Differentially Private Optimal Power Flow for Distribution Grids

Vladimir Dvorkin[†‡] Ferdinando Fioretto[§‡] Pascal Van Hentenryck[‡]

Pierre Pinson[†] Jalal Kazempour[†]

[†]Technical University of Denmark

[§]Syracuse University

[‡]Georgia Institute of Technology

vladvo@elektro.dtu.dk

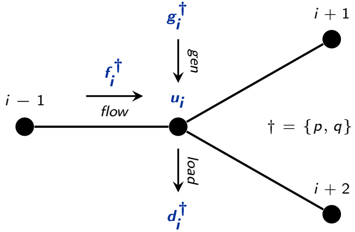
INFORMS, November 2020

Some background

- Growing distribution grid digitalization
  - From analog to digital grid operations
  - New customer engagement and interaction
  - Data is at the core of new business models
- How to utilize data without exposing its sensitive attributed?
  - Increasing responsibility for a grid data utilization
  - Ethics of data curation and utilization
- Real-time surveillance through power grid measurements
- Privacy regulation (GDPR, NYPA, CCPA) is not always a solution

Privacy breaches in distribution OPF

- Distribution grid topology:



- Distribution AC optimal power flow:
  - Minimize total dispatch cost
  - Subject to OPF equations:

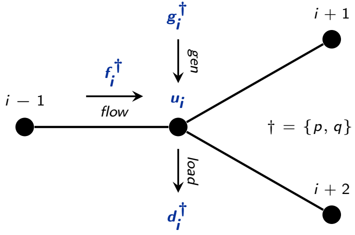
$$\boldsymbol{f_i^\dagger} = \boldsymbol{d_i^\dagger} - \boldsymbol{g_i^\dagger} + \sum_{\ell \in \mathcal{D}_i} f_\ell^\dagger, \quad \forall \ell \in \mathcal{L}$$

$$\boldsymbol{u_i} = u_0 - 2 \sum_{\ell \in \mathcal{R}_i} (f_\ell^p r_\ell + f_\ell^q x_\ell), \quad \forall i \in \mathcal{N}$$

  - ... and flow, generation, and voltage limits

Privacy breaches in distribution OPF

- Distribution grid topology:



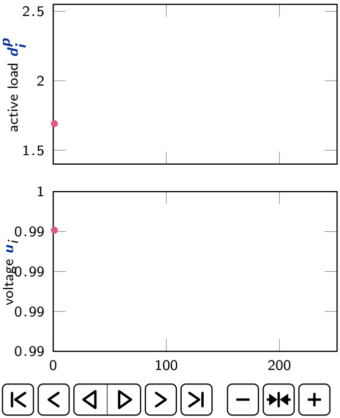
- Distribution AC optimal power flow:
  - Minimize total dispatch cost
  - Subject to OPF equations:

$$f_i^\dagger = d_i^\dagger - g_i^\dagger + \sum_{\ell \in \mathcal{D}_i} f_\ell^\dagger, \quad \forall \ell \in \mathcal{L}$$

$$u_i = u_0 - 2 \sum_{\ell \in \mathcal{R}_i} (f_\ell^p r_\ell + f_\ell^q x_\ell), \quad \forall i \in \mathcal{N}$$

  - ... and flow, generation, and voltage limits

- Loads leak through OPF measurements
- Customer at a terminal feeder node:



- Switching of electrical appliances
- Specific production patterns
- Technological breaches

OPF mechanism and differential privacy

- OPF problem as a mechanism

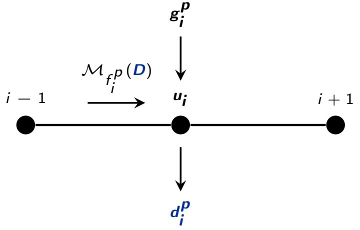
$$\mathcal{M} : \mathbb{R}^n \mapsto \mathbb{R}^m$$

  that maps load datasets to OPF solutions

- OPF solutions expose changes in loads. Two adjacent datasets $\boldsymbol{D}, \boldsymbol{D'} \in \mathbb{R}^n$:

$$\boldsymbol{D} = \{d_1^p, \dots, \boldsymbol{d_i^p}, \dots, d_n^p\}$$
$$\boldsymbol{D'} = \{d_1^p, \dots, \boldsymbol{d_i^{p'}}, \dots, d_n^p\}$$

- Active power flow as a function of the load



$$\mathcal{M}_{f_i^p}(\boldsymbol{D}) \neq \mathcal{M}_{f_i^p}(\boldsymbol{D'})$$

- Mechanism $\mathcal{M}_{f_i^p}$ is made diff. private by adding a random noise ξ to its output

- Formally, the privacy property is described as

$$\mathbb{P}_\xi[\mathcal{M}_{f_i^p}(D) + \xi \in \tilde{f}_i^p] \leqslant \mathbb{P}_\xi[\mathcal{M}_{f_i^p}(D') + \xi \in \tilde{f}_i^p]\exp(\varepsilon) + \delta$$

  where ε and δ are diff. privacy parameters

- Must hold for any pair D and D'

OPF mechanism and differential privacy

- OPF problem as a mechanism

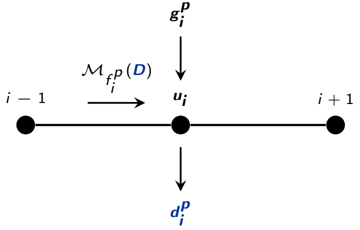
$$\mathcal{M} : \mathbb{R}^n \mapsto \mathbb{R}^m$$

that maps load datasets to OPF solutions

- OPF solutions expose changes in loads. Two adjacent datasets $\boldsymbol{D}, \boldsymbol{D}' \in \mathbb{R}^n$:

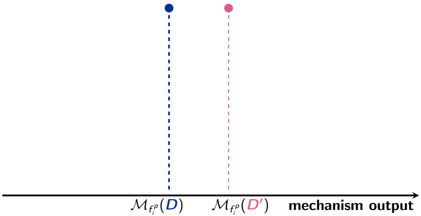
$$\boldsymbol{D} = \{d_1^p, \dots, \boldsymbol{d_i^p}, \dots, d_n^p\}$$
$$\boldsymbol{D}' = \{d_1^p, \dots, \boldsymbol{d_i^{p\prime}}, \dots, d_n^p\}$$

- Active power flow as a function of the load



$$\mathcal{M}_{f_i^p}(\boldsymbol{D}) \neq \mathcal{M}_{f_i^p}(\boldsymbol{D}')$$

- Mechanism $\mathcal{M}_{f_i^p}$ is made diff. private by adding a random noise $\boldsymbol{\xi}$ to its output



- Formally, the privacy property is described as

$$\mathbb{P}_{\xi}[\mathcal{M}_{f_i^p}(\boldsymbol{D}) + \boldsymbol{\xi} \in \tilde{\boldsymbol{f}}_i^p] \leqslant \mathbb{P}_{\xi}[\mathcal{M}_{f_i^p}(\boldsymbol{D}') + \boldsymbol{\xi} \in \tilde{\boldsymbol{f}}_i^p]\exp(\varepsilon) + \delta$$

where ε and δ are diff. privacy parameters

- Must hold for any pair $\boldsymbol{D}$ and $\boldsymbol{D}'$

OPF mechanism and differential privacy

- OPF problem as a mechanism

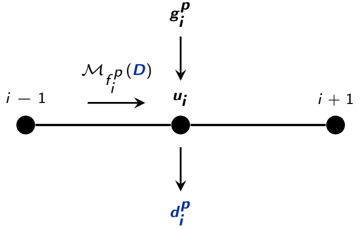
$$\mathcal{M} : \mathbb{R}^n \mapsto \mathbb{R}^m$$

that maps load datasets to OPF solutions

- OPF solutions expose changes in loads. Two adjacent datasets $\boldsymbol{D}, \boldsymbol{D'} \in \mathbb{R}^n$:

