Cyber-Security Analysis of Electric Power Systems: Deception Attacks on the State Estimator

André Teixeira, György Dán, Henrik Sandberg, Karl H. Johansson

ACCESS Linnaeus Centre, KTH Royal Institute of Technology

IFAC World Congress 2011
September 1st, 2011

The story of Bob, the System Operator... ... and Mallory, a malicious hacker

André Teixeira, György Dán, Henrik Sandberg, Karl H. Johansson

ACCESS Linnaeus Centre, KTH Royal Institute of Technology

IFAC World Congress 2011
September 1st, 2011

Outline

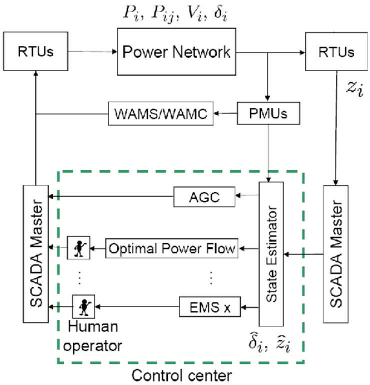
1. Bob and Mallory
   - Meet Bob
   - Meet Mallory
   - Bob vs Mallory
2. Modeling Bob and Mallory
   - Bob's model knowledge
   - Mallory's model knowledge
   - Modeling Mallory's attacks
   - Summary of Bob and Mallory
3. Experimental Results
   - Scenario
   - Mallory's Effort
   - Mallory's Achievements
4. Reporting to Bob

Outline

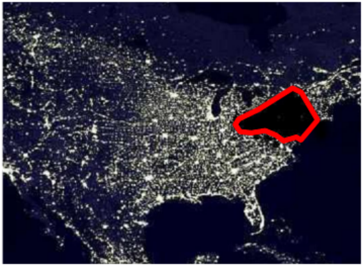
1. Bob and Mallory
   - Meet Bob
   - Meet Mallory
   - Bob vs Mallory
2. Modeling Bob and Mallory
   - Bob's model knowledge
   - Mallory's model knowledge
   - Modeling Mallory's attacks
   - Summary of Bob and Mallory
3. Experimental Results
   - Scenario
   - Mallory's Effort
   - Mallory's Achievements
4. Reporting to Bob

Meet Bob

Bob - The System Operator



- Has many years of experience!
- Is the core of the higher control layer
- Operates the Grid using a SCADA/EMS system that provides
  - the full detailed model of the Grid
  - large amount of measurement data
  - filtering of measurement data (State Estimator)
  - pre and post-filtering outlier detection
  - highly customized software components

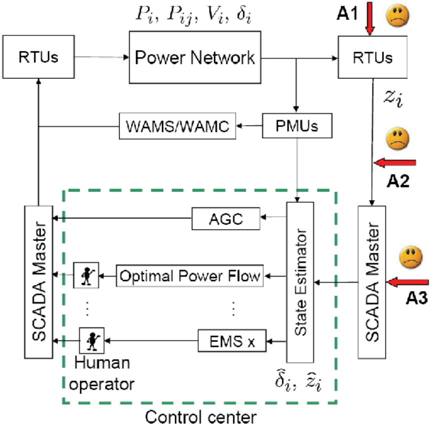


- Ensure the Grid's safe operation
- Avoid major disruptions
- Meet load demand
- Minimize operation costs

- This was a bad day for Bob... (US-Canada 2003 Blackout)

Meet Mallory

Mallory - a malicious hacker



- Has great IT and hacking skills
- Has "some" knowledge about the system model
- Is able to inject false data in a few measuring devices

Meet Mallory

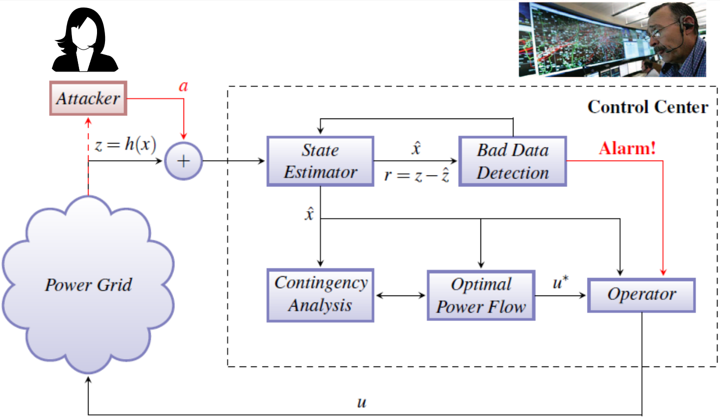
Mallory's Objectives

- Will Bob have another bad day?

