Stochastic Defense Against Complex Grid Attacks

Mauro Escobar & Daniel Bienstock

March 5th, 2019

Columbia University - Industrial Engineering and Operations Research

Motivation

Motivation

Motivation

AC Power Flow Problem

(line physics): admittance matrix

$$Y_{km} = \begin{bmatrix} y_{kk} & y_{km} \\ y_{mk} & y_{mm} \end{bmatrix} \in \mathbb{C}^{2\times 2}$$

$V_k = |V_k| e^{j\theta_k}$ $\qquad$ $V_m = |V_m| e^{j\theta_m}$

$j = \sqrt{-1}$

AC Power Flow Problem

(line physics): admittance matrix

$$Y_{km} = \begin{bmatrix} y_{kk} & y_{km} \\ y_{mk} & y_{mm} \end{bmatrix} \in \mathbb{C}^{2\times 2}$$

$V_k = |V_k| e^{j\theta_k}$ $\qquad$ $V_m = |V_m| e^{j\theta_m}$

$j = \sqrt{-1}$

Active (real) and reactive (imaginary) **power flows**:

$$\begin{aligned} p_{km} &= y_{kk}^{re}|V_k|^2 + y_{km}^{re}|V_k||V_m|\cos(\theta_k - \theta_m) + y_{km}^{im}|V_k||V_m|\sin(\theta_k - \theta_m) \\ q_{km} &= -y_{kk}^{im}|V_k|^2 - y_{km}^{im}|V_k||V_m|\cos(\theta_k - \theta_m) + y_{km}^{re}|V_k||V_m|\sin(\theta_k - \theta_m) \end{aligned}$$

(where $x = x^{re} + jx^{im}$)

Optimal Power Flow Problem

Find a solution to:

- minimize $c(\{P_k^g\}_k)$ *(usually a quadratic function)*
- for each bus $\boldsymbol{k}$ *(power-injection balance)*

$$\sum_{km \in \delta(k)} (p_{km} + j q_{km}) = (P_k^g + j Q_k^g) - (P_k^d + j Q_k^d)$$

- for each branch $\boldsymbol{km}$

$$\begin{aligned}
p_{km} &= y_{kk}^{re} |V_k|^2 + y_{km}^{re} |V_k||V_m| \cos(\theta_k - \theta_m) + y_{km}^{im} |V_k||V_m| \sin(\theta_k - \theta_m) \\
q_{km} &= -y_{kk}^{im} |V_k|^2 - y_{km}^{im} |V_k||V_m| \cos(\theta_k - \theta_m) + y_{km}^{re} |V_k||V_m| \sin(\theta_k - \theta_m) \\
& (p_{km})^2 + (q_{km})^2 \leq (S_{km}^{max})^2 \\
& |\theta_k - \theta_m| \leq \theta_{km}^{max}
\end{aligned}$$

Optimal Power Flow Problem

Find a solution to:

- minimize $c(\{P_k^g\}_k)$ *(usually a quadratic function)*
- for each bus $\boldsymbol{k}$ *(power-injection balance)*

$$\sum_{km \in \delta(k)} (p_{km} + j q_{km}) = (P_k^g + j Q_k^g) - (P_k^d + j Q_k^d)$$

- for each branch $\boldsymbol{km}$

$$\begin{aligned} p_{km} &= y_{kk}^{re} |V_k|^2 + y_{km}^{re} |V_k||V_m| \cos(\theta_k - \theta_m) + y_{km}^{im} |V_k||V_m| \sin(\theta_k - \theta_m) \\ q_{km} &= -y_{kk}^{im} |V_k|^2 - y_{km}^{im} |V_k||V_m| \cos(\theta_k - \theta_m) + y_{km}^{re} |V_k||V_m| \sin(\theta_k - \theta_m) \\ & (p_{km})^2 + (q_{km})^2 \leq (S_{km}^{max})^2 \\ & |\theta_k - \theta_m| \leq \theta_{km}^{max} \end{aligned}$$

Non-convex quadratic problem!

