Variability in power systems:
stochastic defense against ideal grid attacks

Daniel Bienstock, Mauro Escobar, Apurv Shukla

Columbia University

Mopta 2018
Variability in power systems

- The next frontier: controlling short-term variability (seconds or less)
Variability in power systems

- The next frontier: controlling short-term variability (seconds or less)
- Goal: safety and controllability as much as economics, or more
Variability in power systems

- The next frontier: controlling short-term variability (seconds or less)
- Goal: safety and controllability as much as economics, or more
- Driven by smart loads, DERs, DPVs, solid state devices, batteries, etc... and

PMUs = “phasor measurement units,” relatively expensive but the way of the future

Goal: very tight, near-real-time control of power systems

Must be able to learn real-time structure and stochastics

Joint work: Columbia and LANL

Bienstock, Escobar, Shukla (Columbia)
Variability in power systems

- The next frontier: controlling short-term variability (seconds or less)
- Goal: safety and controllability as much as economics, or more
- Driven by smart loads, DERs, DPVs, solid state devices, batteries, etc
  ... and **PMUs**
Variability in power systems

- The next frontier: controlling short-term variability (seconds or less)
- Goal: safety and controllability as much as economics, or more
- Driven by smart loads, DERs, DPVs, solid state devices, batteries, etc... and PMUs
- PMUs = “phasor measurement units,” relatively expensive but the way of the future
Variability in power systems

- The next frontier: controlling short-term variability (seconds or less)
- Goal: safety and controllability as much as economics, or more
- Driven by smart loads, DERs, DPVs, solid state devices, batteries, etc ... and PMUs
- PMUs = “phasor measurement units,” relatively expensive but the way of the future
- Goal: very tight, near-real-time control of power systems
Variability in power systems

- The next frontier: controlling short-term variability (seconds or less)
- Goal: safety and controllability as much as economics, or more
- Driven by smart loads, DERs, DPVs, solid state devices, batteries, etc
  ... and PMUs
- PMUs = “phasor measurement units,” relatively expensive but the way of the future
- Goal: very tight, near-real-time control of power systems
- Must be able to learn real-time structure and stochastics
Variability in power systems

- The next frontier: controlling short-term variability (seconds or less)
- Goal: safety and controllability as much as economics, or more
- Driven by smart loads, DERs, DPVs, solid state devices, batteries, etc... and PMUs
  - PMUs = “phasor measurement units,” relatively expensive but the way of the future
- Goal: very tight, near-real-time control of power systems
- Must be able to learn real-time structure and stochastics
- Joint work: Columbia and LANL
“Cyber-physical” attacks on power grids

An adversary carries out a physical alteration of a grid (example: disconnecting a power line)

This is coordinated with a modification of sensor signals – a hack

The goal is to disguise, or keep completely hidden, the nature of the attack and its likely consequences

Power industry: it will never happen ("we would know what happened")

Really?

Bienstock, Escobar, Shukla (Columbia)
“Cyber-physical” attacks on power grids

Fact or fiction?

1 An adversary carries out a physical alteration of a grid (example: disconnecting a power line)
“Cyber-physical” attacks on power grids

Fact or fiction?

1. An adversary carries out a physical alteration of a grid (example: disconnecting a power line)
2. This is coordinated with a modification of sensor signals – a hack
“Cyber-physical” attacks on power grids

Fact or fiction?

1. An adversary carries out a physical alteration of a grid (example: disconnecting a power line)

2. This is coordinated with a modification of sensor signals – a hack

3. The goal is to disguise, or keep completely hidden, the nature of the attack and its likely consequences
“Cyber-physical” attacks on power grids

Fact or fiction?

1. An adversary carries out a physical alteration of a grid (example: disconnecting a power line)
2. This is coordinated with a modification of sensor signals – a hack
3. The goal is to disguise, or keep completely hidden, the nature of the attack and its likely consequences
4. Power industry: it will never happen (“we would know what happened”)

Bienstock, Escobar, Shukla (Columbia)
“Cyber-physical” attacks on power grids

Fact or fiction?

1. An adversary carries out a physical alteration of a grid (example: disconnecting a power line)

2. This is coordinated with a modification of sensor signals – a hack

3. The goal is to disguise, or keep completely hidden, the nature of the attack and its likely consequences

4. Power industry: it will never happen (“we would know what happened”)

5. Really?
Control centers, RTUs, PMUs, state estimation

- Sensor
- Control center
- Tie line
Control centers, RTUs, PMUs

- Control center performs a regulatory and economic role
- Sensors report to control center
- Control center issues commands to (in particular) smaller generators
- Sensors: RTUs (old), PMUs (new – and more expensive)
- RTUs report **once every four seconds**
- PMUs report
  - **30 to 100 times a second**
  - PMUs report (AC) voltage and current (plus more ...)
- Anecdotal: PMUs overwhelming human operators
- But PMUs are the way of the future
State estimation (very abridged)

A data-driven procedure to estimate relevant grid parameters

- Even with PMUs, data can be “complex”
- Statistical procedure: “state estimation” (at control center)

**DC power flow equations:**

\[ B\theta = P^g - P^d \]

\( B = \) susceptance matrix, \( \theta = \) phase angles, \( P^g, P^d \) generation and load vectors

- Sensors provide information that fit some of the \( \theta, P^d, (P^g?) \) parameters
- State estimation: least squares procedure to estimate the rest, plus more
Some prior basic research on “cyberphysical” attacks

- Intelligent procedures for enriching state estimation so as to detect and reconstruct attacks
- Unavoidable: a model for attacking behavior is essential
- Soltan Yannakakis Zussman (2015 - )
- **Warning**: watch out for those assumptions!
- Attacks are **static**
Some prior basic research on “cyberphysical” attacks

