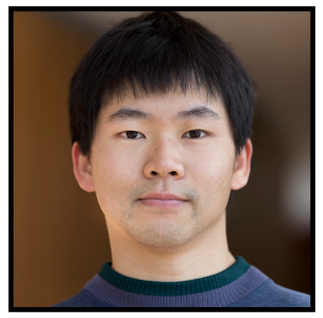
Georgia Tech

CREATING THE NEXT

Privacy-Preserving Obfuscation of Critical Infrastructure Networks

Ferdinando Fioretto
Georgia Tech
Syracuse University



Terrence W.K. Mak
Georgia Tech

Pascal
Van Hentenryck
Georgia Tech

August 15, 2019

Overview

- Motivation
  - Critical Infrastructure Networks
- Background
  - Differential Privacy
- Privacy-preserving Obfuscation mechanism
  - Critical Infrastructure Networks Obfuscation Problem
  - POCIN Mechanism:
    - ➡Location Obfuscation, Value Obfuscation, and Fidelity Restoration
- Experimental Results
  - Power Network Obfuscation Problem
  - Traffic Network Obfuscation Problem
- Conclusion

Motivation

- Release information on *critical* infrastructure network

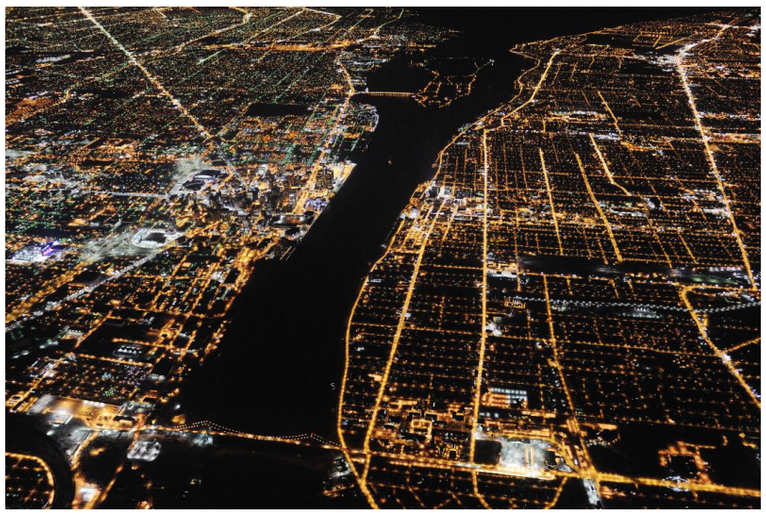
  ➡ Energy Systems: Power Systems / Natural Gas Systems

  ➡Traffic Systems: Road Maps / Traffic Data / Bus operation data

- Why?