$\Rightarrow$ Solvers: IPOPT, others. Matpower package for Matlab

“Cyber-Physical” attacks

Fact or fiction?

- An adversary carries out a physical alteration of a grid (example: disconnecting a power line)
- This is coordinated with a modification of sensor (PMU) signals – a **hack**
- The goal is to disguise, or keep completely hidden, the nature of the attack and its likely consequences

Prior basic research

- All, or mostly, DC-based
- Intelligent procedures for enriching state estimation so as to detect and reconstruct attacks

Prior basic research

- All, or mostly, DC-based
- Intelligent procedures for enriching state estimation so as to detect and reconstruct attacks
- Liu, Ning Rieter (2009), Kim and Poor (2001)
- Deka, Baldick, Vishwanath (2015)
- Soltan, Yannakakis, Zussman (2015 -)

Soltan, Yannakakis, Zussman 2017

- Attacker disconnects lines plus alters sensor output in an (unknown) zone of the grid
- As a result, the equation

$$B\theta = P^g - P^d$$

  is wrong because B is incorrect and measurements θ are (sparsely) false
- A statistical procedure to try to “fit” a correction to B and a discovery of false data

Today: load change, signal hacking – all AC

- An attacker causes physical changes in the network: in particular **load** changes (no generator changes)
- Attacker also hacks the signal flow: the output of some sensors is altered

Today: load change, signal hacking – all AC

- An attacker causes physical changes in the network: in particular **load** changes (no generator changes)
- Attacker also hacks the signal flow: the output of some sensors is altered
- Goal of the attacker is twofold:
  - Hide the location of the attack and even the fact that an attack happened
  - **Cause line overloads that remain hidden**

Today: load change, signal hacking – all AC

- An attacker causes physical changes in the network: in particular **load** changes (no generator changes)
- Attacker also hacks the signal flow: the output of some sensors is altered
- Goal of the attacker is twofold:
  - Hide the location of the attack and even the fact that an attack happened
  - **Cause line overloads that remain hidden**
- We assume **full PMU deployment**. Everything is **AC** based.

Ideal attack: setup

- PMUs everywhere: at both ends of each line

Ideal attack: setup

- PMUs everywhere: at both ends of each line
- Attacker has been in the system long enough to learn the system
- Attacker chooses, in advance, a non-generator, sparse set $\mathcal{A}$ of buses to attack and in particular a line uv to overload

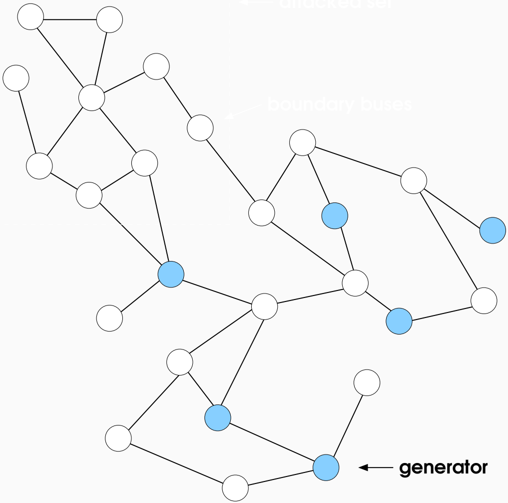
Ideal attack: setup

- PMUs everywhere: at both ends of each line
- Attacker has been in the system long enough to learn the system
- Attacker chooses, in advance, a non-generator, sparse set $\mathcal{A}$ of buses to attack and in particular a line uv to overload
- In near real-time, the attacker learns the current loads **and their stochasticity**
- In near real-time, the attacker solves computational problem that diagrams the attack on $\mathcal{A}$
- This will specify the load changes and the signal distortion

