ADIDS: An Air-gapped Distributed Intrusion Detection System for the Power Grid (Award #: 1929580)

Raheem Beyah, Morris Cohen, Lukas Graber
School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA
Email: rbeyah@coe.gatech.edu

Power Grid Security

- The power grid is the most important critical infrastructure system
- Historical power grid attacks
  - Aurora attack in 2007
  - Dragonfly 2.0 and BlackEnergy 3.0 in 2013-2015
  - Ukrainian power grid blackout in 2015 and 2016
- Substations form the backbone of electric grids
  - Represent the nodes in the SCADA system
  - The main target of the attackers

Proposed Solution

- Air-gapped solution
- Use side-channel signals from VLF receivers to infer substation activities
- Verify the integrity of the SCADA network traffic
- VLF receivers are unique
  - Captured data is naturally encoded with the quasi-random distribution of lightning signals
  - Lightning signals act as a watermark/nonce
  - Prevents sensor spoofing/playback attacks

Broader Impact

- Other potential applications in various CPSs
  - Electric railway systems
  - Object detection in metal shipping containers
  - GPS free localization
  - Remaining life estimation of circuit breakers
  - Remaining life estimation of power transformers
- Random distribution of lightning strokes
  - Random number generator

SCADA System Security

- Existing works are based on the information from the SCADA system in the power grid
- They rely on the very components of the grid they seek to protect (e.g., sensors that monitor power grid equipment)
- They are directly connected to the power grid (and thus “in the line of fire”)
- Purely cybersecurity monitors do not suffice for cyber-physical platforms

Results

- Multiple prototypes were developed and deployed
- The prototype systems were deployed in real substations
- The proposed distributed system defends against
  - False data injection
  - Malicious command injection
  - Unauthorized transformer tap changing
  - Unauthorized circuit breaker operation (open/close)