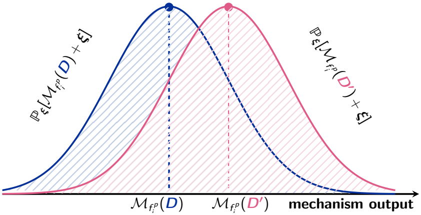
$$\boldsymbol{D} = \{d_1^p, \dots, \boldsymbol{d_i^p}, \dots, d_n^p\}$$
$$\boldsymbol{D'} = \{d_1^p, \dots, \boldsymbol{d_i^{p\prime}}, \dots, d_n^p\}$$

- Active power flow as a function of the load



$$\mathcal{M}_{f_i^p}(\boldsymbol{D}) \neq \mathcal{M}_{f_i^p}(\boldsymbol{D'})$$

- Mechanism $\mathcal{M}_{f_i^p}$ is made diff. private by adding a random noise $\boldsymbol{\xi}$ to its output



- Formally, the privacy property is described as

$$\mathbb{P}_{\xi}[\mathcal{M}_{f_i^p}(\boldsymbol{D}) + \boldsymbol{\xi} \in \tilde{\boldsymbol{f}}_i^p] \leqslant$$
$$\mathbb{P}_{\xi}[\mathcal{M}_{f_i^p}(\boldsymbol{D'}) + \boldsymbol{\xi} \in \tilde{\boldsymbol{f}}_i^p]\exp(\varepsilon) + \delta$$

where ε and δ are diff. privacy parameters

- Must hold for any pair $\boldsymbol{D}$ and $\boldsymbol{D'}$

OPF mechanism and differential privacy

- OPF problem as a mechanism

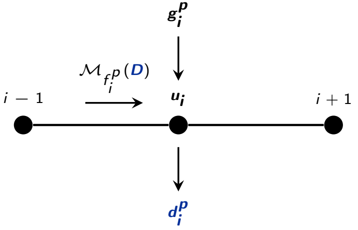
$$\mathcal{M} : \mathbb{R}^n \mapsto \mathbb{R}^m$$

  that maps load datasets to OPF solutions

- OPF solutions expose changes in loads. Two adjacent datasets $\boldsymbol{D}, \boldsymbol{D'} \in \mathbb{R}^n$:

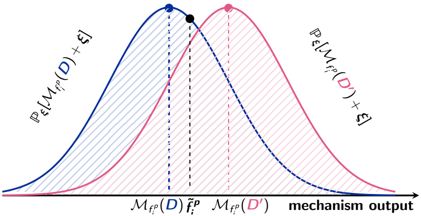
$$\boldsymbol{D} = \{d_1^p, \dots, \boldsymbol{d_i^p}, \dots, d_n^p\}$$
$$\boldsymbol{D'} = \{d_1^p, \dots, \boldsymbol{d_i^{p'}}, \dots, d_n^p\}$$

- Active power flow as a function of the load



$$\mathcal{M}_{f_i^p}(\boldsymbol{D}) \neq \mathcal{M}_{f_i^p}(\boldsymbol{D'})$$

- Mechanism $\mathcal{M}_{f_i^p}$ is made diff. private by adding a random noise $\boldsymbol{\xi}$ to its output



- Formally, the privacy property is described as

$$\mathbb{P}_{\xi}[\mathcal{M}_{f_i^p}(\boldsymbol{D}) + \boldsymbol{\xi} \in \tilde{\boldsymbol{f}}_i^p] \leqslant$$
$$\mathbb{P}_{\xi}[\mathcal{M}_{f_i^p}(\boldsymbol{D'}) + \boldsymbol{\xi} \in \tilde{\boldsymbol{f}}_i^p]\exp(\varepsilon) + \delta$$

  where ε and δ are diff. privacy parameters

- Must hold for any pair $\boldsymbol{D}$ and $\boldsymbol{D'}$

OPF mechanism and differential privacy

- OPF problem as a mechanism

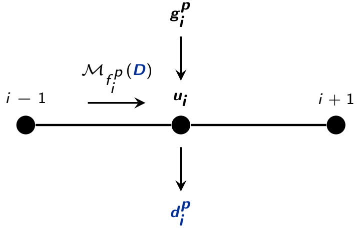
$$\mathcal{M} : \mathbb{R}^n \mapsto \mathbb{R}^m$$

  that maps load datasets to OPF solutions

- OPF solutions expose changes in loads. Two adjacent datasets $\boldsymbol{D}, \boldsymbol{D'} \in \mathbb{R}^n$:

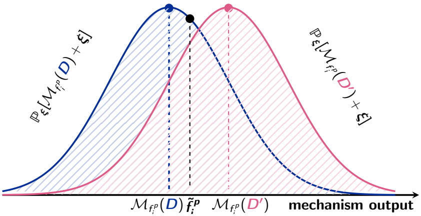
$$\boldsymbol{D} = \{d_1^p, \dots, \boldsymbol{d_i^p}, \dots, d_n^p\}$$
$$\boldsymbol{D'} = \{d_1^p, \dots, \boldsymbol{d_i^{p'}}, \dots, d_n^p\}$$

- Active power flow as a function of the load



$$\mathcal{M}_{f_i^p}(\boldsymbol{D}) \neq \mathcal{M}_{f_i^p}(\boldsymbol{D'})$$

- Mechanism $\mathcal{M}_{f_i^p}$ is made diff. private by adding a random noise $\boldsymbol{\xi}$ to its output



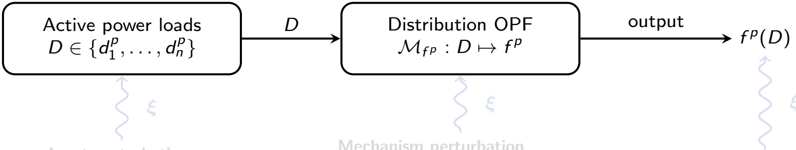
- Formally, the privacy property is described as

$$\mathbb{P}_{\boldsymbol{\xi}}[\mathcal{M}_{f_i^p}(\boldsymbol{D}) + \boldsymbol{\xi} \in \tilde{\boldsymbol{f}}_{\boldsymbol{i}}^{\boldsymbol{p}}] \leqslant$$
$$\mathbb{P}_{\boldsymbol{\xi}}[\mathcal{M}_{f_i^p}(\boldsymbol{D'}) + \boldsymbol{\xi} \in \tilde{\boldsymbol{f}}_{\boldsymbol{i}}^{\boldsymbol{p}}]\exp(\boldsymbol{\varepsilon}) + \boldsymbol{\delta}$$

  where $\boldsymbol{\varepsilon}$ and $\boldsymbol{\delta}$ are diff. privacy parameters

- Must hold for any pair $\boldsymbol{D}$ and $\boldsymbol{D'}$

Perturbation of the OPF solution



Input perturbation
- Post-proc. immunity
- OPF infeasibility

Mechanism perturbation
- Random solution at every run
- Feasibility is a design parameter
- Control of random OPF outcomes

Output perturbation
- OPF infeasibility

Mechanism perturbation example:

Grid is balanced if $\alpha_{i-1} = 1$ and $\alpha_{i+1} = -1$

- Randomized generator policy:

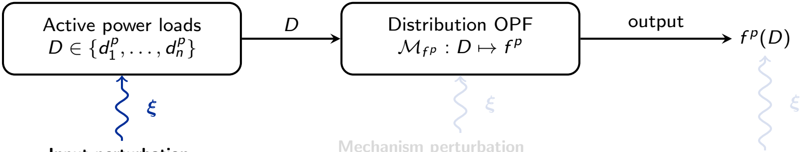
$$\tilde{g}_i^p(\xi) = \underbrace{g_i^p}_{\text{mean}} + \underbrace{(T_i \circ \alpha_i)\xi}_{\text{random component}}$$

$$\sum_{i \in \mathcal{U}_\ell} \alpha_{i\ell} = 1, \quad \sum_{i \in \mathcal{D}_\ell} \alpha_{i\ell} = 1, \; \forall \ell \in \mathcal{L},$$

- From AC-OPF equations, active power flow

$$\tilde{f}_\ell^p(\xi) = \underbrace{f_\ell^p}_{\text{mean}} + \underbrace{\left[T_i \circ \alpha_i + \sum_{j \in \mathcal{D}_\ell} T_j \circ \alpha_j\right]\xi}_{\text{random component}}$$

Perturbation of the OPF solution



Input perturbation

- Post-proc. immunity
- OPF infeasibility

Mechanism perturbation

- Random solution at every run
- Feasibility is a design parameter
- Control of random OPF outcomes

Output perturbation

- OPF infeasibility

Mechanism perturbation example:

Grid is balanced if $\alpha_{i-1} = 1$ and $\alpha_{i+1} = -1$

- Randomized generator policy:

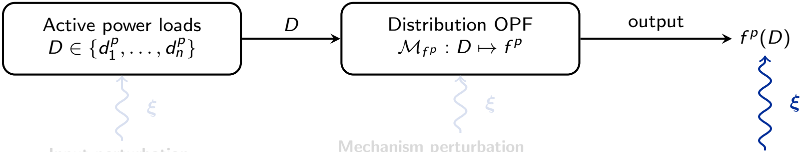
$$\tilde{g}_i^p(\xi) = \underbrace{g_i^p}_{\text{mean}} + \underbrace{(T_i \circ \alpha_i)\xi}_{\text{random component}}$$

$$\sum_{i\in\mathcal{U}_\ell} \alpha_{i\ell} = 1, \quad \sum_{i\in\mathcal{D}_\ell} \alpha_{i\ell} = 1, \; \forall \ell \in \mathcal{L},$$

- From AC-OPF equations, active power flow

$$\tilde{f}_\ell^p(\xi) = \underbrace{f_\ell^p}_{\text{mean}} + \underbrace{\Big[T_i \circ \alpha_i + \sum_{j\in\mathcal{D}_\ell} T_j \circ \alpha_j\Big]\xi}_{\text{random component}}$$

Perturbation of the OPF solution



Input perturbation
- Post-proc. immunity
- OPF infeasibility

Mechanism perturbation
- Random solution at every run
- Feasibility is a design parameter
- Control of random OPF outcomes

Output perturbation
- OPF infeasibility

Mechanism perturbation example:

Grid is balanced if $\alpha_{i-1} = 1$ and $\alpha_{i+1} = -1$

- Randomized generator policy:

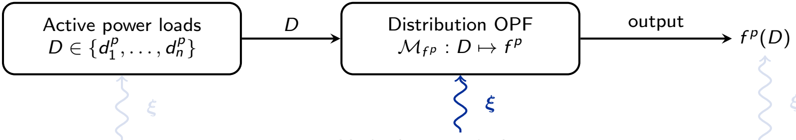
$$\tilde{g}_i^p(\xi) = \underbrace{g_i^p}_{\text{mean}} + \underbrace{(T_i \circ \alpha_i)\xi}_{\text{random component}}$$

$$\sum_{i \in \mathcal{U}_\ell} \alpha_{i\ell} = 1, \quad \sum_{i \in \mathcal{D}_\ell} \alpha_{i\ell} = 1, \ \forall \ell \in \mathcal{L},$$

- From AC-OPF equations, active power flow

$$\tilde{f}_\ell^p(\xi) = \underbrace{f_\ell^p}_{\text{mean}} + \underbrace{\Big[T_i \circ \alpha_i + \sum_{j \in \mathcal{D}_\ell} T_j \circ \alpha_j\Big]\xi}_{\text{random component}}$$

Perturbation of the OPF solution



Input perturbation

- Post-proc. immunity
- OPF infeasibility

Mechanism perturbation

- Random solution at every run
- Feasibility is a design parameter
- Control of random OPF outcomes

Output perturbation

- OPF infeasibility

Mechanism perturbation example:

Grid is balanced if $\alpha_{i-1} = 1$ and $\alpha_{i+1} = -1$

- Randomized generator policy:

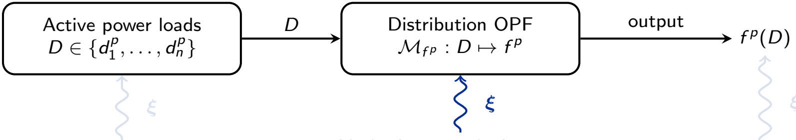
$$\tilde{g}_i^p(\xi) = \underbrace{g_i^p}_{\text{mean}} + \underbrace{(T_i \circ \alpha_i)\xi}_{\text{random component}}$$

$$\sum_{i \in \mathcal{U}_\ell} \alpha_{i\ell} = 1, \quad \sum_{i \in \mathcal{D}_\ell} \alpha_{i\ell} = 1, \ \forall \ell \in \mathcal{L},$$

- From AC-OPF equations, active power flow

$$\tilde{f}_\ell^p(\xi) = \underbrace{f_\ell^p}_{\text{mean}} + \underbrace{\Big[T_i \circ \alpha_i + \sum_{j \in \mathcal{D}_\ell} T_j \circ \alpha_j\Big]\xi}_{\text{random component}}$$

Perturbation of the OPF solution

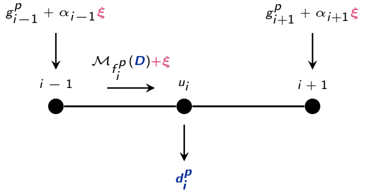


Input perturbation
- Post-proc. immunity
- OPF infeasibility

Mechanism perturbation
- Random solution at every run
- Feasibility is a design parameter
- Control of random OPF outcomes

Output perturbation
- OPF infeasibility

Mechanism perturbation example:



Grid is balanced if $\alpha_{i-1} = 1$ and $\alpha_{i+1} = -1$

- Randomized generator policy:

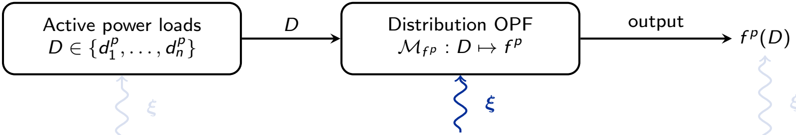
$$\tilde{g}_i^p(\xi) = \underbrace{g_i^p}_{\text{mean}} + \underbrace{(T_i \circ \alpha_i)\xi}_{\text{random component}}$$

$$\sum_{i \in \mathcal{U}_\ell} \alpha_{i\ell} = 1, \quad \sum_{i \in \mathcal{D}_\ell} \alpha_{i\ell} = 1, \ \forall \ell \in \mathcal{L},$$

- From AC-OPF equations, active power flow

$$\tilde{f}_\ell^p(\xi) = \underbrace{f_\ell^p}_{\text{mean}} + \underbrace{\Big[T_i \circ \alpha_i + \sum_{j \in \mathcal{D}_\ell} T_j \circ \alpha_j\Big]\xi}_{\text{random component}}$$