- Intelligent procedures for enriching state estimation so as to detect and reconstruct attacks
- Unavoidable: a model for attacking behavior is essential
- Liu Ning Reiter (2009), Kim Poor (2011),
- Deka Baldick Vishwanath (2015)
- Soltan Yannakakis Zussman (2015 - )
- **Warning:** watch out for those assumptions!
- Attacks are **static** and defense is **passive**
Today: load change, signal hacking – all AC

- An attacker causes physical changes in the network:
An attacker causes physical changes in the network:
- In particular **load** changes (no generator changes)
- Possibly also line disconnections
An attacker causes physical changes in the network:

- In particular **load** changes (no generator changes)
- Possibly also line disconnections

Attacker also hacks the signal flow: the output of some sensors is altered

Goal of the attacker is twofold:

1. Hide the location of the attack and even the fact that an attack happened
2. **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)
  - Possibly also line disconnections

- Attacker also hacks the signal flow: the output of some sensors is altered

- Goal of the attacker is twofold:
  1. Hide the location of the attack and even the fact that an attack happened
  2. **Cause line overloads that remain hidden**

- Attacker expects **full PMU deployment**. Everything is AC based.
Basic AC model of a power line in steady state

- Line between buses (nodes) \( k \) and \( m \).
- \( Y_{km} \): 2 × 2 (complex) admittance matrix (physics of the line)
- \( V_k = \text{voltage at } k = |V_k|e^{j\theta_k}, \ j = \sqrt{-1}, \text{ similarly with } V_m \)
- Current-voltage relationship:
  \[
  \begin{pmatrix}
  I_{km} \\
  I_{mk}
  \end{pmatrix} = Y_{km} \begin{pmatrix}
  V_k \\
  V_m
  \end{pmatrix}
  \]
- \( I_{km}, I_{mk} = \text{(complex) current injected into line at } k \ \text{(resp. } m) \)
- \( S_{km} = \text{(complex) power injected into line at } k = V_k I_{km}^* \)
What happens when there is a generation/load mismatch

Frequency response:

\[ \Delta P \Rightarrow \text{frequency change } \Delta \omega \approx -c \Delta P \]
What happens when there is a generation/load mismatch

Frequency response:

\[
\Delta P \Rightarrow \omega \approx -c \Delta P
\]
What happens when there is a generation/load mismatch

Frequency response:

mismatch $\Delta P$
What happens when there is a generation/load mismatch

Frequency response:

mismatch $\Delta P \Rightarrow$ frequency change $\Delta \omega \approx -c \Delta P$
AGC, primary and secondary response (simplified!, abridged!)

Suppose generation vs loads balance spontaneously changes (i.e. a net imbalance)?

- AC frequency changes proportionally (to first order) near-instantaneously

\[ \text{Primary response.} \]
\[ \text{Secondary response.} \]
AGC, primary and secondary response (simplified!, abridged!)

Suppose generation vs loads balance spontaneously changes (i.e. a net imbalance)?

- AC frequency changes proportionally (to first order) near-instantaneously

- **Primary response.** (very quick) Inertia in generators contributes electrical energy to the system

\[
\text{Generator } g \text{ changes output by } \alpha_g \Delta P
\sum \alpha_g = 1, \quad \alpha_g \geq 0, \quad \alpha_g > 0 \text{ for “participating” generators}
\]

Preset participation factors sensed by control center, which issues generator commands
AGC, primary and secondary response (simplified!, abridged!)

Suppose generation vs loads balance spontaneously changes (i.e. a net imbalance)?

- AC frequency changes proportionally (to first order) near-instantaneously
- **Primary response.** (very quick) Inertia in generators contributes electrical energy to the system
- **Secondary response.** (seconds) Suppose estimated generation shortfall $= \Delta P$. Then:

$$\sum g \alpha_g = 1, \quad \alpha_g \geq 0, \quad \alpha_g > 0$$

Preset participation factors sensed by control center, which issues generator commands.
AGC, primary and secondary response (simplified!, abridged!)

Suppose generation vs loads balance spontaneously changes (i.e. a net imbalance)?

- AC frequency changes proportionally (to first order) near-instantaneously
- **Primary response.** (very quick) Inertia in generators contributes electrical energy to the system
- **Secondary response.** (seconds) Suppose estimated generation shortfall $\Delta P$. Then:

Generator $g$ changes output by $\alpha_g \Delta P$
AGC, primary and secondary response (simplified!, abridged!)

Suppose generation vs loads balance spontaneously changes (i.e. a net imbalance)?

- AC frequency changes proportionally (to first order) near-instantaneously

- **Primary response.** (very quick) Inertia in generators contributes electrical energy to the system

- **Secondary response.** (seconds) Suppose estimated generation shortfall = $\Delta P$. Then:

  Generator $g$ changes output by $\alpha_g \Delta P$

  - $\sum_g \alpha_g = 1$, $\alpha \geq 0$, 
AGC, primary and secondary response (simplified!, abridged!)

Suppose generation vs loads balance spontaneously changes (i.e. a net imbalance)?

- **AC frequency changes proportionally (to first order)** near-instantaneously
- **Primary response.** (very quick) Inertia in generators contributes electrical energy to the system
- **Secondary response.** (seconds) Suppose **estimated** generation shortfall \( \Delta P \). Then:

Generator \( g \) changes output by \( \alpha_g \Delta P \)

- \( \sum_g \alpha_g = 1, \alpha \geq 0, \alpha > 0 \) for “participating” generators
- **Preset** participation factors
- **\( \Delta \omega \)** sensed by control center, which issues generator commands
Ideal ("perfect") static attack: setup

- PMUs everywhere: at both ends of each line

Attacker has been in the system long enough to learn the system (data-wise)
Attacker chooses, in advance, a non-generator, sparse set $A$ of buses to attack and in particular a line $uv$ to overload
In near real-time, the attacker learns the current loads, up to small error
In near real-time, the attacker solves computational problem that diagrams the attack on $A$
This will specify the load changes and the signal distortion
Post-attack, attacker cannot recompute much and only relies on adding "noise" to the computed distorted signals
Ideal ("perfect") static attack: setup

- PMUs everywhere: at both ends of each line
- Attacker has been in the system long enough to learn the system (data-wise)

Attacker chooses, in advance, a non-generator, sparse set $A$ of buses $uv$ to attack and in particular a line. In near real-time, the attacker learns the current loads, up to small error. In near real-time, the attacker solves computational problem that diagrams the attack on $A$. This will specify the load changes and the signal distortion.

