Leveraging Physics for EDS Security

Al Valdes, University of Illinois

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security | cred-c.org

Defending Energy Delivery Systems (EDS)

- EDS are characterized by measurement and control interfaces to the physical world
- Concern: cyber attacks can interfere with controls, causing damage or dangerous situations
- On the bright side, physical measurements can provide detection mechanisms beyond conventional cyber defense
  - Are the measurements consistent with the protocol commands?
- In general, we want to:
  - Define the space where an attacker can act, using the laws governing the physical process
  - Reduce this space to the degree possible
  - Focus defenses on the rest

Leveraging Physics to Enhance Security in Electric Power Systems

- Based on Kirchhoff Current Law (KCL)
  - $A \text{ x } I \;=\; 0$
  - A: Signed Topology Matrix
  - I: Vector of current measurements
- Generally, there are many X that satisfy
  - $A \text{ x } X \;= 0$
- Therefore, an adversary can inject any multiple of *X* (false current value) and evade detection, since KCL is still satisfied:
  - $A \text{ x } (I \;+\; cX) \;=\; 0$

CREDC

Detecting Bad Measurements

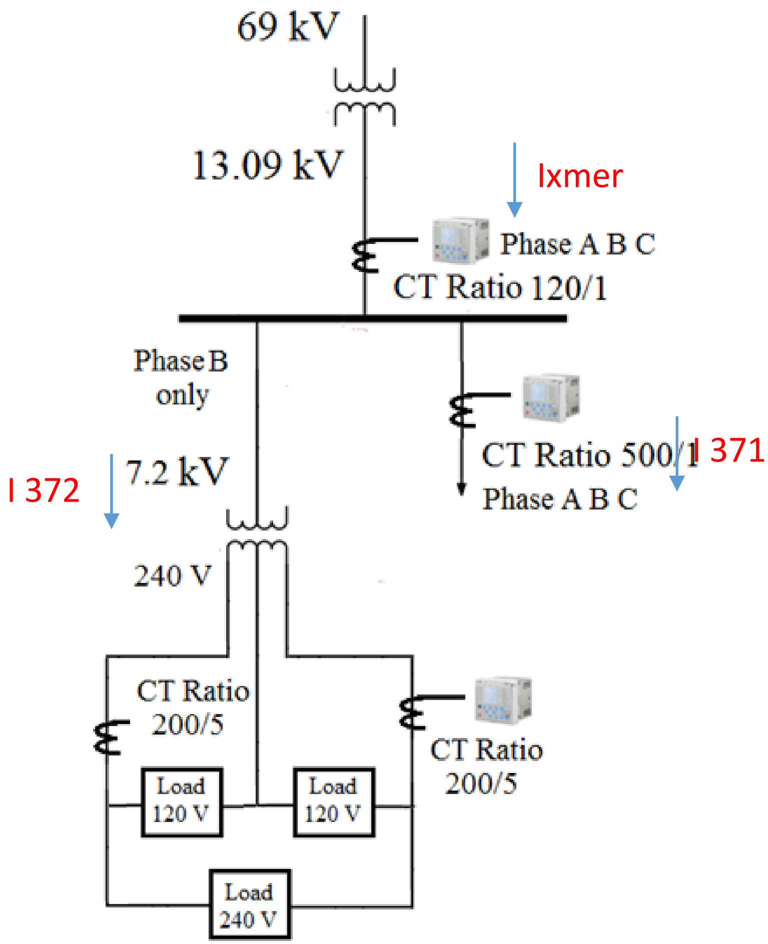
- Suppose attacker injects ΔI in position j

$$A[I + \Delta I] = AI + A\Delta I = S \neq 0$$
$$\Longrightarrow S = A\Delta I$$

- If attacker can corrupt one measurement j, then ΔI has one non-zero element f at position j, and S is f times column j of A
- May want to replace S_j by SIGN(S_j)
  - The result will match the column of A corresponding to the bad measurement
- Analogous to Hamming error correction and geometric single-observer fault detection
- Strategy: Reconcile this condition with observed protocol traffic (IEC 61850) in an agreement algorithm

CREDC

Agreement Algorithm:
TAC Substation topology



$$Ixmer - I371 - I372 = 0$$

$$I371 - \frac{V}{Z371} = 0$$

$$I372 - \frac{V}{Z372} = 0$$

$$\begin{bmatrix} 0 & -1 & -1 & 1 \\ -{}^{1}/_{Z371} & 0 & 1 & 0 \\ -{}^{1}/_{Z372} & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} V \\ I372 \\ I371 \\ Ixmer \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

[A] [I|V]'

Syndrome Vector [Y] = Transpose ([I|V] * [A]) * [A] * Diag[W]

Agreement Protocol Implementation

- Developed agreement as an error-correcting code
- Matlab/Simulink simulation
  - System parameters (voltages, currents, complex impedances) based on typical values, but do not represent any specific system
- Migrated to an emulation environment with
  - ABB REF 615 relays
  - Real Time Digital Simulator (RTDS) representing circuits of interest
  - Supplemented by emulated/virtual devices (BeagleBone)
- Demonstrated in the lab, with RTDS as the simulation driver
- Demonstrated in the field at the Ameren Technology Application Center (TAC)

Approach 2: Machine Learning

- How can we automate the coding of physical constraints (i.e., KCL) in a circuit?
- One possible answer: unsupervised machine learning
- Uses aspects of Self-Organizing Maps (SOM) and Adaptive Resonance Theory (ART)
- Hypothesis: KCL/KVL lead to induced patterns of measurements that can be learned.
  - Normal operation and actual faults obey KCL/KVL
  - False measurement injection requires simultaneous, precise measurement injections at various points, increasing adversary burden

Results

Table 1. Summary of Results

Number of Anomalous Samples in Event Trace				
Event	Starting Sample (Approx)	Training 5000	Training 5500	Training 6000
F92(2X)	2006	0	0	0
F91(2x)	3833	0	0	0
F93(2x)	5400	15	0	0
A90(5x)	5920	28	28	0
F91(2x)	13126	0	0	0
F93(2x)	14523	14	0	0
F92(2x)	15829	0	2	0
F92(5x)	17135	2	0	1
F91(7x)	18442	0	0	0
F93(10x)	19748	15	0	0
A92(5x)	20504	24	24	24
A90(5x)	21807	25	25	0
A91(5x)	23106	27	27	27
A93(5x)	24411	29	21	21
A91(10x)	24930	28	28	28
A93(3x)	26233	27	0	0
A92(7x)	27535	28	28	28
A90(10x)	28838	30	30	0
FA		0.01%	0.01%	0.00%
Detection	Samples	92.06%	78.15%	71.11%
	Traces	100.00%	88.89%	83.33%

8

Summary

- Leveraging physics is an effective strategy to secure EDS
- Our project derived distributed agreement algorithm based on KCL/KVL
  - Demonstrations of important use cases implemented with real hardware-in-the-loop
  - In the lab with RTDS and ABB relays (September 2015)
  - In the field (March 2016)
- We further explored the hypothesis that the physical laws induce system states amenable to machine learning
  - Based on an unsupervised approach to learn patterns corresponding to these system states
  - Demonstrated in simulation

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

http://cred-c.org

@credcresearch

facebook.com/credcresearch/

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security