Perturbation of the OPF solution

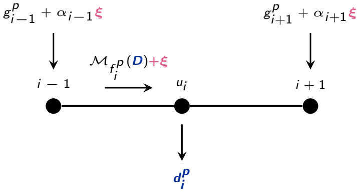


Input perturbation
- Post-proc. immunity
- OPF infeasibility

Mechanism perturbation
- Random solution at every run
- Feasibility is a design parameter
- Control of random OPF outcomes

Output perturbation
- OPF infeasibility

Mechanism perturbation example:



Grid is balanced if $\alpha_{i-1} = 1$ and $\alpha_{i+1} = -1$

- Randomized generator policy:

$$\tilde{g}_i^p(\xi) = \underbrace{g_i^p}_{\text{mean}} + \underbrace{(T_i \circ \alpha_i)\xi}_{\text{random component}}$$

$$\sum_{i \in \mathcal{U}_\ell} \alpha_{i\ell} = 1, \quad \sum_{i \in \mathcal{D}_\ell} \alpha_{i\ell} = 1, \; \forall \ell \in \mathcal{L},$$

- From AC-OPF equations, active power flow

$$\tilde{f}_\ell^p(\xi) = \underbrace{f_\ell^p}_{\text{mean}} + \underbrace{\Big[T_i \circ \alpha_i + \sum_{j \in \mathcal{D}_\ell} T_j \circ \alpha_j\Big]\xi}_{\text{random component}}$$

Differentially private distribution OPF mechanism (privacy)

- Any load $d_i^p \in D$ must be indistinguishable from any other load $d_i^{p\prime}$ for some $\boldsymbol{\beta_i} \geqslant 0$

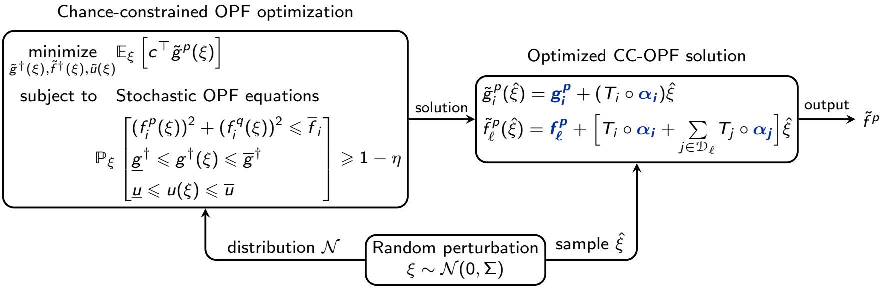
$$d_i^{p\prime} \in [d_i^p - \boldsymbol{\beta_i}; d_i^p + \boldsymbol{\beta_i}]$$

- Using the randomized generator policy, the private OPF mechanism $\tilde{\mathcal{M}}(D)$ is

- Any load $d_i^p \in D$ must be indistinguishable from any other load $d_i^{p\prime}$ for some $\boldsymbol{\beta_i} \geqslant 0$

$$d_i^{p\prime} \in [d_i^p - \boldsymbol{\beta_i}; d_i^p + \boldsymbol{\beta_i}]$$

- Using the randomized generator policy, the private OPF mechanism $\tilde{\mathcal{M}}(D)$ is



Differentially private distribution OPF mechanism (privacy)

- Any load $d_i^p \in D$ must be indistinguishable from any other load $d_i^{p\prime}$ for some $\boldsymbol{\beta_i} \geqslant 0$

$$d_i^{p\prime} \in [d_i^p - \boldsymbol{\beta_i}; d_i^p + \boldsymbol{\beta_i}]$$

- Using the randomized generator policy, the private OPF mechanism $\tilde{\mathcal{M}}(D)$ is

Chance-constrained OPF optimization

$$\underset{\tilde{g}^\dagger(\xi),\tilde{f}^\dagger(\xi),\tilde{u}(\xi)}{\text{minimize}} \quad \mathbb{E}_\xi \left[c^\top \tilde{g}^p(\xi)\right]$$

subject to Stochastic OPF equations

$$\mathbb{P}_\xi \begin{bmatrix} (f_i^p(\xi))^2 + (f_i^q(\xi))^2 \leqslant \overline{f}_i \\ \underline{g}^\dagger \leqslant g^\dagger(\xi) \leqslant \overline{g}^\dagger \\ \underline{u} \leqslant u(\xi) \leqslant \overline{u} \end{bmatrix} \geqslant 1 - \eta$$

solution →

Optimized CC-OPF solution

$$\tilde{g}_i^p(\hat{\xi}) = \boldsymbol{g_i^p} + (T_i \circ \boldsymbol{\alpha_i})\hat{\xi}$$

$$\tilde{f}_\ell^p(\hat{\xi}) = \boldsymbol{f_\ell^p} + \Big[T_i \circ \boldsymbol{\alpha_i} + \sum_{j\in\mathcal{D}_\ell} T_j \circ \boldsymbol{\alpha_j}\Big]\hat{\xi}$$

output → $\tilde{f}^p$

Random perturbation $\xi \sim \mathcal{N}(0, \Sigma)$

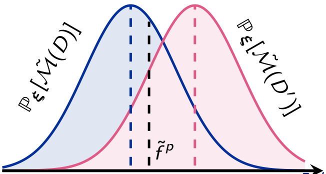
distribution $\mathcal{N}$ (to the optimization); sample $\hat{\xi}$ (to the solution)

(ε, δ)−differential distribution OPF privacy

Let $\xi_i \in \mathcal{N}(0, \sigma_i)$ and $\sigma_i \geqslant \boldsymbol{\beta_i}\sqrt{2\ln(1.25/\boldsymbol{\delta})}/\boldsymbol{\varepsilon}$, $\forall i \in \mathcal{L}$. Then, for β-adjacent load datasets D and D' :

$$\mathbb{P}[\tilde{\mathcal{M}}(D) \in \tilde{f}^p] \leqslant \exp(\boldsymbol{\varepsilon})\mathbb{P}[\tilde{\mathcal{M}}(D') \in \tilde{f}^p] + \boldsymbol{\delta},$$

where $\mathbb{P}$ is the probability over runs of $\tilde{\mathcal{M}}$.

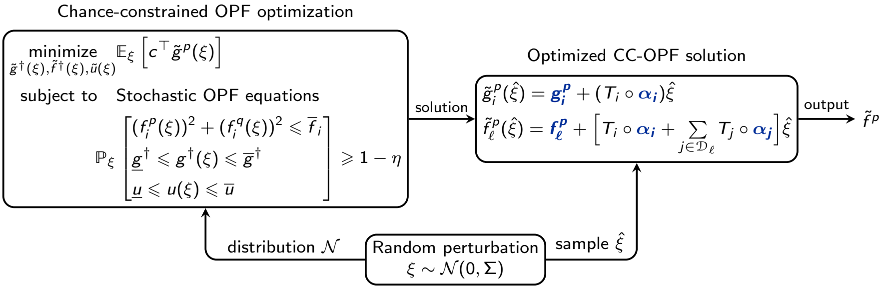


Differentially private distribution OPF mechanism (privacy)

- Any load $d_i^p \in D$ must be indistinguishable from any other load $d_i^{p\prime}$ for some $\boldsymbol{\beta_i} \geqslant 0$

$$d_i^{p\prime} \in [d_i^p - \boldsymbol{\beta_i}; d_i^p + \boldsymbol{\beta_i}]$$

- Using the randomized generator policy, the private OPF mechanism $\tilde{\mathcal{M}}(D)$ is

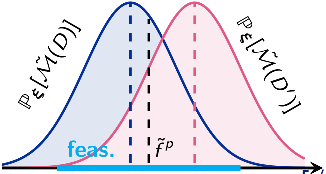


$(\varepsilon, \delta)-$differential distribution OPF privacy

Let $\xi_i \in \mathcal{N}(0, \sigma_i)$ and $\sigma_i \geqslant \boldsymbol{\beta_i}\sqrt{2\ln(1.25/\boldsymbol{\delta})}/\boldsymbol{\varepsilon}$, $\forall i \in \mathcal{L}$.
Then, for β-adjacent load datasets D and D' :

$$\mathbb{P}[\tilde{\mathcal{M}}(D) \in \tilde{f}^p] \leqslant \exp(\boldsymbol{\varepsilon})\mathbb{P}[\tilde{\mathcal{M}}(D') \in \tilde{f}^p] + \boldsymbol{\delta},$$

where $\mathbb{P}$ is the probability over runs of $\tilde{\mathcal{M}}$.