Post-attack, attacker cannot recompute much and only relies on adding "noise" to the computed distorted signals.
Ideal ("perfect") static attack: setup

- PMUs everywhere: at both ends of each line
- Attacker has been in the system long enough to learn the system (data-wise)
- Attacker chooses, in advance, a non-generator, sparse set $A$ of buses to attack and in particular a line $uv$ to overload
Ideal ("perfect") static attack: setup

- PMUs everywhere: at both ends of each line
- Attacker has been in the system long enough to learn the system (data-wise)
- Attacker chooses, in advance, a non-generator, sparse set $A$ of buses to attack and in particular a line $uv$ to overload
- In near real-time, the attacker learns the current loads, up to small error
Ideal ("perfect") static attack: setup

- PMUs everywhere: at both ends of each line
- Attacker has been in the system long enough to learn the system (data-wise)
- 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, up to small error
- In near real-time, the attacker solves computational problem that diagrams the attack on $\mathcal{A}$
Ideal ("perfect") static attack: setup

- PMUs everywhere: at both ends of each line
- Attacker has been in the system long enough to learn the system (data-wise)
- 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, up to small error
- 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 the computed distorted signals
Undetectable attack: The attacker’s perspective

- Attacked set
- Participating generator
- Boundary
- Generator

Bienstock, Escobar, Shukla (Columbia)
For every bus in $\mathcal{A}$, a “true” and “reported” complex voltage

But:

$$V_k = Y_{km} V_m$$

so $V_k$ must be truthful.
For every bus in $\mathcal{A}$, a “true” and “reported” complex voltage

But: \[ \begin{pmatrix} l_{km} \\ l_{mk} \end{pmatrix} = Y_{km} \begin{pmatrix} v_k \\ v_m \end{pmatrix} \text{ so } v_k \text{ must be truthful} \]
Undetectable attack: tasks for the attacker (abridged!)

- For every bus in $\mathcal{A}$, compute a “true” and “reported” complex voltage (magnitude and angle) $V_k^T$ and $V_k^R$
- True and reported voltages must agree on the boundary of $\mathcal{A}$!
- Compute true and reported currents for lines within $\mathcal{A}$
- Compute voltages and currents on all other lines (true and reported are identical)
- Compute two power flow solutions; each must satisfy AC power equations, load changes a variable
- On responding generators: compute generation change consistent with secondary response if loads are modified
- Restriction to attacker: attacked zone does not include any generators.
Undetectable attack: tasks for the attacker (abridged!)

- For every bus in $\mathcal{A}$, compute a “true” and “reported” complex voltage (magnitude and angle) $V_k^T$ and $V_k^R$
- True and reported voltages **must** agree on the boundary of $\mathcal{A}$!
- Compute true and reported **currents** for lines within $\mathcal{A}$
- Compute voltages and currents on all other lines (true and reported are identical)
- Compute two power flow solutions; each must satisfy AC power equations, load changes a variable
- On responding generators: compute generation change consistent with secondary response if loads are modified
- Restriction to attacker: attacked zone does not include any generators. Why?
- Some additional lying
Undetectable static attack
(load modification, no line tripping, abridged!)

\[
\begin{align*}
\text{Max} & \quad (p_{uv}^T)^2 + (q_{uv}^T)^2 \quad \text{square norm of flow on } uv \\
\text{s.t.} & \\
\forall k \in \mathcal{A}^c \cup \partial \mathcal{A}, \quad V_k^T = V_k^R \quad \text{(truthful voltages outside attacked zone)}
\end{align*}
\] (1a)

\[
\forall k \in \mathcal{A}, \quad -(P_k^d,R + jQ_k^d,R) = \sum_{km \in \delta(k)} (p_{km}^R + jq_{km}^R), \quad \text{(true power flow balance in attacked zone)}
\] (1b)

\[
- (P_k^d,T + jQ_k^d,T) = \sum_{km \in \delta(k)} (p_{km}^T + jq_{km}^T), \quad \text{(reported power flow balance in attacked zone)}
\] (1c)

\[
\forall k \in \mathcal{A}^c \setminus \mathcal{R} : \quad \hat{P}_g^k - \hat{P}_d^k + j(\hat{Q}_g^k - \hat{Q}_d^k) = \sum_{km \in \delta(k)} (p_{km}^T + jq_{km}^T) \quad \text{(LHS is data, not variables)}
\] (1d)

\[
\forall k \in \mathcal{R} : \quad P_g^k - \hat{P}_d^k + j(Q_g^k - \hat{Q}_d^k) = \sum_{km \in \delta(k)} (p_{km}^T + jq_{km}^T) \quad \text{($P_g^k, Q_g^k$ are variables)}
\] (1e)

\[
P_g^k - \hat{P}_g^k = \alpha_k \Delta \quad \text{(AGC response) } \Delta \text{ is a variable,}
\] (1f)

reported data: operational limits on all buses, generators and lines

all $p_{km}^T, q_{km}^T$ related to $|V_k^T|, |V_m^T|, \theta_k^T, \theta_m^T$ through AC power flow laws

Bienstock, Escobar, Shukla (Columbia)  Variance Analysis  Mopla 2018 16 / 40
Undetectable static attack
(load modification, no line tripping, abridged!)

