On the Security of Distributed Power System State Estimation under Targeted Attacks

Ognjen Vuković, György Dán

School of Electrical Engineering, KTH Royal Institute of Technology
Stockholm, Sweden

ACM SAC
Coimbra, 19. March 2013
Power System Supervision and Control

- **Supervisory Control and Data Acquisition (SCADA)**
- **Energy Management System (EMS)**
  - State Estimation (SE) – a core EMS component
- **Distributed Supervision and Control**
  - Cooperation between operators; ICCP
Distributed State Estimation (DSE)

- **State Estimate of the Entire Interconnected System**
  - Local state estimation + synchronization

- **Security of Distributed State Estimation**
  - Violation of the integrity of exchanged data
  - Stuxnet, Flame

Can the attack affect the DSE?

Detection?

Mitigation?
Outline

- Motivation
- System Model
- Attack Model and Strategies
- Attack Impact
- Detection and Mitigation
- Conclusion
System Model

- Transmission Network: buses and branches
  - Power injections and power flows: \( P = [P_1, P_2, \ldots, P_M]^T \)

- Measurements: \( z = [z_1, z_2, \ldots, z_M]^T, z_i = P_i + e_i \)

- State Vector \( x \): bus voltage angles and magnitudes
  - \( P = f(x^*), x^*: \) actual state of the system
System Model

- **State Estimation**
  - Find $x^*$; Weighted Least Square estimation
  - Gauss-Newton algorithm: $x^{(k+1)} = x^{(k)} + [H^{(k)^T}W^{-1}H^{(k)}]^{-1}H^{(k)^T}W^{-1}[z-f(x^{(k)})]$

- **Distributed State Estimation**
  - Local measurements $z_r$; find $x_r^*$; send $x_{r,r^*}^{(k)}$, use $x_{r,r^*}^{(k)} (x_{b,r^*}^{(k)})$ in k+1

![Diagram of System Model with regions r1 and r2, control center, and state estimation algorithm]
Attack Model

- Attacked region $r_a$; attack vector $a^{(k)}_{r,r_a}$, attack size $\|a^{(k)}_{b,r_a}\|_2$
- Iterations under attack: $x^{(k+1)}_r = x^{(k)}_r + \Delta \tilde{x}^{(k)}_r \neq x^{(k)}_r + \Delta x^{(k)}_r$
- Attacker’s objective:
  \[
  \max_{a^{(k)}_{r,r_a}, k=1,...} c \quad \text{s.t.} \quad \|a^{(k)}_{r,r_a}\|_2 < \beta \\
  \max_{a^{(k)}_{r,r_a}, k=1,...} \|\Delta \tilde{x}^{(k)}_r\|_2 \quad \text{s.t.} \quad \|a^{(k)}_{r,r_a}\|_2 < \beta
  \]
Attack Strategies

First Singular Vector (FSV)

\[
\Delta \tilde{x}_r^{(k)} = \Delta x_r^{(k)} - \left[ H^{(k)T} W^{-1} H^{(k)} \right]^{-1} H^{(k)T} W^{-1} H_b^{(k)} a_{r,r_a}^{(k)}
\]

\[
a_{r,r_a}^{(k)} = u_1, \text{ first singular vector of the matrix } A
\]

- Required knowledge of the system model (matrix \(H\))
- Required knowledge of power flows/injections (\(\text{sign}(a_{r,r_a}^{(k)})\))

Other Strategies

- Maximal Update Vector attack (MUV)
- Uniform Rotation Attack
- A couple more…
- Attack may significantly increase $c$ and introduce high errors
- Attacks can prevent the convergence of DSE
- Protect $z$
All regions affected
Detection and Mitigation

- **Evolution of the state vector**
  - $x^{(k+1)} = g(x^{(k)})$, when converged $x^{(k+1)} \approx g(x^{(k+1)})$
  - If $||g(x) - x^*||_\infty \leq ||x - x^*||_\infty$ ($\forall x$, $\forall x^*$), then $x(k) \to x^*$

- **Detection based on the number of outliers**
  - $||x^{(k+1)} - x^{(k)}||_\infty \leq ||x^{(k')} - x^{(k)}||_\infty$ for large $k$

- The attack can be detected
- Mitigation: perform independent SE
Conclusion

- Vulnerability of the DSE to attacks against exchanged data

- Multiple attack strategies
  - Even just one compromised CC can significantly disturb the DSE
  - Important to protect the confidentiality of measurements

- Detection and mitigation
  - Detection possible based on the number of outliers
  - A simple mitigation scheme

- Localization and an improved mitigation scheme
On the Security of Distributed Power System State Estimation under Targeted Attacks

Ognjen Vuković, György Dán

School of Electrical Engineering, KTH Royal Institute of Technology
Stockholm, Sweden

ACM SAC
Coimbra, 19. March 2013
ICCP

- ICCP servers/clients are often in Demilitarized Zones (DMZ)

- Attacker corrupts ICCP server/client to modify the exchanged data