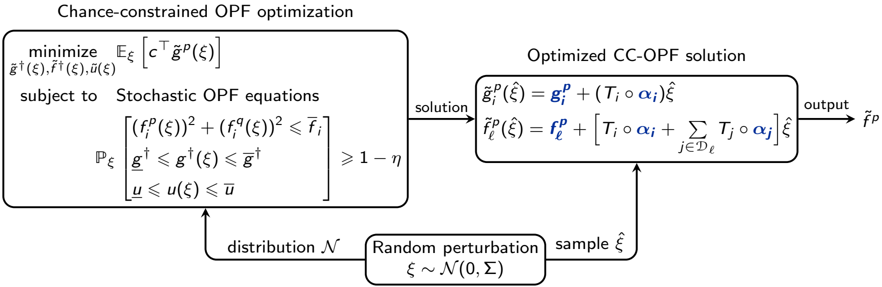


Differentially private distribution OPF mechanism (feasibility)

- Any load $d_i^p \in D$ must be indistinguishable from any other load $d_i^{p\prime}$ for some $\boldsymbol{\beta_i} \geqslant 0$

$$d_i^{p\prime} \in [d_i^p - \boldsymbol{\beta_i}; d_i^p + \boldsymbol{\beta_i}]$$

- Using the randomized generator policy, the private OPF mechanism $\tilde{\mathcal{M}}(D)$ is

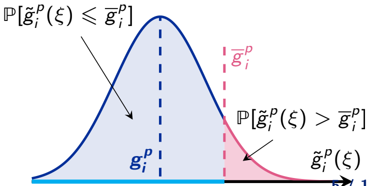


Feasibility of distribution OPF mechanism

$$\mathbb{P}_\xi[\boldsymbol{g_i^p} + (T_i \circ \boldsymbol{\alpha_i})\xi \leqslant \overline{g}_i^p] \geqslant 1 - \hat{\eta}_i \quad \Longleftrightarrow$$

$$\boldsymbol{g_i^p} \leqslant \overline{g}_i^p - \text{CDF}_{\mathcal{N}}^{-1}(1 - \hat{\eta}_i)\|\Sigma^{\frac{1}{2}}(T_i \circ \boldsymbol{\alpha_i})\|_2$$

Joint constraint satisfaction if $\sum_i \hat{\eta}_i \leqslant \eta$

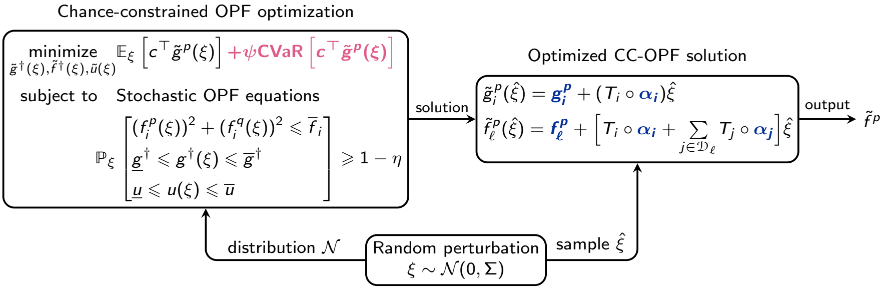


Differentially private distribution OPF mechanism (optimality loss)

- Any load $d_i^p \in D$ must be indistinguishable from any other load $d_i^{p\prime}$ for some $\boldsymbol{\beta_i} \geqslant 0$

$$d_i^{p\prime} \in [d_i^p - \boldsymbol{\beta_i}; d_i^p + \boldsymbol{\beta_i}]$$

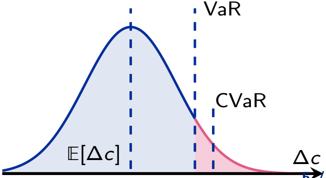
- Using the randomized generator policy, the private OPF mechanism $\tilde{\mathcal{M}}(D)$ is



- Noise induces the **optimality loss**
- CC-OPF optimizes the exp. optimality loss:

$$\Delta c = \|\tilde{\mathcal{M}}_{\text{obj}}(D) - \mathcal{M}_{\text{obj}}(D)\|_2$$

- Expected optimality loss versus CVaR ($\psi > 0$)

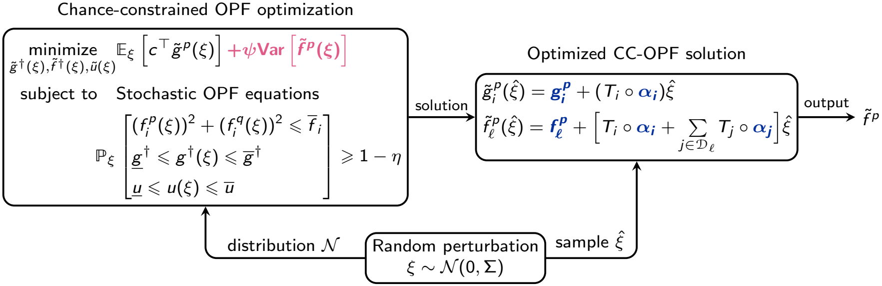


Differentially private distribution OPF mechanism (OPF variance)

- Any load $d_i^p \in D$ must be indistinguishable from any other load $d_i^{p\prime}$ for some $\boldsymbol{\beta_i} \geqslant 0$

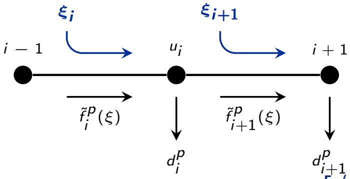
$$d_i^{p\prime} \in [d_i^p - \boldsymbol{\beta_i}; d_i^p + \boldsymbol{\beta_i}]$$

- Using the randomized generator policy, the private OPF mechanism $\tilde{\mathcal{M}}(D)$ is



- Since the network graph is connected

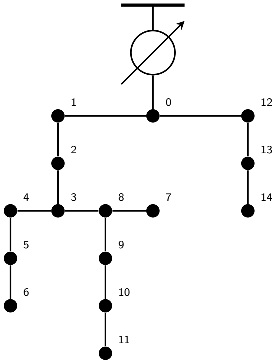
$$\text{Var}[\tilde{f}_i^p(\boldsymbol{\xi})] \geqslant \text{Var}[\boldsymbol{\xi_i}],\ \text{Var}[\tilde{f}_{i+1}^p(\boldsymbol{\xi})] \geqslant \text{Var}[\boldsymbol{\xi_{i+1}}]$$



- Independent perturbations accumulate **OPF variance**
- OPF variance (flow, voltage, generation) can be penalized in objective function for some factor $\psi > 0$