Max \((p_{uv}^T)^2 + (q_{uv}^T)^2\) \quad \text{square norm of flow on } uv \quad (1a)

\text{s.t.}

\forall k \in A^C \cup \partial A, \ V_k^T = V_k^R \quad \text{(truthful voltages outside attacked zone)} \quad (1b)

\forall k \in A, \ - (p_k^d, R + jQ_k^d, R) = \sum_{km \in \delta (k)} (p_{km}^R + jq_{km}^R), \quad \text{(true power flow balance in attacked zone)} \quad (1c)

\quad - (p_k^d, T + jQ_k^d, T) = \sum_{km \in \delta (k)} (p_{km}^T + jq_{km}^T), \quad \text{(reported power flow balance in attacked zone)} \quad (1d)

\forall k \in A^C \setminus R: \ \hat{P}^g_k - \hat{P}^d_k + j(\hat{Q}^g_k - \hat{Q}^d_k) = \sum_{km \in \delta (k)} (p_{km}^T + jq_{km}^T) \quad \text{(LHS is data, not variables)} \quad (1e)

\forall k \in R: \ P^g_k - \hat{P}^d_k + j(Q^g_k - \hat{Q}^d_k) = \sum_{km \in \delta (k)} (p_{km}^T + jq_{km}^T) \quad \text{\(P^g_k, Q^g_k\) are variables} \quad (1f)

\ P^g_k - \hat{P}^g_k = \alpha_k \Delta \quad \text{(AGC response) \(\Delta\) is a variable,} \quad (1g)

\text{reported data: operational limits on all buses, generators and lines} \quad (1h)

all \(p_{km}^T, q_{km}^T\) related to \(|V_k^T|, |V_m^T|, \theta_k^T, \theta_m^T\) through AC power flow laws \quad (1i)

\textbf{AC OPF-like problem, local-solvable in seconds}
A large-scale example: case2746wp

(2746 buses, 3514 lines, 520 generators, 25GW total load)
A large-scale example: case2746wp

(2746 buses, 3514 lines, 520 generators, 25GW total load)

Undetectable attack with strong overloads on branches:

(1361, 1141):
\[ \|\text{reported flow}\| = 109, \|\text{true flow}\| = 229, \text{limit} = 114 \]

(1138, 1141):
\[ \|\text{reported flow}\| = 98, \|\text{true flow}\| = 209, \text{limit} = 114 \]

Net load change: \textbf{135 MW ($< 0.5\%$)} of total load
Non-static attack: follow-up

A blind spot in prior work?
Non-static attack: follow-up

A blind spot in prior work?

“Noisy-data”

Following the attack, for any bus $\in A - \partial A$ the attacker reports (at each time $t$) a complex voltage value

$$\tilde{\mathcal{V}}_k(t) = V_k^R + \nu_k(t)$$

Here, $\nu_k(t)$ is random, with

$$\mathbb{E}(\nu_k(t)) = 0,$$
Non-static attack: follow-up

A blind spot in prior work?

“Noisy-data”

Following the attack, for any bus $\in A - \partial A$ the attacker reports (at each time $t$) a complex voltage value

$$\tilde{V}_k(t) = V_k^R + \nu_k(t)$$

Here, $\nu_k(t)$ is random, with

$$E(\nu_k(t)) = 0,$$

(consistent with zero expected load change)
Non-static attack: follow-up

A blind spot in prior work?

“Noisy-data”

Following the attack, for any bus $\in A - \partial A$ the attacker reports (at each time $t$) a complex voltage value

$$\tilde{V}_k(t) = V_k^R + \nu_k(t)$$

Here, $\nu_k(t)$ is random, with

$$E(\nu_k(t)) = 0,$$

(consistent with zero expected load change)
Non-static attack: follow-up

A blind spot in prior work?

“Noisy-data”

Following the attack, for any bus $\in \mathcal{A} - \partial \mathcal{A}$ the attacker reports (at each time $t$) a complex voltage value

$$\tilde{V}_k(t) = V_k^R + \nu_k(t)$$

Here, $\nu_k(t)$ is random, with

$$E(\nu_k(t)) = 0,$$

(consistent with zero expected load change)

and?
Non-static attack: follow-up

A blind spot in prior work?

“Noisy-data”

Following the attack, for any bus $\in \mathcal{A} - \partial \mathcal{A}$ the attacker reports (at each time $t$) a complex voltage value

$$\tilde{V}_k(t) = V_k^R + \nu_k(t)$$

Here, $\nu_k(t)$ is random, with

$$E(\nu_k(t)) = 0,$$

(consistent with zero expected load change)

and? what else?
Non-static attack: follow-up

A blind spot in prior work?

“Noisy-data”

Following the attack, for any bus $\in \mathcal{A} - \partial \mathcal{A}$ the attacker reports (at each time $t$) a complex voltage value

$$\tilde{V}_k(t) = V_k^R + \nu_k(t)$$

Here, $\nu_k(t)$ is random, with

$$\mathbb{E}(\nu_k(t)) = 0,$$

(consistent with zero expected load change)

and? what else?
Defense, 0

- Defender is likely to know that “something” happened (and quickly). But sensor data is noisy and “something” may be inconsequential.

Solution: change the power quantities in a way that the attacker cannot anticipate, and identify inconsistent signals. How?

A solution: change generator output by a random injection that yields a valid power flow solution ("AGC-lite" plus redispatch).
Defense, 0

- Defender is likely to know that “something” happened (and quickly). But sensor data is noisy and “something” may be inconsequential.

- We want a defensive action that is nearly implementable in terms of today’s grid operation.
Defender is likely to know that “something” happened (and quickly). But sensor data is noisy and “something” may be inconsequential.