- Make Bob have a "bad day" by either:
  - Disrupting the Grid's operation
  - Increasing the operation costs
  - Making money from perturbing the Grid's operation
- Perform the attacks while remaining undetected

Bob vs Mallory

Deception Attacks on the SE



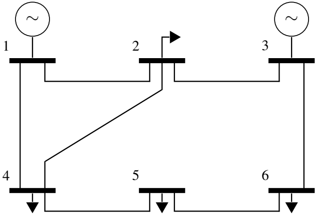
- Bob wants to know
  - if his system is vulnerable to Mallory
  - if adding more measurements would help decrease vulnerabilities
  - where to deploy protection devices to eliminate vulnerabilities
- So he hired us to analyze the situation!

Outline

1. Bob and Mallory
   - Meet Bob
   - Meet Mallory
   - Bob vs Mallory
2. Modeling Bob and Mallory
   - Bob's model knowledge
   - Mallory's model knowledge
   - Modeling Mallory's attacks
   - Summary of Bob and Mallory
3. Experimental Results
   - Scenario
   - Mallory's Effort
   - Mallory's Achievements
4. Reporting to Bob

Modeling Bob and Mallory
Bob's model

- **Detailed Steady-State Model:**
  $z = h(x) + \epsilon$
  measurements: $z \in \mathbb{R}^m$
  state: $x = [\theta^\top V^\top]^\top \in \mathbb{R}^n$
  noise: $\epsilon \sim \mathcal{N}(0, R)$.
  For simplicity, assume $R = I$.



Consider $\theta_{ij} = \theta_i - \theta_j$.

- Power injection measurement model

$$\begin{aligned} P_i &= V_i \sum_{j \in N_i} V_j \left(G_{ij} \cos(\theta_{ij}) + B_{ij} \sin(\theta_{ij}) \right) \\ Q_i &= V_i \sum_{j \in N_i} V_j \left(G_{ij} \sin(\theta_{ij}) - B_{ij} \cos(\theta_{ij}) \right) \end{aligned},$$

- Power flow measurement model

$$\begin{aligned} P_{ij} &= V_i^2 (g_{si} + g_{ij}) - V_i V_j \left(g_{ij} \cos(\theta_{ij}) + b_{ij} \sin(\theta_{ij}) \right) \\ Q_{ij} &= -V_i^2 (b_{si} + b_{ij}) - V_i V_j \left(g_{ij} \sin(\theta_{ij}) - b_{ij} \cos(\theta_{ij}) \right) \end{aligned},$$

Ex.: $P_{14} = V_1^2 (g_{s1} + g_{14}) - V_1 V_4 (g_{14} \cos(\theta_1 - \theta_4) + b_{14} \sin(\theta_1 - \theta_4))$

- **Nonlinear Least-Squares:**

$$\hat{x} = \arg\min_{x \in \mathbb{R}^n} r(x)^\top r(x),$$

where $r(x) = z - h(x)$ is the measurement residual

  - $r(\hat{x}) \approx S\epsilon$, $S = S^\top = S^2$
  - $J(\hat{x}) = r(\hat{x})^\top r(\hat{x})$

- **BDD - Performance index test:**
  $J(\hat{x}) = \epsilon^\top S \epsilon \sim \chi^2_{m-n}$:
  No bad data if $\|r\|_2 \leq \tau_\chi(\alpha)$

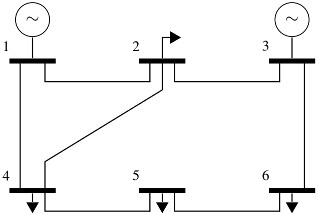
  - $\alpha \in [0,\ 1]$ is the **desired** false alarm rate

- **General expression:** $\|Wr(\hat{x})\|_p < \tau$, for suitable W, p and τ.

Modeling Bob and Mallory

Mallory's model

- **Simplified Steady-State Model (DC-Model):** $z = Hx + \epsilon$
  state: $x = \theta \in \mathbb{R}^{\tilde{n}}$, $\tilde{n} = \frac{n-1}{2}$
  Assumption: $V_i = 1$ for all buses
  No reactive power flows or injections!



- Power injection measurement model

$$P_i \quad = \quad \sum_{j \in N_i} b_{ij}\theta_{ij}$$

- Power flow measurement model

$$P_{ij} \quad = \quad -V_i V_j b_{ij}\theta_{ij}$$

Ex.: $P_{14} = -V_1 V_4 b_{14}(\theta_1 - \theta_4)$

Modeling Bob and Mallory

Mallory's SE model

- **Linear Weighted Least-Squares:**

$$\hat{x} = \left[H^\top H\right]^{-1} H^\top z = H^\dagger z,$$

  - $r(\hat{x}) = z - H\hat{x} = (I - HH^\dagger)(Hx + \epsilon) = S\epsilon,\ S = (I - HH^\dagger)$

- **Mallory corrupting measurements:**

$$z^a = z + a \Rightarrow \hat{x}^a = H^\dagger z^a = H^\dagger (z + a),$$

- **Mallory's idea for stealthy attacks:**
  $a \in \mathrm{Im}(H) \Rightarrow Sa = 0 \Rightarrow r(\hat{x}) = r(\hat{x}^a)$
  [Clements et al. 81, Liu et al. 09]

Modeling Bob and Mallory

Modeling Mallory's stealthy attacks

- **Mallory's Goals**
  - Convergence of the estimator (trivial for the linear model);
  - Stealthiness: $\|Wr(\hat{x}^a)\|_p < \tau$;
  - Induce a desired bias on a subset of measurements - "making Bob have a bad day"

- **Minimum "Effort" Attack Synthesis**

$$\min_a \|a\|_p$$
$$\text{s.t. } a \in \mathcal{G} \cap \mathcal{U} \cap \mathcal{C}$$

  - $\mathcal{G}$ - set of goals
  - $\mathcal{U}$ - set of stealthy attacks
  - $\mathcal{C}$ - set of constraints

- **Different metrics for "effort"**
  - $p = 0$: cardinality of a ($\#$ of measurements to be corrupted) - not convex, can be solved through MILP
  - $p = 1$: may be used as a convex approximation of $p = 0$

Summary of Bob and Mallory

	Bob	**Mallory**
Model	Detailed Nonlinear	Simplified Linear
# Measurements	Large	Small
Active Power	+	+
Reactive Power	+	0
Pre-SE BDD	+	-
Post-SE BDD	+	-

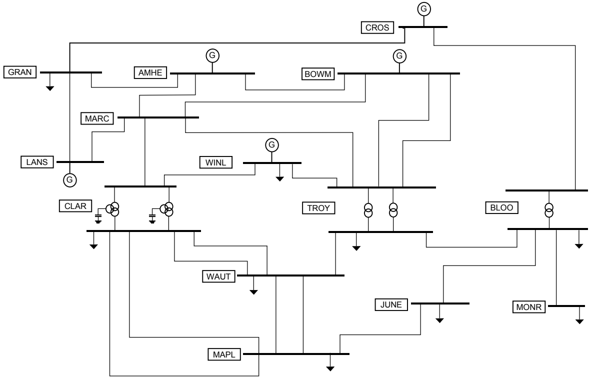
- Does Bob really have reasons to be worried?!