Experiments: network description

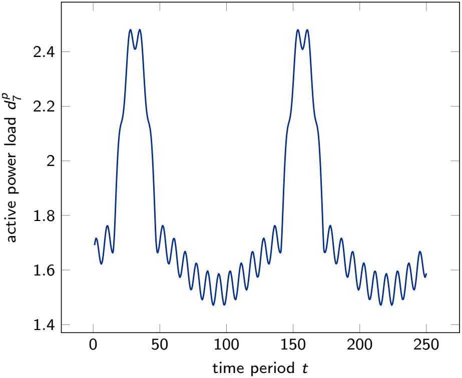
- 15-node radial distribution network
- 14 customers with DER, 1 substation
- Full grid observability (requires many perturbations)
- Full data and codes are available on `GitHub`



Experiments: illustrative example

- Customer at node 7 with a load pattern

$$\max\left\{\sin\tfrac{5}{10^2}t,\,\tfrac{7}{10}\right\}+\tfrac{5}{10^2}\sin\tfrac{5}{10^2}t+\tfrac{25}{10^3}\sin\tfrac{75}{10^2}t$$



Experiments: illustrative example

- Customer at node 7 with a load pattern

$$\max\left\{\sin\frac{5}{10^2}t, \frac{7}{10}\right\} + \frac{5}{10^2}\sin\frac{5}{10^2}t + \frac{25}{10^3}\sin\frac{75}{10^2}t$$

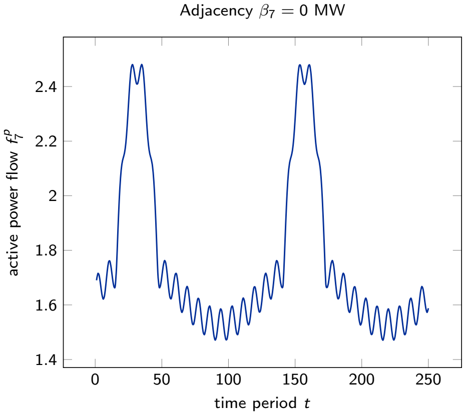
- The goal is to obfuscate this load pattern in power flow and voltage readings
- d_7^p must me indistinguishable from any $d_7^{p'} \in [d_7^p - \beta_7; d_7^p + \beta_7]$, for some $\beta_7 \in \mathbb{R}_+$

Experiments: illustrative example

- Customer at node 7 with a load pattern

$$\max\left\{\sin\frac{5}{10^2}t, \frac{7}{10}\right\} + \frac{5}{10^2}\sin\frac{5}{10^2}t + \frac{25}{10^3}\sin\frac{75}{10^2}t$$

- The goal is to obfuscate this load pattern in power flow and voltage readings
- d_7^p must me indistinguishable from any $d_7^{p'} \in [d_7^p - \beta_7; d_7^p + \beta_7]$, for some $\beta_7 \in \mathbb{R}_+$



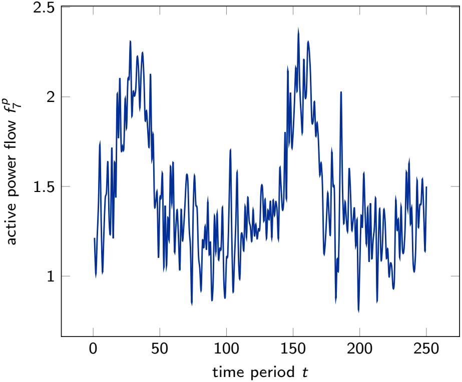
Experiments: illustrative example

- Customer at node 7 with a load pattern

$$\max\left\{\sin\frac{5}{10^2}t, \frac{7}{10}\right\} + \frac{5}{10^2}\sin\frac{5}{10^2}t + \frac{25}{10^3}\sin\frac{75}{10^2}t$$

- The goal is to obfuscate this load pattern in power flow and voltage readings
- d_7^p must me indistinguishable from any $d_7^{p'} \in [d_7^p - \beta_7; d_7^p + \beta_7]$, for some $\beta_7 \in \mathbb{R}_+$

Adjacency $\beta_7 = 0.07$ MW

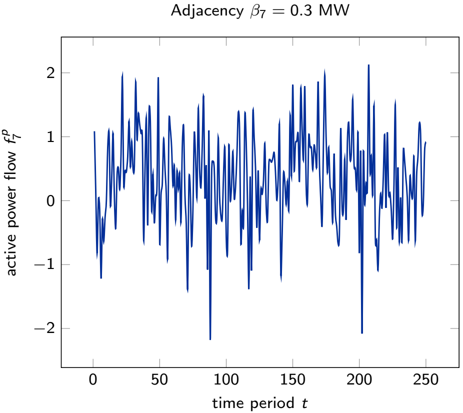


Experiments: illustrative example

- Customer at node 7 with a load pattern

$$\max\left\{\sin \tfrac{5}{10^2}t, \tfrac{7}{10}\right\} + \tfrac{5}{10^2}\sin \tfrac{5}{10^2}t + \tfrac{25}{10^3}\sin \tfrac{75}{10^2}t$$

- The goal is to obfuscate this load pattern in power flow and voltage readings
- d_7^p must me indistinguishable from any $d_7^{p'} \in [d_7^p - \beta_7; d_7^p + \beta_7]$, for some $\beta_7 \in \mathbb{R}_+$

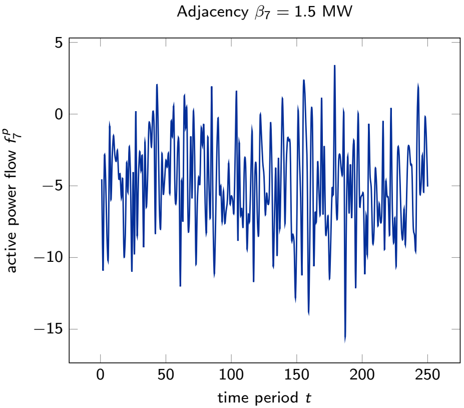


Experiments: illustrative example

- Customer at node 7 with a load pattern

$$\max\left\{\sin \tfrac{5}{10^2}t, \tfrac{7}{10}\right\} + \tfrac{5}{10^2}\sin \tfrac{5}{10^2}t + \tfrac{25}{10^3}\sin \tfrac{75}{10^2}t$$

- The goal is to obfuscate this load pattern in power flow and voltage readings
- d_7^p must me indistinguishable from any $d_7^{p'} \in [d_7^p - \beta_7; d_7^p + \beta_7]$, for some $\beta_7 \in \mathbb{R}_+$

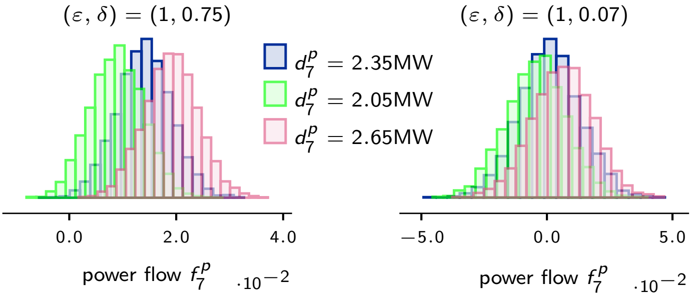


Experiments: illustrative example

- Customer at node 7 with a load pattern

$$\max\left\{\sin\frac{5}{10^2}t,\frac{7}{10}\right\}+\frac{5}{10^2}\sin\frac{5}{10^2}t+\frac{25}{10^3}\sin\frac{75}{10^2}t$$

- The goal is to obfuscate this load pattern in power flow and voltage readings
- d_7^p must me indistinguishable from any $d_7^{p'}\in[d_7^p-\beta_7;d_7^p+\beta_7]$, for some $\beta_7\in\mathbb{R}_+$