- We want a defensive action that is nearly implementable in terms of today’s grid operation.

- Should not lead to false positives.
Defender is likely to know that “something” happened (and quickly). But sensor data is noisy and “something” may be inconsequential.

We want a defensive action that is nearly implementable in terms of today’s grid operation.

Should not lead to false positives.

**Solution:** change the power quantities in a way that the attacker cannot anticipate, and identify inconsistent signals. How?
Defense, 0

- Defender is likely to know that “something” happened (and quickly). But sensor data is noisy and “something” may be inconsequential.

- We want a defensive action that is nearly implementable in terms of today’s grid operation.

- Should not lead to false positives.

- **Solution:** change the power quantities in a way that the attacker cannot anticipate, and identify inconsistent signals. How?

- A solution: change generator output by a **random** injection that yields a **valid** power flow solution (“AGC-lite” plus redispatch).
Defense, 0’ (optimization problem)

Following attack, and in suspicion of an attack

- Defender only has access to **reported** data, which is accurate in the non-attacked zone. But the defender **does not** know the attacked zone.
Defense, 0’ (optimization problem)

Following attack, and in suspicion of an attack

- Defender only has access to reported data, which is accurate in the non-attacked zone. But the defender does not know the attacked zone.

- (repeatedly) Defender chooses a random subset of the AGC-responding generators, and
Defense, 0’ (optimization problem)

Following attack, and in suspicion of an attack

- Defender only has access to **reported** data, which is accurate in the non-attacked zone. But the defender **does not** know the attacked zone.

- (repeatedly) Defender chooses a random subset of the AGC-responding generators, and

- Defender computes a random power flow solution where the chosen generators are allowed to change (up or down) their output, within limits. Other generators can change output by small amounts, within limits. The power flow solution must satisfy e.g. **voltage constraints**.
Defense, $0^*$ (optimization problem)

Following attack, and in suspicion of an attack:

- Defender only has access to **reported** data, which is accurate in the non-attacked zone. But the defender **does not** know the attacked zone.

- **(repeatedly)** Defender chooses a random subset of the AGC-responding generators, and

- Defender computes a random power flow solution where the chosen generators are allowed to change (up or down) their output, within limits. Other generators can change output by small amounts, within limits. The power flow solution must satisfy e.g. **voltage constraints**.

- Defender seeks to make the changes in generation large subject to above constraints.
Defense, 0’ (optimization problem)

Following attack, and in suspicion of an attack

- Defender only has access to **reported** data, which is accurate in the non-attacked zone. But the defender **does not** know the attacked zone.

- **(repeatedly)** Defender chooses a random subset of the AGC-responding generators, and

- Defender computes a random power flow solution where the chosen generators are allowed to change (up or down) their output, within limits. Other generators can change output by small amounts, within limits. The power flow solution must satisfy e.g. **voltage constraints**.

- Defender seeks to make the changes in generation large subject to above constraints. **ACOPF**-like problem, solvable in seconds.
But attacker cannot anticipate this random action, even if the defense is known.
But attacker cannot anticipate this random action, even if the defense is known. **Therefore:**
But attacker cannot anticipate this random action, even if the defense is known. **Therefore:**

(under noisy-data attack)

- Reported currents, and implied power flows, will have **near-constant** values within attacked zone
- But outside of attacked zone, with high-probability (?) most lines will see significant changes in current and power flows
But attacker cannot anticipate this random action, even if the defense is known. **Therefore:**

(under noisy-data attack)

- Reported currents, and implied power flows, will have near-constant values within attacked zone
- But outside of attacked zone, with high-probability (?) most lines will see significant changes in current and power flows

Above example (case2746wp) has over **3500** lines, but in a few iterations we reduce the number of suspicious lines to < **100**.
But attacker cannot anticipate this random action, even if the defense is known. **Therefore:**
(under noisy-data attack)

- Reported currents, and implied power flows, will have **near-constant** values within attacked zone
- But outside of attacked zone, with high-probability (?) most lines will see significant changes in current and power flows

Above example (**case2746wp**) has over **3500** lines, but in a few iterations we reduce the number of suspicious lines to **< 100**.
Defense, 1

But attacker cannot anticipate this random action, even if the defense is known. Therefore:
(under noisy-data attack)

- Reported currents, and implied power flows, will have near-constant values within attacked zone
- But outside of attacked zone, with high-probability (?) most lines will see significant changes in current and power flows

Above example (case2746wp) has over 3500 lines, but in a few iterations we reduce the number of suspicious lines to < 100.

Good, but not good enough
Defense, 2: \[
\left( \frac{l_{km}}{l_{mk}} \right) = Y_{km} \left( \begin{array}{c} V_k \\ V_m \end{array} \right)
\]

- boundary of attacked zone must report near-accurate voltage
- within attacked zone
  - near constant (and false) reported voltage
- not attacked
Defense, 2: \( \left( \frac{l_{km}}{l_{mk}} \right) = Y_{km} \left( \frac{V_k}{V_m} \right) \)

On a line going from boundary to interior of attacked zone
Defense, 2: \[
\begin{pmatrix}
I_{km} \\
I_{mk}
\end{pmatrix}
= Y_{km}
\begin{pmatrix}
V_k \\
V_m
\end{pmatrix}
\]

On a line going from boundary to interior of attacked zone reported current will be wrong
Defense, 2: \[ \begin{pmatrix} I_{km} \\ I_{mk} \end{pmatrix} = Y_{km} \begin{pmatrix} V_k \\ V_m \end{pmatrix} \]

On a line going from boundary to interior of attacked zone, reported current will be wrong because voltage at boundary bus is changing with our defense.
Defense, 2: \[ \begin{pmatrix} I_{km} \\ I_{mk} \end{pmatrix} = Y_{km} \begin{pmatrix} V_k \\ V_m \end{pmatrix} \]