Outline

1. Bob and Mallory
   - Meet Bob
   - Meet Mallory
   - Bob vs Mallory
2. Modeling Bob and Mallory
   - Bob's model knowledge
   - Mallory's model knowledge
   - Modeling Mallory's attacks
   - Summary of Bob and Mallory
3. Experimental Results
   - Scenario
   - Mallory's Effort
   - Mallory's Achievements
4. Reporting to Bob

Experimental Results

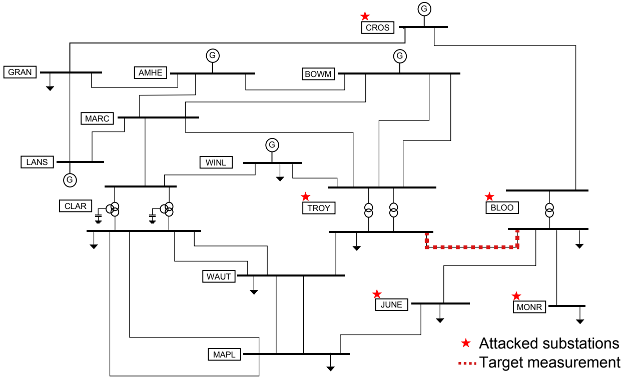
Bob's System



- Typical SCADA/EMS software present in control centers is used
- Virtual grid for training purposes
- Nonlinear model of active and reactive power flows is used

Experimental Results

Mallory's Attack Scenario



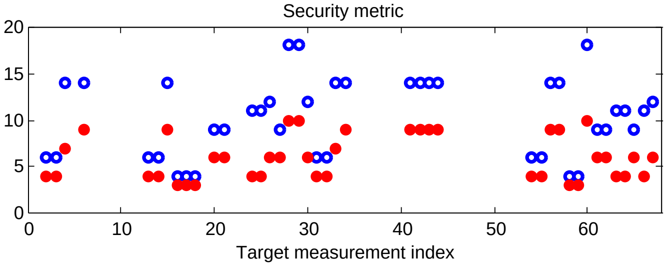
- Only **linear** model of active power flow is known
- Corrupted measurements are sent to the database
- Objective: inject a bias on flow between TROY and BLOO

Mallory's Effort

Adding more measurements vs Deploying protection devices

$$\alpha_k = \min_a \|a\|_0 \quad \text{s.t. } a \in \mathcal{G}_k \cap \mathcal{U} \cap \mathcal{C}$$

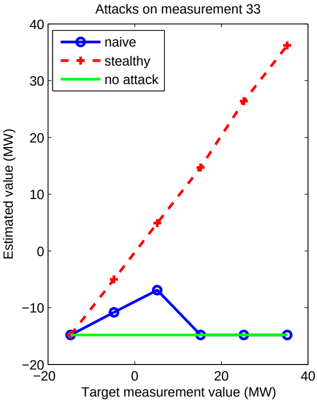
- $\mathcal{G}_k = \{a\colon a_k = 1\}$
- $\mathcal{U} = \mathrm{Im}(H)$
- $\mathcal{C} = \{a\colon a_i = 0, \forall i \in \mathcal{P}\}$ (protected measurements)



Blue circles: α_k with **all** measurements

Red circles: α_k with **only a subset** of measurements

Small attacks



Large attacks

Target bias (MW), a_{33}	Estimate (MW), $\hat{z}^a_{33}$	#BDD Alarms
0	-14.8	0
50	36.2	0
100	86.7	0
150	137.5	0
200	-	-

- Stealthily injected **150MW!** - that's around 60% of the transmission line rating - 260MW.
    - Perhaps Bob would have a "bad day" with this...

Outline

1. Bob and Mallory
   - Meet Bob
   - Meet Mallory
   - Bob vs Mallory
2. Modeling Bob and Mallory
   - Bob's model knowledge
   - Mallory's model knowledge
   - Modeling Mallory's attacks
   - Summary of Bob and Mallory
3. Experimental Results
   - Scenario
   - Mallory's Effort
   - Mallory's Achievements
4. Reporting to Bob

Reporting to Bob

- Mallory has been modeled using a flexible optimization framework that enables the embedding of relevant aspects such as
  - encrypted measurements;
  - pseudo-measurements;
  - finite resources;
  - reduced model knowledge.
- Mallory's model has been applied to Bob's SCADA/EMS software
  - Bob's system seems to be vulnerable to Mallory - reasonably sized biases were injected using linear models;
  - Increasing measurement redundancy of Bob's system does not eliminate all vulnerabilities;
  - Bob got an idea of which measurements are more vulnerable to Mallory.

The End

Thank you!

Questions?