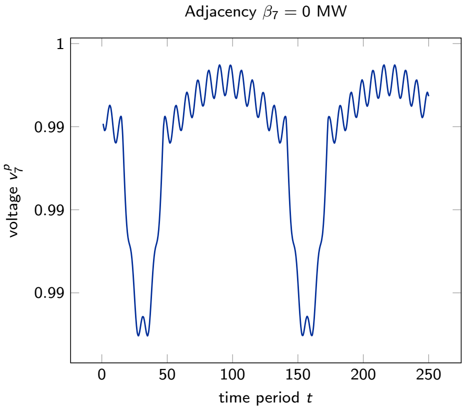
- The mechanism outputs similar results on different datasets up to DP parameters ε and δ

Experiments: illustrative example

- Customer at node 7 with a load pattern

$$\max\left\{\sin \frac{5}{10^2}t, \frac{7}{10}\right\} + \frac{5}{10^2}\sin\frac{5}{10^2}t + \frac{25}{10^3}\sin\frac{75}{10^2}t$$

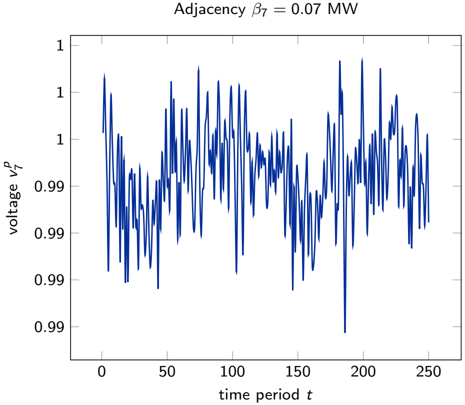
- The goal is to obfuscate this load pattern in power flow and voltage readings
- d_7^p must me indistinguishable from any $d_7^{p'} \in [d_7^p - \beta_7; d_7^p + \beta_7]$, for some $\beta_7 \in \mathbb{R}_+$



- Customer at node 7 with a load pattern

$$\max\left\{\sin \tfrac{5}{10^2} t, \tfrac{7}{10}\right\} + \tfrac{5}{10^2} \sin \tfrac{5}{10^2} t + \tfrac{25}{10^3} \sin \tfrac{75}{10^2} t$$

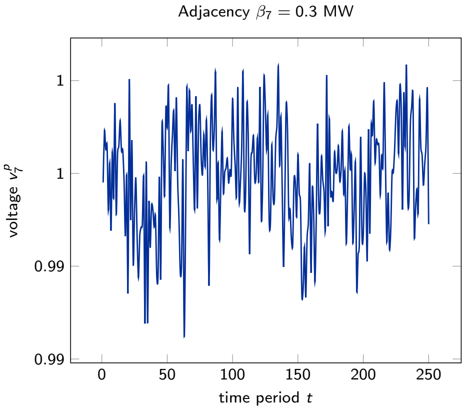
- The goal is to obfuscate this load pattern in power flow and voltage readings
- d_7^p must me indistinguishable from any $d_7^{p'} \in [d_7^p - \beta_7; d_7^p + \beta_7]$, for some $\beta_7 \in \mathbb{R}_+$



- Customer at node 7 with a load pattern

$$\max\left\{\sin \tfrac{5}{10^2}t, \tfrac{7}{10}\right\} + \tfrac{5}{10^2}\sin \tfrac{5}{10^2}t + \tfrac{25}{10^3}\sin \tfrac{75}{10^2}t$$

- The goal is to obfuscate this load pattern in power flow and voltage readings
- d_7^p must me indistinguishable from any $d_7^{p'} \in [d_7^p - \beta_7; d_7^p + \beta_7]$, for some $\beta_7 \in \mathbb{R}_+$

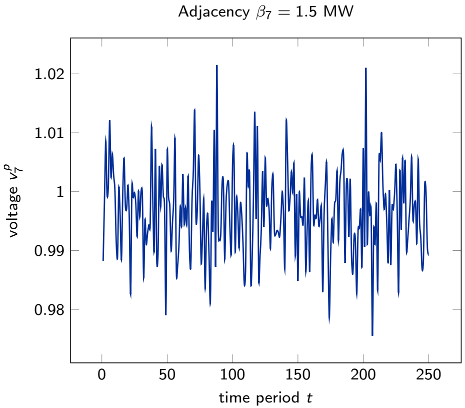


Experiments: illustrative example

- Customer at node 7 with a load pattern

$$\max\left\{\sin \frac{5}{10^2} t, \frac{7}{10}\right\} + \frac{5}{10^2} \sin \frac{5}{10^2} t + \frac{25}{10^3} \sin \frac{75}{10^2} t$$

- The goal is to obfuscate this load pattern in power flow and voltage readings
- d_7^p must me indistinguishable from any $d_7^{p'} \in [d_7^p - \beta_7; d_7^p + \beta_7]$, for some $\beta_7 \in \mathbb{R}_+$



Experiments: OPF variance control

- D-OPF — non-private, deterministic OPF
- CC-OPF — variance-agnostic DP OPF
- V-CC-OPF — variance-aware DP OPF

i	d_i^p	σ_i	D-OPF		CC-OPF				V-CC-OPF			
			f_i^p	v_i	f_i^p		v_i		f_i^p		v_i	
					mean	std	mean	std	mean	std	mean	std
0	0	–	–	1.00	–	–	1.00	–	–	–	1.00	–
1	2.01	**0.48**	8.5	1.00	11.3	**2.68**	1.00	0.0016	12.6	**0.69**	1.00	0.0004
2	2.01	**0.48**	6.5	1.00	9.3	**2.68**	0.99	0.0057	11.4	**0.71**	0.99	0.0015
3	2.01	**0.48**	4.4	1.00	7.3	**2.68**	0.99	0.0123	10.2	**0.78**	0.97	0.0033
4	1.73	**0.41**	-8.0	1.00	-1.4	**1.72**	0.99	0.0128	3.6	**0.69**	0.97	0.0034
5	2.91	**0.70**	5.1	1.00	3.1	**0.87**	0.99	0.0128	2.5	**0.82**	0.97	0.0035
6	2.19	**0.52**	2.2	1.00	0.1	**0.87**	0.99	0.0128	0.7	**0.63**	0.97	0.0038
7	2.35	**0.56**	2.3	0.99	0.9	**0.63**	0.98	0.0134	0.9	**0.61**	0.97	0.0039
8	2.35	**0.56**	10.5	0.99	6.7	**1.18**	0.98	0.0130	5.8	**0.78**	0.97	0.0036
9	2.29	**0.55**	5.8	0.99	3.5	**0.88**	0.98	0.0132	3.1	**0.70**	0.97	0.0037
10	2.17	**0.52**	3.5	0.99	1.2	**0.88**	0.98	0.0135	1.6	**0.65**	0.97	0.0038
11	1.32	**0.32**	1.3	0.99	0.4	**0.39**	0.98	0.0135	0.4	**0.40**	0.97	0.0038
12	2.01	**0.48**	6.5	1.00	3.6	**1.23**	1.00	0.0008	3.3	**0.73**	1.00	0.0004
13	2.24	**0.54**	4.5	0.99	1.6	**1.23**	1.00	0.0034	2.1	**0.72**	1.00	0.0019
14	2.24	**0.54**	2.2	0.99	-0.6	**1.23**	1.00	0.0050	0.8	**0.64**	0.99	0.0027
Cost ($\mathbb{E}[\Delta c]$)			\$396.0 (0%)		\$428.0 (8.1%)				\$463.5 (17.1%)			
$\sum_i \text{std}[f_i^p]$			0 MW		19.1 MW				9.5 MW			
infeas. $\hat{\eta}$			0%		3.3%				6.9%			
CPU time			0.016s		0.037s				0.043s			

