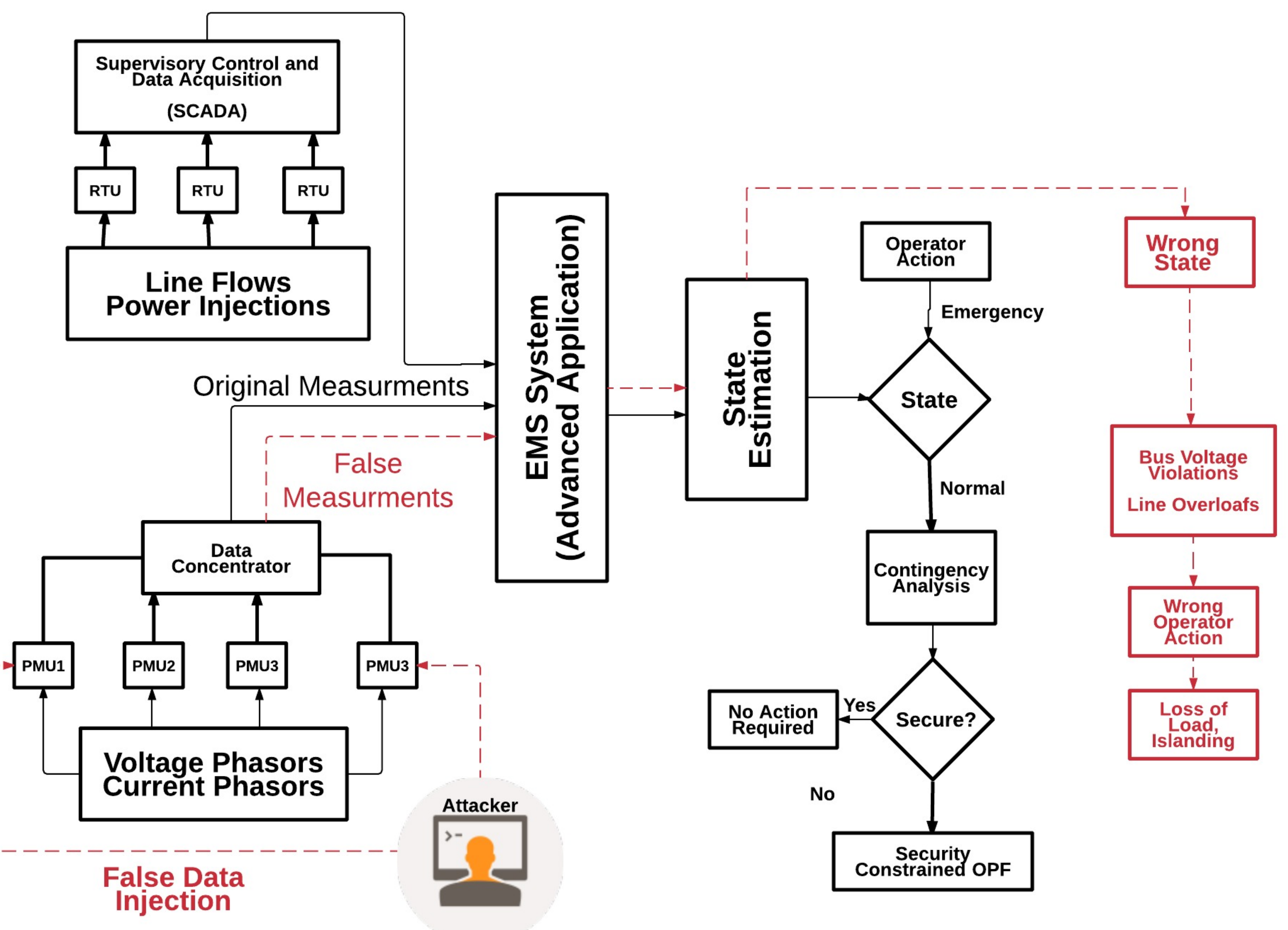
Project Objective: The objective of this project is to: investigate impact of false-data injection attacks on PMU-based power system state estimation; develop methods to detect these attacks before they result in cascading failures; propose methods to prevent wide-spread blackouts once attacks occur.

State Estimation

State estimation allows continuous monitoring of a power system by estimating power system state variables from measurement data provided by SCADA and PMUs. These measurements, can serve as ***attack vectors*** for false data injection attacks.

Threat Model

- ❑ More traditional meters in power systems are being replaced by network connected PMUs.
- ❑ These complex power networks are now subject to possible threats from cyber-attacks which threaten the integrity of the system.
- ❑ The cyber-intruder aims to inject false data in meter measurements such that they remain close to the original, and remain undetected by bad data detection systems.
- ❑ These results in wrong state estimation results that eventually misleads power system operators and special protection systems.
- ❑ This may lead to wrong actions that can cause blackouts.