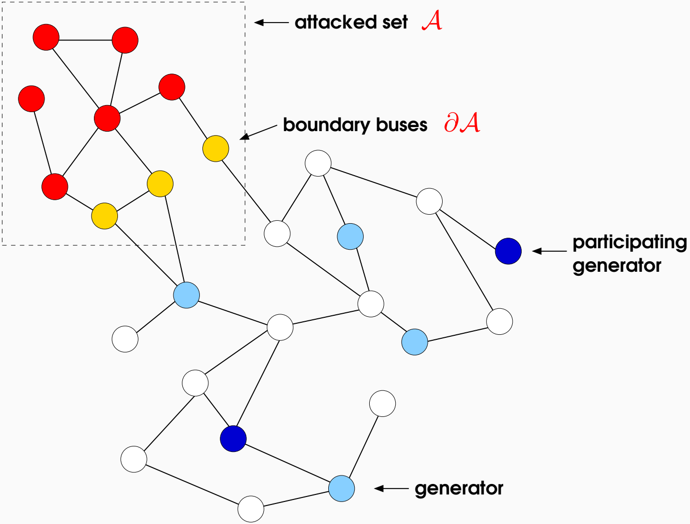
Ideal attack: setup

- PMUs everywhere: at both ends of each line
- Attacker has been in the system long enough to learn the system
- Attacker chooses, in advance, a non-generator, sparse set $\mathcal{A}$ of buses to attack and in particular a line uv to overload
- In near real-time, the attacker learns the current loads **and their stochasticity**
- In near real-time, the attacker solves computational problem that diagrams the attack on $\mathcal{A}$
- This will specify the load changes and the signal distortion
- Post-attack: attacker cannot recompute much and only relies on adding "noise" to computed distorted signals

Undetectable attack: The attacker's perspective



Undetectable attack: The attacker's perspective



Undetectable attack: The attacker's perspective (abridged!)

- For every bus, a "true" and "reported" complex voltage (magnitude and angle) V_k^T and V_k^R

Undetectable attack: The attacker's perspective (abridged!)

- For every bus, a "true" and "reported" complex voltage (magnitude and angle) V_k^T and V_k^R
- True and reported voltages **must** agree on $\mathcal{A}^C \cup \partial\mathcal{A}$

Undetectable attack: The attacker's perspective (abridged!)

- For every bus, a "true" and "reported" complex voltage (magnitude and angle) V_k^T and V_k^R
- True and reported voltages **must** agree on $\mathcal{A}^C \cup \partial\mathcal{A}$
- True and reported **currents** may differ for lines within $\mathcal{A}$

Undetectable attack: The attacker's perspective (abridged!)

- For every bus, a "true" and "reported" complex voltage (magnitude and angle) V_k^T and V_k^R
- True and reported voltages **must** agree on $\mathcal{A}^C \cup \partial\mathcal{A}$
- True and reported **currents** may differ for lines within $\mathcal{A}$
- Voltages and currents agree on all other lines (true and reported are identical)

Undetectable attack: The attacker's perspective (abridged!)

- For every bus, a "true" and "reported" complex voltage (magnitude and angle) V_k^T and V_k^R
- True and reported voltages **must** agree on $\mathcal{A}^C \cup \partial\mathcal{A}$
- True and reported **currents** may differ for lines within $\mathcal{A}$
- Voltages and currents agree on all other lines (true and reported are identical)
- Two power flow solutions; each mush satisfy AC power flow

Undetectable attack: The attacker's perspective (abridged!)

- For every bus, a "true" and "reported" complex voltage (magnitude and angle) V_k^T and V_k^R
- True and reported voltages **must** agree on $\mathcal{A}^C \cup \partial\mathcal{A}$
- True and reported **currents** may differ for lines within $\mathcal{A}$
- Voltages and currents agree on all other lines (true and reported are identical)
- Two power flow solutions; each mush satisfy AC power flow
- A generation change consistent with AGC (automatic generation control)

Undetectable attack: formulation (abridged!)

$$\text{Max } (p^T_{uv})^2 + (q^T_{uv})^2 \tag{1a}$$

s.t.

$$\forall k \in \mathcal{A}^C \cup \partial\mathcal{A}, \quad |V^T_k| = |V^R_k|, \ \theta^T_k = \theta^R_k \tag{1b}$$

$$\forall k \in \mathcal{A}: \quad -(P^{d,R}_k + jQ^{d,R}_k) = \sum_{km \in \delta(k)} (p^R_{km} + jq^R_{km}), \quad P^{d,R}_k \geq 0 \tag{1c}$$

$$-(P^{d,T}_k + jQ^{d,T}_k) = \sum_{km \in \delta(k)} (p^T_{km} + jq^T_{km}), \quad P^{d,T}_k \geq 0 \tag{1d}$$

$$\forall k \in \mathcal{A}^C \backslash \mathcal{R}, \ \hat{P}^g_k - \hat{P}^d_k + j(\hat{Q}^g_k - \hat{Q}^g_k) = \sum_{km \in \delta(k)} (p^T_{km} + jq^T_{km}) \tag{1e}$$

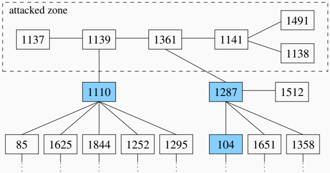
$$\forall k \in \mathcal{R}: \quad P^g_k - \hat{P}^d_k + j(Q^g_k - \hat{Q}^g_k) = \sum_{km \in \delta(k)} (p^T_{km} + jq^T_{km}) \tag{1f}$$

$$P^g_k - \hat{P}^g_k = \alpha_k \Delta \tag{1g}$$

operational limits on all buses, generators, and
lines (outside of attacked area) (1h)

all p^T_{km}, q^T_{km} related to V^T_k, V^T_m and
all p^R_{km}, q^R_{km} related to V^R_k, V^R_m through AC power flow laws (1i)

From case2746wp (that has 2746 buses) from the Matpower case library



bus k	bus m	p^T_{km} p^R_{km}	q^T_{km} q^R_{km}	$\|(p^T_{km}, q^T_{km})\|$ $\|(p^R_{km}, q^R_{km})\|$	S^{max}_{km}
1139	1137	3.36 3.36	2.66 2.66	4.29 4.28	114.00
1361	1141	229.01 108.51	10.49 10.49	**229.25** 109.02	114.00
1141	1491	13.46 6.20	2.41 2.39	13.68 6.64	114.00
1141	1138	209.25 98.06	4.44 5.24	**209.29** 98.20	114.00

Undetectable attack with strong overloads on branches $(1361, 1141)$ and $(1141, 1138)$

Ideal attack: follow-up

Following the attack, attacker needs to **report dynamic data** that satisfy:

- current-voltage consistency: $I^R_{km}(t) \approx y_{kk} V^R_k(t) + y_{km} V^R_m(t)$
- power-injection consistency: $\sum_{km \in \delta(k)} V^R_k(t) I^R_{km}(t)^* \approx \text{net-injection at } k$

Ideal attack: follow-up

Following the attack, attacker needs to **report dynamic data** that satisfy:

- current-voltage consistency: $I_{km}^R(t) \approx y_{kk} V_k^R(t) + y_{km} V_m^R(t)$
- power-injection consistency: $\sum_{km \in \delta(k)} V_k^R(t) I_{km}^R(t)^* \approx$ net-injection at k

We assume that the attack is perpetrated in ambient conditions, and consider two scenarios:

1. Noisy Data Attack. For any bus and line in $\mathcal{A}$ the attacker reports

$$V_k^R(t) = V_k^R + \boldsymbol{\nu_k}(\boldsymbol{t}), \qquad I_{km}^R(t) = I_{km}^R + \boldsymbol{\mu_{km}}(\boldsymbol{t})$$

where $\boldsymbol{\nu_k}(\boldsymbol{t})$ and $\boldsymbol{\mu_{km}}(\boldsymbol{t})$ are drawn from a small variance, zero mean distribution.

Ideal attack: follow-up

Following the attack, attacker needs to **report dynamic data** that satisfy:

- current-voltage consistency: $I_{km}^R(t) \approx y_{kk} V_k^R(t) + y_{km} V_m^R(t)$
- power-injection consistency: $\sum_{km \in \delta(k)} V_k^R(t) I_{km}^R(t)^* \approx$ net-injection at k

We assume that the attack is perpetrated in ambient conditions, and consider two scenarios:

1. Noisy Data Attack. For any bus and line in $\mathcal{A}$ the attacker reports

$$V_k^R(t) = V_k^R + \boldsymbol{\nu_k}(\boldsymbol{t}), \qquad I_{km}^R(t) = I_{km}^R + \boldsymbol{\mu_{km}}(\boldsymbol{t})$$

where $\boldsymbol{\nu_k}(\boldsymbol{t})$ and $\boldsymbol{\mu_{km}}(\boldsymbol{t})$ are drawn from a small variance, zero mean distribution.

2. Data Replay Attack. Attacker supplies previously observed/computed series $V_k^R(t)$, $I_{km}^R(t)$.

Defense: Random Defense Strategy

- Defender is likely to know that "something" happened (and quickly)
- We want a defensive action that is easily implementable in terms of today's grid operation
- Should not lead to false positive

Defense: Random Defense Strategy

- Defender is likely to know that "something" happened (and quickly)
- We want a defensive action that is easily implementable in terms of today's grid operation
- Should not lead to false positive

Random Defense Strategy. Iterate the following steps:

1. For each generator $k \in \mathcal{G}$, randomly choose δ_k such that $\sum_{k \in \mathcal{G}} \delta_k \approx 0$
2. Command each generator to change its output to $P_k^g + \delta_k$
3. Identify inconsistencies in the observed PMUs

Remark: Feasibility in step 1, OPF-like problem

Defense: Identifying Inconsistencies

For a phasor ϕ, denote by
ϕ^T the true value, ϕ^R the reported value, and ϕ^S the **sensed** value

Defense: Identifying Inconsistencies

For a phasor ϕ, denote by
ϕ^T the true value, ϕ^R the reported value, and ϕ^S the **sensed** value

PMU standards guarantee that $|\phi^S - \phi^T| < \tau|\phi^T|$, for $\tau = 1\%$

Defense: Identifying Inconsistencies

For a phasor ϕ, denote by

ϕ^T the true value, ϕ^R the reported value, and ϕ^S the **sensed** value

PMU standards guarantee that $|\phi^S - \phi^T| < \tau|\phi^T|$, for $\tau = 1\%$

Sensed values V_k^S, V_m^S, I_{km}^S, I_{mk}^S must satisfy following **Criteria**:

1. $|V_k^S - y_{mk}^{-1}(I_{mk}^S - y_{mm}V_m^S)| < \frac{2\tau|y_{mk}^{-1}|}{1-\tau}(|I_{mk}^S| + |y_{mm}||V_m^S|)$
2. $|I_{km}^S - y_{kk}V_k^S - y_{km}V_m^S| < \frac{\tau}{1-\tau}(|I_{km}^S| + |y_{kk}||V_k^S| + |y_{km}||V_m^S|)$

If reported phasors do not satisfy these criteria, then line *km* is **flagged**

Defense: Identifying Inconsistencies

Consider

and let $V_k^T(*)$ be true voltage at k at the start of the current iteration of the random defense

Defense: Identifying Inconsistencies

Consider

and let $V_k^T(*)$ be true voltage at k at the start of the current iteration of the random defense

Lemma. *Suppose that*

$$|V_k^T(*) - V_k^R(0)| > \frac{2\tau|y_{km}^{-1}|}{1-\tau}(|I_{mk}^T(*)| + |y_{mm}||V_m^T(*)|) + \frac{2\tau|y_{ka}^{-1}|}{1-\tau}(|I_{ak}^R(0)| + |y_{aa}||V_a^R(0)|)$$

Then, it is impossible for the noise data attacker to statistically satisfy Criterion 1 on both lines ak and mk

Pf. sketch: Use Criterion 1 for lines ak and mk.

Defense: Identifying Inconsistencies, Experiment

	Experiment 1	Experiment 2
$\sum_{k\in\mathcal{G}} \lvert\delta_k\rvert$	463.48	1220.81
Line $(k = 1139, a = 1137)$		
$\lvert V_a^R(0)\rvert\angle\theta_a^R(0)$	$1.0919\angle-6.993^\circ$	$1.0919\angle-6.993^\circ$
$I_{ak}^R(0)$	$-0.0275+0.0281j$	$-0.0275+0.0281j$
Line $(k = 1139, m = 1110)$		
$\lvert V_m^T(*)\rvert\angle\theta_m^T(*)$	$1.0309\angle-7.822^\circ$	$1.0391\angle-7.848^\circ$
$I_{mk}^T(*)$	$0.0905-0.4976j$	$0.1289-0.4901j$
Voltages at $k = 1139$		
$\lvert V_k^R(0)\rvert\angle\theta_k^R(0)$	$1.0919\angle-6.991^\circ$	$1.0919\angle-6.991^\circ$
$\lvert V_k^T(*)\rvert\angle\theta_k^T(*)$	$1.0104\angle-7.822^\circ$	$1.0187\angle-7.936^\circ$
Lemma applied to bus $k = 1139$		
Ratio	1.913	1.732

Covariance Defense

Motivation: Real-world PMU data exhibit **low rank** covariance matrices, and non-Gaussian "noise"

Covariance Defense

Motivation: Real-world PMU data exhibit **low rank** covariance matrices, and non-Gaussian "noise"

Consider the vector of post-attack voltage angles $\theta^R(t) = (\theta_k^R(t) : k \in \mathcal{N})$.
Control center **can learn statistics** of θ^R, denote by Ω its covariance matrix.

(Bienstock, Shukla, Yun, *Non-Stationary Streaming PCA*,
Proc. 2017 NIPS Times Series Workshop.)

Covariance Defense

Motivation: Real-world PMU data exhibit **low rank** covariance matrices, and non-Gaussian "noise"

Consider the vector of post-attack voltage angles $\theta^R(t) = (\theta^R_k(t) : k \in \mathcal{N})$. Control center **can learn statistics** of θ^R, denote by Ω its covariance matrix.

(Bienstock, Shukla, Yun, *Non-Stationary Streaming PCA*, Proc. 2017 NIPS Times Series Workshop.)

Consider:

- $\lambda_1 \geq \cdots \geq \lambda_r > 0$ eigenvalues of Ω larger than certain $\epsilon > 0$
- $w_1, \ldots, w_r$ its corresponding eigenvectors
- $\Gamma > 0$ larger compared to ϵ
- a zero-mean distribution $\mathcal{P}$ with support in $[-1, 1]$
- the bus susceptance matrix B (from DC-model)
- set $\mathcal{F}$ of trusted generators

Covariance Defense

- $\lambda_1 \geq \cdots \geq \lambda_r > 0$ eigenvalues of Ω larger than certain $\epsilon > 0$
- $w_1, \ldots, w_r$ its corresponding eigenvectors
- $\Gamma > 0$ larger compared to ϵ
- a zero-mean distribution $\mathcal{P}$ with support in $[-1, 1]$
- the bus susceptance matrix B (from DC-model)
- set $\mathcal{F}$ of trusted generators

Covariance Defense

- $\lambda_1 \geq \cdots \geq \lambda_r > 0$ eigenvalues of Ω larger than certain $\epsilon > 0$
- $w_1, \ldots, w_r$ its corresponding eigenvectors
- $\Gamma > 0$ larger compared to ϵ
- a zero-mean distribution $\mathcal{P}$ with support in $[-1, 1]$
- the bus susceptance matrix B (from DC-model)
- set $\mathcal{F}$ of trusted generators

Covariance Defense Procedure. Iterate:

V1. Choose a nonzero vector $v \in \mathbb{R}^n$ such that
   (a) $(Bv)_k = 0$ for all $k \notin \mathcal{F}$
   (b) $w_i^\top v = 0$ for $i = 1, \ldots, r$
   (c) for each $k \in \mathcal{F}$, $P_k^g \pm \Gamma(Bv)_k$ is feasible for generator k

V2. For $s = 1, 2, \ldots$ perform epoch s:
   (a) Draw $\boldsymbol{x}$ from $\mathcal{P}$
   (b) Alter power injection at each $k \in \mathcal{F}$ by $\boldsymbol{x}\Gamma(Bv)_k$

Covariance Defense

Covariance Defense Procedure. Iterate:

V1. Choose a nonzero vector $v \in \mathbb{R}^n$ such that

(a) $(Bv)_k = 0$ for all $k \notin \mathcal{F}$

(b) $w_i^\top v = 0$ for $i = 1, \ldots, r$

(c) for each $k \in \mathcal{F}$, $P_k^g \pm \Gamma(Bv)_k$ is feasible for generator k

V2. For $s = 1, 2, \ldots$ perform epoch s:

(a) Draw $\boldsymbol{x}$ from $\mathcal{P}$

(b) Alter power injection at each $k \in \mathcal{F}$ by $\boldsymbol{x}\Gamma(Bv)_k$

Covariance Defense

Covariance Defense Procedure. Iterate:

V1. Choose a nonzero vector $v \in \mathbb{R}^n$ such that

(a) $(Bv)_k = 0$ for all $k \notin \mathcal{F}$

(b) $w_i^\top v = 0$ for $i = 1, \ldots, r$

(c) for each $k \in \mathcal{F}$, $P_k^g \pm \Gamma(Bv)_k$ is feasible for generator k

V2. For $s = 1, 2, \ldots$ perform epoch s:

(a) Draw $\boldsymbol{x}$ from $\mathcal{P}$

(b) Alter power injection at each $k \in \mathcal{F}$ by $\boldsymbol{x}\Gamma(Bv)_k$

If $\boldsymbol{\delta} = \boldsymbol{x}\Gamma v$, then $\quad \mathbf{E}[\delta] = 0, \quad \mathbf{Var}(\delta) = \mathbf{Var}(\boldsymbol{x})\Gamma^2 vv^\top$

Let $B\hat{\boldsymbol{\theta}}^{\boldsymbol{T}} = P^g - P^d + B\boldsymbol{\delta}$

Covariance Defense

Covariance Defense Procedure. Iterate:

V1. Choose a nonzero vector $v \in \mathbb{R}^n$ such that

(a) $(Bv)_k = 0$ for all $k \notin \mathcal{F}$

(b) $w_i^\top v = 0$ for $i = 1, \ldots, r$

(c) for each $k \in \mathcal{F}$, $P_k^g \pm \Gamma(Bv)_k$ is feasible for generator k

V2. For $s = 1, 2, \ldots$ perform epoch s:

(a) Draw $\boldsymbol{x}$ from $\mathcal{P}$

(b) Alter power injection at each $k \in \mathcal{F}$ by $\boldsymbol{x}\Gamma(Bv)_k$

If $\boldsymbol{\delta} = \boldsymbol{x}\Gamma v$, then $\quad \mathbf{E}[\delta] = 0, \quad \mathbf{Var}(\delta) = \mathbf{Var}(\boldsymbol{x})\Gamma^2 vv^\top$

Let $B\hat{\boldsymbol{\theta}}^{\boldsymbol{T}} = P^g - P^d + B\boldsymbol{\delta}$

Lemma: *Suppose $\boldsymbol{x}$ is stochastically independent of ambient noise. Then, under DC model,* $\mathbf{Var}(\hat{\boldsymbol{\theta}}^{\boldsymbol{T}}) = \mathbf{Var}(\boldsymbol{\theta}^{\boldsymbol{T}}) + \mathbf{Var}(\boldsymbol{x})\Gamma^2 vv^\top$.

Final Remarks

- "Ideal" attacks that cause and hide overloads are feasible on large networks
- Two realistic mechanisms to detect an attack, when suspected, changing the generation at certain buses
  - Identifying the boundary lines of the attacked zone, or
  - Changing the covariance matrix of the vector of voltage angles
- Paper available: arxiv.org/abs/1807.06707

Final Remarks

- "Ideal" attacks that cause and hide overloads are feasible on large networks
- Two realistic mechanisms to detect an attack, when suspected, changing the generation at certain buses
  - Identifying the boundary lines of the attacked zone, or
  - Changing the covariance matrix of the vector of voltage angles
- Paper available: arxiv.org/abs/1807.06707

Thank you!