Experiments: OPF variance control

- D-OPF — non-private, deterministic OPF
- CC-OPF — variance-agnostic DP OPF
- V-CC-OPF — variance-aware DP OPF

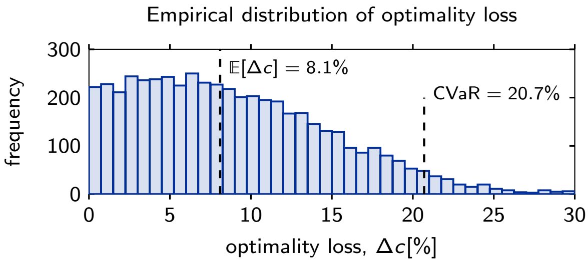
i	d_i^p	σ_i	D-OPF		CC-OPF				V-CC-OPF			
			f_i^p	v_i	f_i^p		v_i		f_i^p		v_i	
					mean	std	mean	std	mean	std	mean	std
0	0	–	–	1.00	–	–	1.00	–	–	–	1.00	–
1	2.01	**0.48**	8.5	1.00	11.3	**2.68**	1.00	0.0016	12.6	**0.69**	1.00	0.0004
2	2.01	**0.48**	6.5	1.00	9.3	**2.68**	0.99	0.0057	11.4	**0.71**	0.99	0.0015
3	2.01	**0.48**	4.4	1.00	7.3	**2.68**	0.99	0.0123	10.2	**0.78**	0.97	0.0033
4	1.73	**0.41**	-8.0	1.00	-1.4	**1.72**	0.99	0.0128	3.6	**0.69**	0.97	0.0034
5	2.91	**0.70**	5.1	1.00	3.1	**0.87**	0.99	0.0128	2.5	**0.82**	0.97	0.0035
6	2.19	**0.52**	2.2	1.00	0.1	**0.87**	0.99	0.0128	0.7	**0.63**	0.97	0.0038
7	2.35	**0.56**	2.3	0.99	0.9	**0.63**	0.98	0.0134	0.9	**0.61**	0.97	0.0039
8	2.35	**0.56**	10.5	0.99	6.7	**1.18**	0.98	0.0130	5.8	**0.78**	0.97	0.0036
9	2.29	**0.55**	5.8	0.99	3.5	**0.88**	0.98	0.0132	3.1	**0.70**	0.97	0.0037
10	2.17	**0.52**	3.5	0.99	1.2	**0.88**	0.98	0.0135	1.6	**0.65**	0.97	0.0038
11	1.32	**0.32**	1.3	0.99	0.4	**0.39**	0.98	0.0135	0.4	**0.40**	0.97	0.0038
12	2.01	**0.48**	6.5	1.00	3.6	**1.23**	1.00	0.0008	3.3	**0.73**	1.00	0.0004
13	2.24	**0.54**	4.5	0.99	1.6	**1.23**	1.00	0.0034	2.1	**0.72**	1.00	0.0019
14	2.24	**0.54**	2.2	0.99	-0.6	**1.23**	1.00	0.0050	0.8	**0.64**	0.99	0.0027
Cost ($\mathbb{E}[\Delta c]$)			\$396.0 (0%)		\$428.0 (8.1%)				\$463.5 (17.1%)			
$\sum_i$ std$[f_i^p]$			0 MW		19.1 MW				9.5 MW			
infeas. $\hat{\eta}$			0%		3.3%				6.9%			
CPU time			0.016s		0.037s				0.043s			

Experiments: OPF variance control

- D-OPF — non-private, deterministic OPF
- CC-OPF — variance-agnostic DP OPF
- V-CC-OPF — variance-aware DP OPF

i	d_i^p	σ_i	D-OPF		CC-OPF				V-CC-OPF			
			f_i^p	v_i	f_i^p		v_i		f_i^p		v_i	
					mean	std	mean	std	mean	std	mean	std
0	0	–	–	1.00	–	–	1.00	–	–	–	1.00	–
1	2.01	**0.48**	8.5	1.00	11.3	**2.68**	1.00	0.0016	12.6	**0.69**	1.00	0.0004
2	2.01	**0.48**	6.5	1.00	9.3	**2.68**	0.99	0.0057	11.4	**0.71**	0.99	0.0015
3	2.01	**0.48**	4.4	1.00	7.3	**2.68**	0.99	0.0123	10.2	**0.78**	0.97	0.0033
4	1.73	**0.41**	-8.0	1.00	-1.4	**1.72**	0.99	0.0128	3.6	**0.69**	0.97	0.0034
5	2.91	**0.70**	5.1	1.00	3.1	**0.87**	0.99	0.0128	2.5	**0.82**	0.97	0.0035
6	2.19	**0.52**	2.2	1.00	0.1	**0.87**	0.99	0.0128	0.7	**0.63**	0.97	0.0038
7	2.35	**0.56**	2.3	0.99	0.9	**0.63**	0.98	0.0134	0.9	**0.61**	0.97	0.0039
8	2.35	**0.56**	10.5	0.99	6.7	**1.18**	0.98	0.0130	5.8	**0.78**	0.97	0.0036
9	2.29	**0.55**	5.8	0.99	3.5	**0.88**	0.98	0.0132	3.1	**0.70**	0.97	0.0037
10	2.17	**0.52**	3.5	0.99	1.2	**0.88**	0.98	0.0135	1.6	**0.65**	0.97	0.0038
11	1.32	**0.32**	1.3	0.99	0.4	**0.39**	0.98	0.0135	0.4	**0.40**	0.97	0.0038
12	2.01	**0.48**	6.5	1.00	3.6	**1.23**	1.00	0.0008	3.3	**0.73**	1.00	0.0004
13	2.24	**0.54**	4.5	0.99	1.6	**1.23**	1.00	0.0034	2.1	**0.72**	1.00	0.0019
14	2.24	**0.54**	2.2	0.99	-0.6	**1.23**	1.00	0.0050	0.8	**0.64**	0.99	0.0027
Cost ($\mathbb{E}[\Delta c]$)			\$396.0 (0%)		\$428.0 (8.1%)				\$463.5 (17.1%)			
$\sum_i \text{std}[f_i^p]$			0 MW		19.1 MW				9.5 MW			
infeas. $\hat{\eta}$			0%		3.3%				6.9%			
CPU time			0.016s		0.037s				0.043s			

Experiments: optimality loss control



ψ	exp. value		$CVaR_{10\%}$	
	cost, \$	Δc,%	cost, \$	Δc,%
0.0	428.0	8.1	478.1	20.7
0.1	428.0	8.1	476.3	20.3
0.2	428.3	8.2	475.0	19.9
0.3	428.9	8.3	473.3	19.5
0.4	431.9	9.1	467.8	18.1
0.5	434.5	9.7	464.4	17.3
0.6	438.2	10.7	461.7	16.6
0.7	452.9	14.4	452.9	14.4

Conclusions

- Distribution OPF models tend to leak sensitive information of grid customers
- We augment OPFs model with a privacy-preserving layer, while offering:
  - Robust privacy guarantees
  - Formal feasibility guarantees
  - Means to control the randomized OPF solution
- Distribution DP OPF models are open source and available at

  `https://github.com/wdvorkin/DP_CC_OPF`

Thank you for your attention!

V. Dvorkin, F. Fioretto, P. Van Hentenryck, P. Pinson and J. Kazempour
Differentially Private Optimal Power Flow for Distribution Grids
IEEE Transactions on Power Systems (to appear), 2020
`https://github.com/wdvorkin/DP_CC_OPF`

SCAN ME