Investigating the Impact of Attacks on PMUs

PMUs are placed at high voltage or buses with the highest connection degree, in IEEE-30 and 118 bus systems. Both false and random data were injected in PMU measurements to observe system violations.

Detection of Attacks

We will identify critical PMUs in the network considering four aspects: critical buses, critical lines, bad data detection and measurement redundancy.

Results

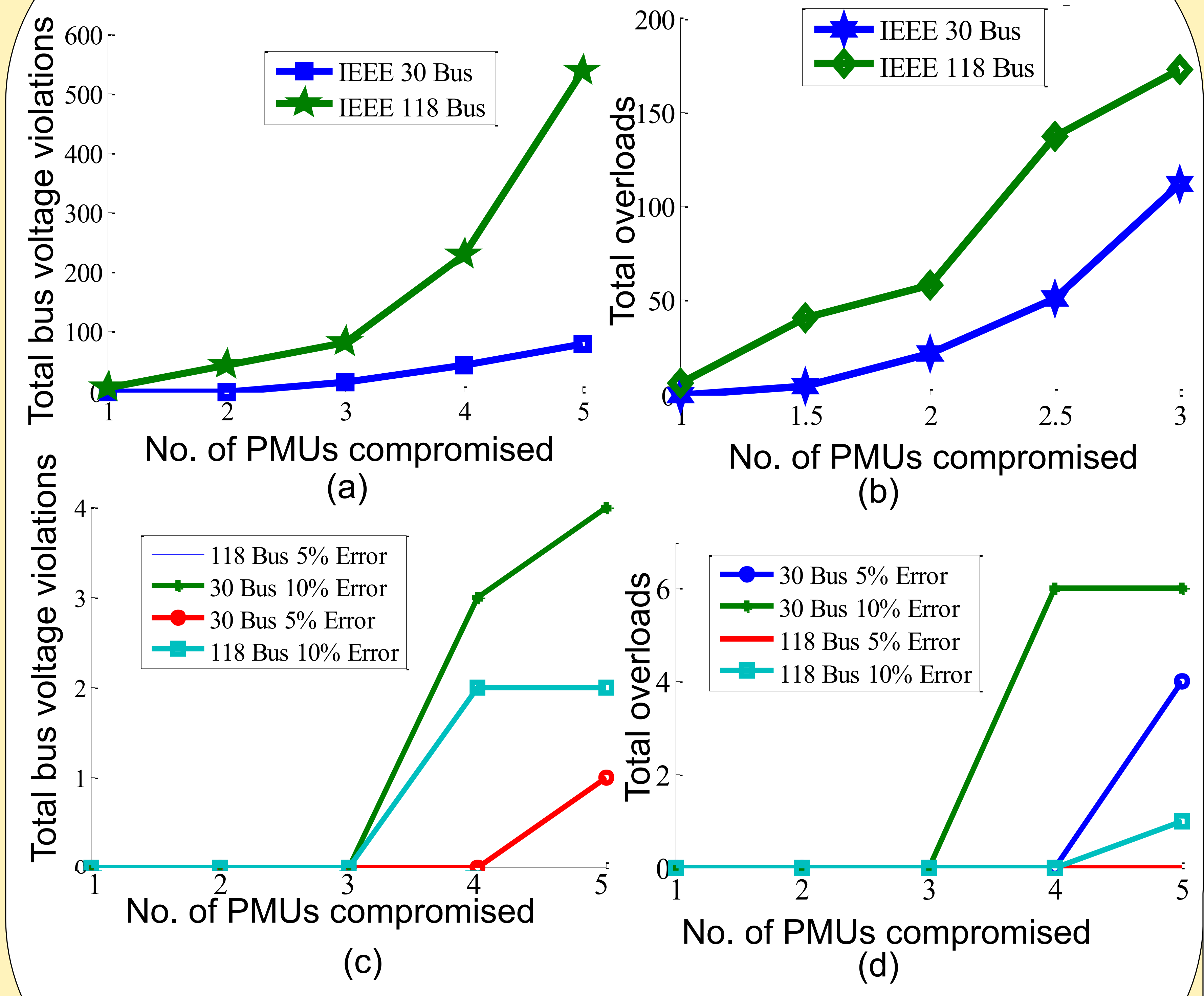


Fig. 1. (a) Total bus voltage violations and (b) Total overloads for false data injections (c) Total bus voltage violations and (d) Total overloads for random data injections

Discussion

- ❑ When false data is injected in a fraction of PMUs placed at the buses connected to the largest number of branches in the system, it resulted in multiple bus violations and overloads, and a significant loss of load.
- ❑ When false data was injected in PMUs placed at only high voltage buses, the total number of bus voltage violations and overloads were smaller than the first scenario.
- ❑ Random data injections were mostly rejected by the bad data detection system, and there were very few cases which resulted in system overloads.

Conclusion

Compromising PMUs in the system resulted in system violations. Systems are the most vulnerable when centrally located PMUs were compromised with addition of designed false data.

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia