TCIPG

Security and Robustness Evaluation and Enhancement of Power System Applications:

Trustworthy Cloud Computing for Power

György Dán, Rakesh B. Bobba, Ognjen Vuković, George Gross, and Roy H. Campbell

GOALS

- Explore the use of the cloud computing paradigm and technologies for power grid operations.
- Understand the drivers for adopting cloud computing and the associated security and reliability concerns.
- Understand the impact of cloud computing on current security compliance regimes.
- Develop techniques to use cloud technologies for power operations while addressing security, reliability, and compliance concerns.

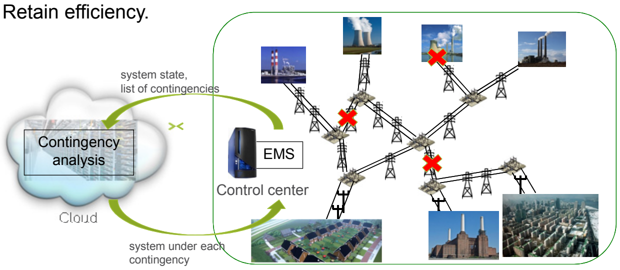
FUNDAMENTAL QUESTIONS/CHALLENGES

- For what power applications is cloud computing suitable?
  - Can real-time or operational applications leverage clouds?
- What are the benefits of moving to the cloud or using cloud technologies?
  - Are they just cost/efficiency and resource elasticity?
  - Are there security benefits from pooled and dedicated operational security teams?
- Can we use existing cloud technologies and meet the reliability, security, real-time performance, and compliance needs of power applications?
  - Multi-user, shared, best-effort systems rather than dedicated or real-time systems.
  - Shared infrastructure with no isolation guarantees.
  - Doesn't support the perimeter-based security model underlying the compliance regime.
- Can we design or tailor cloud technologies to meet the reliability, security, real-time performance, and compliance needs of power applications?

CASE STUDY: CONTINGENCY ANALYSIS IN CLOUD

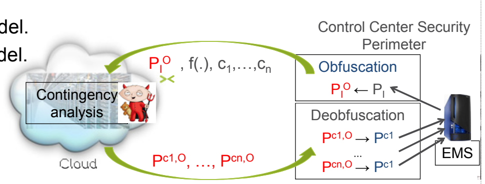
Goal: Perform contingency analysis in the cloud while masking sensitive data.

- Mask knowledge about critical contingencies.
- Mask real power flows.
- Retain efficiency.

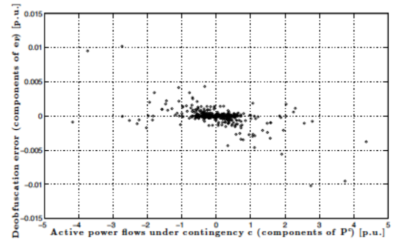


Approach: Apply obfuscation to CA problem before sending it to the cloud & apply deobfuscation on the results.

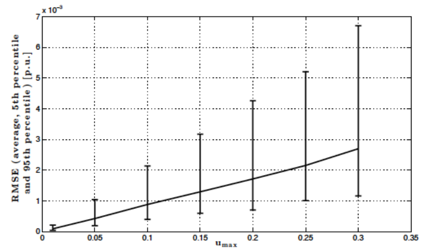
- Obfuscation: Actual flows increased with random values.
  - $P^O = P + P^o$; $P^o = Hx^o$; x^o is computed by fitting power flows perturbed uniformly at random to the system model.
- Deobfuscation: Subtract the random perturbation introduced.
  - $P'^c = P^{c,O} - H_c J_c^{-1} P_I^{c,o}$ $(P_I^{c,o} = F_I^c P_I^o)$
- Error: $e_P = P^c - P'^c$
  - $e_P = 0$ for DC model.
  - $e_P \neq 0$ for AC model.



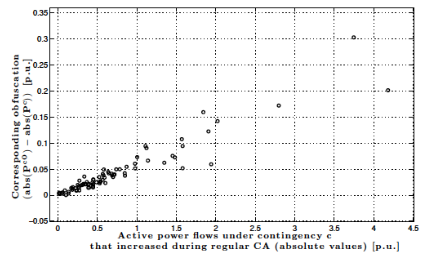
RESEARCH RESULTS



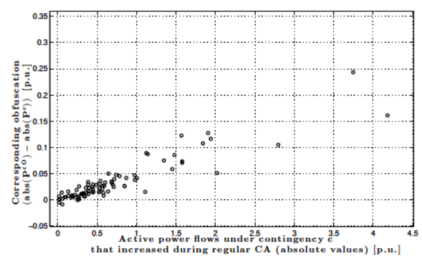
- Error introduced is small.



- Error proportional to original perturbation.



- Power flows that increased under contingency (without obfuscation).
  - Increased for the most part when obfuscated.
  - Decreased in some cases.



- Adversary observing obfuscated power flows cannot be sure of existence of violating contingencies.

FUTURE EFFORTS

- Improve the adversary model for CA in the cloud.
- Bound the error introduced by obfuscation.
- Quantify the obfuscation and security provided.
- Develop reliable and secure cloud technologies suitable for power system applications.

RELATED PUBLICATIONS

- Alex R. Borden, Daniel K. Molzahn, Parmeswaran Ramanathan, and Bernard C. Lesieutre. "Confidentiality-preserving Optimal Power Flow for Cloud Computing." In *50th IEEE Annual Allerton Conference on Communication, Control, and Computing (Allerton), 2012.*
- György Dán, Rakesh B. Bobba, George Gross, and Roy H. Campbell. "Cloud Computing for the Power Grid: From Service Composition to Assured Clouds." *Proc. of the 5th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud)*, June 2013.
- Ognjen Vuković, György Dán, and Rakesh B. Bobba. "Confidentiality-preserving Obfuscation for Cloud-based Power System Contingency Analysis." *Proc. of IEEE SmartGridComm,* October 2013.

TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID | TCIPG.ORG
UNIVERSITY OF ILLINOIS | DARTMOUTH COLLEGE | UC DAVIS | WASHINGTON STATE UNIVERSITY
FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T