On a line going from boundary to interior of attacked zone reported current will be wrong because voltage at boundary bus is changing with our defense but voltage at interior bus is changing by very small amounts.
Defense, 2: \[
\begin{pmatrix}
I_{km} \\
I_{mk}
\end{pmatrix}
= Y_{km} \begin{pmatrix}
V_k \\
V_m
\end{pmatrix}
\]

On a line going from boundary to interior of attacked zone **reported** current will be wrong

because voltage at boundary bus is changing with our defense

but voltage at interior bus is changing by very small amounts

In above example, **one** iteration identifies all boundary lines with **no** false positives
<table>
<thead>
<tr>
<th></th>
<th>Experiment 1</th>
<th>Experiment 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sum_{j \in G} \delta_j^+$</td>
<td>289.01</td>
<td>964.77</td>
</tr>
<tr>
<td>$\sum_{j \in G} \delta_j^-$</td>
<td>174.47</td>
<td>256.04</td>
</tr>
</tbody>
</table>

Branch ($k = 1137, m = 1139$)

1137 inside attack, 1139 on boundary

|                     | $V_{1137}^R(0)|\angle \theta_{1137}^R(0)$ | $V_{1139}^R(0)|\angle \theta_{1139}^R(0)$ | $V_{1139}^R(t)|\angle \theta_{1139}^R(t)$ |
|---------------------|-------------------------------------------------|-------------------------------------------------|-------------------------------------------------|
|                     | 1.0919 $\angle - 6.993^\circ$                   | 1.0919 $\angle - 6.991^\circ$                   | 1.0105 $\angle - 7.882^\circ$                   |
|                     | 1.0919 $\angle - 6.991^\circ$                   | 1.0919 $\angle - 6.991^\circ$                   | 1.0187 $\angle - 7.936^\circ$                   |

<table>
<thead>
<tr>
<th></th>
<th>$I_{1137,1139}^R(0)$</th>
<th>$Y_{1137,1139}^R\left(\frac{V_{1137}^R(0)}{V_{1139}^R(t)}\right)$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$-0.0275 + 0.0281j$</td>
<td>$20.967 - 55.978j$</td>
</tr>
<tr>
<td></td>
<td>$-0.0275 + 0.0281j$</td>
<td>$21.435 - 49.918j$</td>
</tr>
</tbody>
</table>
Non-static attack: follow-up

“Noisy-data” attack

Following the attack, for any bus $\in A - \partial A$ the attacker reports (at each time $t$) a complex voltage value

$$\tilde{V}_k(t) = V^R_k + \nu_k(t)$$

Here, $\nu_k(t)$ is random, with

$$E(\nu_k(t)) = 0,$$
Non-static attack: follow-up

“Noisy-data” attack

Following the attack, for any bus $\in A - \partial A$ the attacker reports (at each time $t$) a complex voltage value

$$\tilde{V}_k(t) = V_k^R + \nu_k(t)$$

Here, $\nu_k(t)$ is random, with

$$E(\nu_k(t)) = 0,$$

(consistent with zero expected load change)
Non-static attack: follow-up

“Noisy-data” attack

Following the attack, for any bus $\in A - \partial A$ the attacker reports (at each time $t$) a complex voltage value

$$\tilde{V}_k(t) = V_k^R + \nu_k(t)$$

Here, $\nu_k(t)$ is random, with

$$E(\nu_k(t)) = 0,$$

(consistent with zero expected load change)

and?
Non-static attack: follow-up

“Noisy-data” attack

Following the attack, for any bus \( \in A - \partial A \) the attacker reports (at each time \( t \)) a complex voltage value

\[
\tilde{V}_k(t) = V_k^R + \nu_k(t)
\]

Here, \( \nu_k(t) \) is random, with

\[
E(\nu_k(t)) = 0,
\]

(consistent with zero expected load change)

and? what else?
Non-static attack: follow-up

“Noisy-data” attack

Following the attack, for any bus $b \in A - \partial A$ the attacker reports (at each time $t$) a complex voltage value

$$\tilde{V}_k(t) = V_k^R + \nu_k(t)$$

Here, $\nu_k(t)$ is random, with

$$E(\nu_k(t)) = 0,$$

(consistent with zero expected load change)

and? what else?

→ stochastics of $\nu_k(t)$ should “make sense”
We have data from an industrial partner:

- 240 PMUs
- 2 years of reported data
- 28 TB
- Soon, 500 PMUs and higher detail
Moving Average of Voltage Angle for bus 6
More PMU fun: a voltage phase angle
More PMU fun: 3 voltage angles)
More PMU fun: difference between two voltage angles (10 seconds)
More PMU fun: frequency at two different buses
Noise is not just noise

From real time series, voltage angle deviation histogram

Kolmogorov-Smirnoff gaussianity test strongly rejected, always
Noise is not just noise

From real time series, voltage magnitude deviations

Strong and nontrivial correlation structure
Covariances matrices of PMU data have **low rank!!**
Covariances matrices of PMU data have **low rank!!**

**Example: 50 PMUs, Voltage Angle, one minute**

<table>
<thead>
<tr>
<th></th>
<th>Scaled Eigenvalue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.000</td>
</tr>
<tr>
<td>2</td>
<td>0.078</td>
</tr>
<tr>
<td>3</td>
<td>0.012</td>
</tr>
<tr>
<td>4</td>
<td>0.009</td>
</tr>
<tr>
<td>5</td>
<td>0.007</td>
</tr>
<tr>
<td>6</td>
<td>0.004</td>
</tr>
<tr>
<td>7</td>
<td>0.003</td>
</tr>
<tr>
<td>8</td>
<td>0.002</td>
</tr>
<tr>
<td>9</td>
<td>0.001</td>
</tr>
<tr>
<td>10</td>
<td>0.001</td>
</tr>
</tbody>
</table>
Covariances matrices of PMU data have **low rank!!**

<table>
<thead>
<tr>
<th>Scaled Eigenvalue</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.000</td>
</tr>
<tr>
<td>2</td>
<td>0.618</td>
</tr>
<tr>
<td>3</td>
<td>0.061</td>
</tr>
<tr>
<td>4</td>
<td>0.023</td>
</tr>
<tr>
<td>5</td>
<td>0.017</td>
</tr>
<tr>
<td>6</td>
<td>0.010</td>
</tr>
<tr>
<td>7</td>
<td>0.008</td>
</tr>
<tr>
<td>8</td>
<td>0.004</td>
</tr>
<tr>
<td>9</td>
<td>0.003</td>
</tr>
<tr>
<td>10</td>
<td>0.002</td>
</tr>
</tbody>
</table>
Covariances matrices of PMU data have **low rank!!**

**Example: 100 PMUs, voltage magnitude, five minutes**

<table>
<thead>
<tr>
<th></th>
<th>Scaled Eigenvalue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.000</td>
</tr>
<tr>
<td>2</td>
<td>0.618</td>
</tr>
<tr>
<td>3</td>
<td>0.061</td>
</tr>
<tr>
<td>4</td>
<td>0.023</td>
</tr>
<tr>
<td>5</td>
<td>0.017</td>
</tr>
<tr>
<td>6</td>
<td>0.010</td>
</tr>
<tr>
<td>7</td>
<td>0.008</td>
</tr>
<tr>
<td>8</td>
<td>0.004</td>
</tr>
<tr>
<td>9</td>
<td>0.004</td>
</tr>
<tr>
<td>10</td>
<td>0.002</td>
</tr>
</tbody>
</table>
Non-static attack: follow-up

“Noisy-data” attack

Following the attack, for any bus $k \in \mathcal{A} \setminus \partial \mathcal{A}$ the attacker reports (at each time $t$) a complex voltage value

$$\tilde{V}_k^R(t) = V_k^R + \nu_k(t)$$

Here, $\nu_k(t)$ is random, with

$$E(\nu_k(t)) = 0,$$
Non-static attack: follow-up

“Noisy-data” attack

Following the attack, for any bus $k \in A - \partial A$ the attacker reports (at each time $t$) a complex voltage value

$$\tilde{V}_k^R(t) = V_k^R + \nu_k(t)$$

Here, $\nu_k(t)$ is random, with

$$E(\nu_k(t)) = 0,$$

(consistent with zero expected load change)
Non-static attack: follow-up

“Noisy-data” attack

Following the attack, for any bus $k \in A - \partial A$ the attacker reports (at each time $t$) a complex voltage value

$$\tilde{V}_k^R(t) = V_k^R + \nu_k(t)$$

Here, $\nu_k(t)$ is random, with

$$\mathbb{E}(\nu_k(t)) = 0,$$

(consistent with zero expected load change)

and?

Bienstock, Escobar, Shukla (Columbia)
Non-static attack: follow-up

“Noisy-data” attack

Following the attack, for any bus $k \in \mathcal{A} - \partial \mathcal{A}$ the attacker reports (at each time $t$) a complex voltage value

$$\tilde{V}^R_k(t) = V^R_k + \nu_k(t)$$

Here, $\nu_k(t)$ is random, with

$$\mathbb{E}(\nu_k(t)) = 0,$$

(consistent with zero expected load change)

and? what else?
Non-static attack: follow-up

“Noisy-data” attack

Following the attack, for any bus $k \in A - \partial A$ the attacker reports (at each time $t$) a complex voltage value

$$\tilde{V}_k^R(t) = V_k^R + \nu_k(t)$$

Here, $\nu_k(t)$ is random, with

$$E(\nu_k(t)) = 0,$$

(consistent with zero expected load change)

and? what else?

→ covariance of $\nu(t)$ should be make sense
Learning variances

**Theorem.** (Co)variance of time series can be learned

- In real time
- In streaming fashion
- Under evolving stochasticity

Shukla, Yun and a fool from Columbia:

Covariance defense

- Under **whatever** assumptions, the attacker will produce a time series for e.g. phase angles.
Covariance defense

- Under \textbf{whatever} assumptions, the attacker will produce a time series for e.g. phase angles.
- Assume covariance of phase angles is learned by the defender.
Covariance defense

- Under *whatever* assumptions, the attacker will produce a time series for e.g. phase angles.
- Assume covariance of phase angles is learned by the defender
- (Assume of low rank)
Covariance defense

- Under **whatever** assumptions, the attacker will produce a time series for e.g. phase angles.
- Assume covariance of phase angles is learned by the defender
- (Assume of low rank)
- Defender chooses **random generator injections** so as to **significantly change covariance of phase angles**
Covariance defense

- Under *whatever* assumptions, the attacker will produce a time series for e.g. phase angles.

- Assume covariance of phase angles is learned by the defender

- (Assume of low rank)

- Defender chooses *random generator injections* so as to *significantly change covariance of phase angles*

- Attacker is caught with pants down
Covariance defense (technical, abridged)

- Let $\Omega =$ covariance of **observed** voltage phase angles

Theorem: there is a random set of power injections (by generators) that results in covariance of phase angles $\approx \Omega + \lambda v v^T$ where $\lambda > 0$.
Covariance defense (technical, abridged)

- Let $\Omega$ = covariance of observed voltage phase angles

- Let $w_1, w_2, \ldots, w_r$ = eigenvectors with positive large enough eigenvalues.

Theorem: there is a random set of power injections (by generators) that results in covariance of phase angles $\approx \Omega + \lambda vv^T$ where $\lambda > 0$.
Covariance defense (technical, abridged)

- Let $\Omega = \text{covariance of observed voltage phase angles}$

- Let $w_1, w_2, \ldots, w_r = \text{eigenvectors with positive large enough eigenvalues. } r \ll n \text{ (number of buses)}$
Covariance defense (technical, abridged)

- Let $\Omega = \text{covariance of observed voltage phase angles}$
- Let $w_1, w_2, \ldots, w_r = \text{eigenvectors with positive large enough eigenvalues}$. $r \ll n$ (number of buses)
- Defender chooses vector $v \in \mathbb{R}^n$ with:
  \[ w_i^T v = 0 \text{ for } 1 \leq i \leq r \] (plus other conditions)

Theorem: there is a random set of power injections (by generators) that results in covariance of phase angles $\approx \Omega + \lambda vv^T$ where $\lambda > 0$
Covariance defense (technical, abridged)

- Let $\Omega =$ covariance of observed voltage phase angles
- Let $w_1, w_2, \ldots, w_r =$ eigenvectors with positive large enough eigenvalues. $r \ll n$ (number of buses)
- Defender chooses vector $v \in \mathbb{R}^n$ with:
  \[ w_i^T v = 0 \] for $1 \leq i \leq r$ (plus other conditions)
- **Theorem:** there is a random set of power injections (by generators) that results in covariance of phase angles
  \[ \approx \Omega + \lambda vv^T \]
Covariance defense (technical, abridged)

- Let $\Omega = \text{covariance of observed voltage phase angles}$

- Let $w_1, w_2, \ldots, w_r = \text{eigenvectors with positive large enough eigenvalues}$. $r \ll n$ (number of buses)

- Defender chooses vector $v \in \mathbb{R}^n$ with:
  
  \[ w_i^T v = 0 \quad \text{for} \quad 1 \leq i \leq r \quad (\text{plus other conditions}) \]

- **Theorem**: there is a random set of power injections (by generators) that results in covariance of phase angles
  
  \[ \approx \Omega + \lambda v v^T \quad \text{where} \quad \lambda > 0 \]
Covariance defense (technical, abridged)

- Let $\Omega =$ covariance of observed voltage phase angles

- Let $w_1, w_2, \ldots, w_r =$ eigenvectors with positive large enough eigenvalues. $r \ll n$ (number of buses)

- Defender chooses vector $v \in \mathbb{R}^n$ with:

  \[ w_i^T v = 0 \text{ for } 1 \leq i \leq r \] (plus other conditions)

- **Theorem:** there is a random set of power injections (by generators) that results in covariance of phase angles

  \[ \approx \Omega + \lambda vv^T \text{ where } \lambda > 0 \]

- On case2746wp, $\approx 10$ vectors $v$ cover all buses.
  (Dense null space vector computation: LP heuristic)
Let \( \Omega \) = covariance of observed voltage phase angles

Let \( w_1, w_2, \ldots, w_r \) = eigenvectors with positive large enough eigenvalues.
Covariance defense (technical, less abridged)

1. Let $\Omega = \text{covariance of observed voltage phase angles}$

2. Let $w_1, w_2, \ldots, w_r = \text{eigenvectors with positive large enough eigenvalues. } r \ll n \text{ (number of buses)}$

3. Defender chooses vector $v \in \mathbb{R}^n$ with:
   \[ w_i^T v = 0 \text{ for } 1 \leq i \leq r \text{ and } [Bv]_i = 0 \text{ for all non-generator } i \]

4. **Theorem:** there is a random set of power injections (by generators) that results in covariance of phase angles
   \[ \approx \Omega + \lambda vv^T \]
Covariance defense (technical, less abridged)

1. Let $\Omega = \text{covariance of observed voltage phase angles}$

2. Let $w_1, w_2, \ldots, w_r = \text{eigenvectors with positive large enough eigenvalues. } r \ll n \text{ (number of buses)}$

3. Defender chooses vector $v \in \mathbb{R}^n$ with:
   
   $w_i^T v = 0 \text{ for } 1 \leq i \leq r \text{ and } [Bv]_i = 0 \text{ for all non-generator } i$

4. **Theorem:** there is a random set of power injections (by generators) that results in covariance of phase angles
   
   $\approx \Omega + \lambda vv^T \text{ where } \lambda > 0$

5. On case2746wp, there is a single vector $v$ that covers all buses.
Let $\Omega = \text{covariance of observed voltage phase angles}$

Let $w_1, w_2, \ldots, w_r = \text{eigenvectors with positive large enough eigenvalues. } r \ll n \text{ (number of buses)}$

Defender chooses vector $v \in \mathbb{R}^n$ with:

$$w_i^T v = 0 \text{ for } 1 \leq i \leq r \text{ and } [Bv]_i = 0 \text{ for all non-generator } i$$

Theorem: there is a random set of power injections (by generators) that results in covariance of phase angles

$$\approx \Omega + \lambda vv^T \text{ where } \lambda > 0$$

On case2746wp, there is a single vector $v$ that covers all buses.

Theorem: if $v^1, v^2 \in \text{subspace } S$, then $\exists \infty \text{ many } v \in S \text{ with}$

$$\text{support}(v) = \text{support}(v^1) \cup \text{support}(v^2)$$
Summary

- Very high-fidelity grid attacks appear easily computable.

- Defensive idea 1: use network resources to change power flow physics in unpredictable ways

- Defensive idea 2: change covariance structure in a way that cannot be instantaneously learned
Summary

- Very high-fidelity grid attacks appear easily computable.

- Defensive idea 1: use network resources to change power flow physics in unpredictable ways

- Defensive idea 2: change covariance structure in a way that cannot be instantaneously learned

- Adversarial learning of moments under streaming data is a nice problem!

Wed.Aug.15.113946.2018@blacknwhite