  - Research highly dependent on realistic test cases

    ➡Tackling: traffic congestions / power system stability issues



https://commons.wikimedia.org/wiki/File:Atlanta_75.85.jpg

Georgia Tech

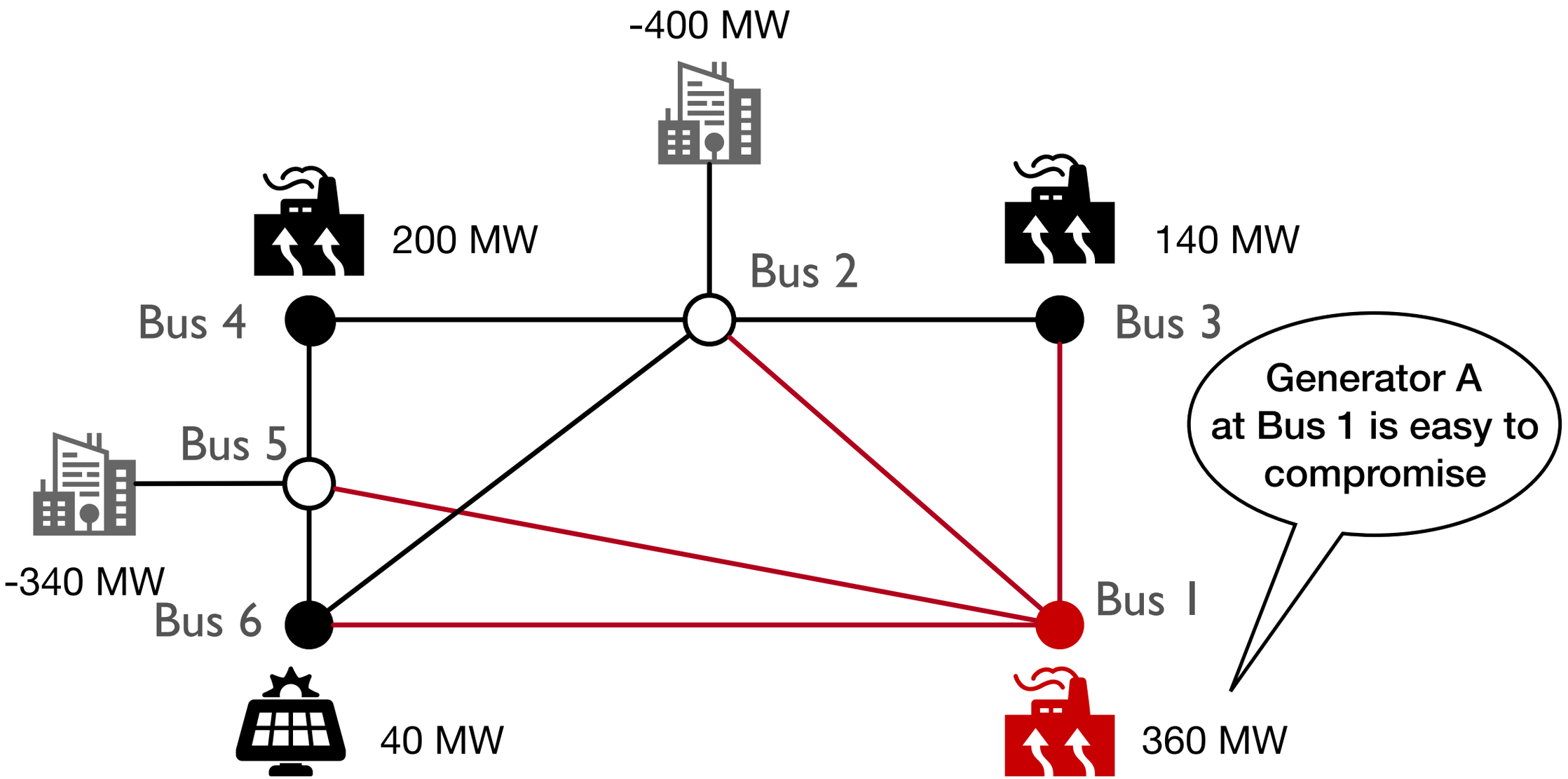
However …

- Privacy and security concerns:
  - Energy Systems:
    - ➡Revealing customer/company information
    - ➡Revealing national secret/protected assets
  - Traffic Systems:
    - ➡Revealing driver personal data

https://commons.wikimedia.org/wiki/File:Sanduo_1st_Road_after_Explosion_Record_20140811-021.JPG

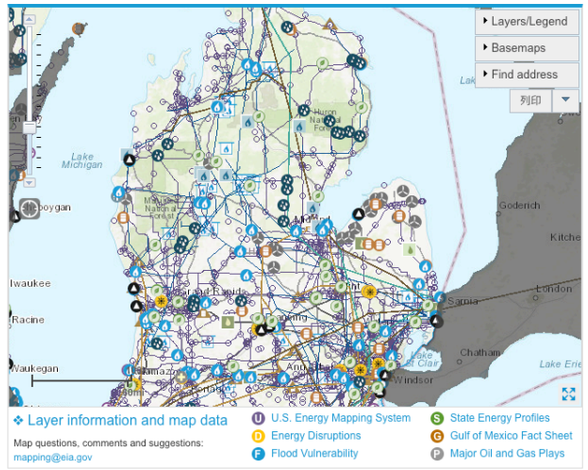
Georgia Tech

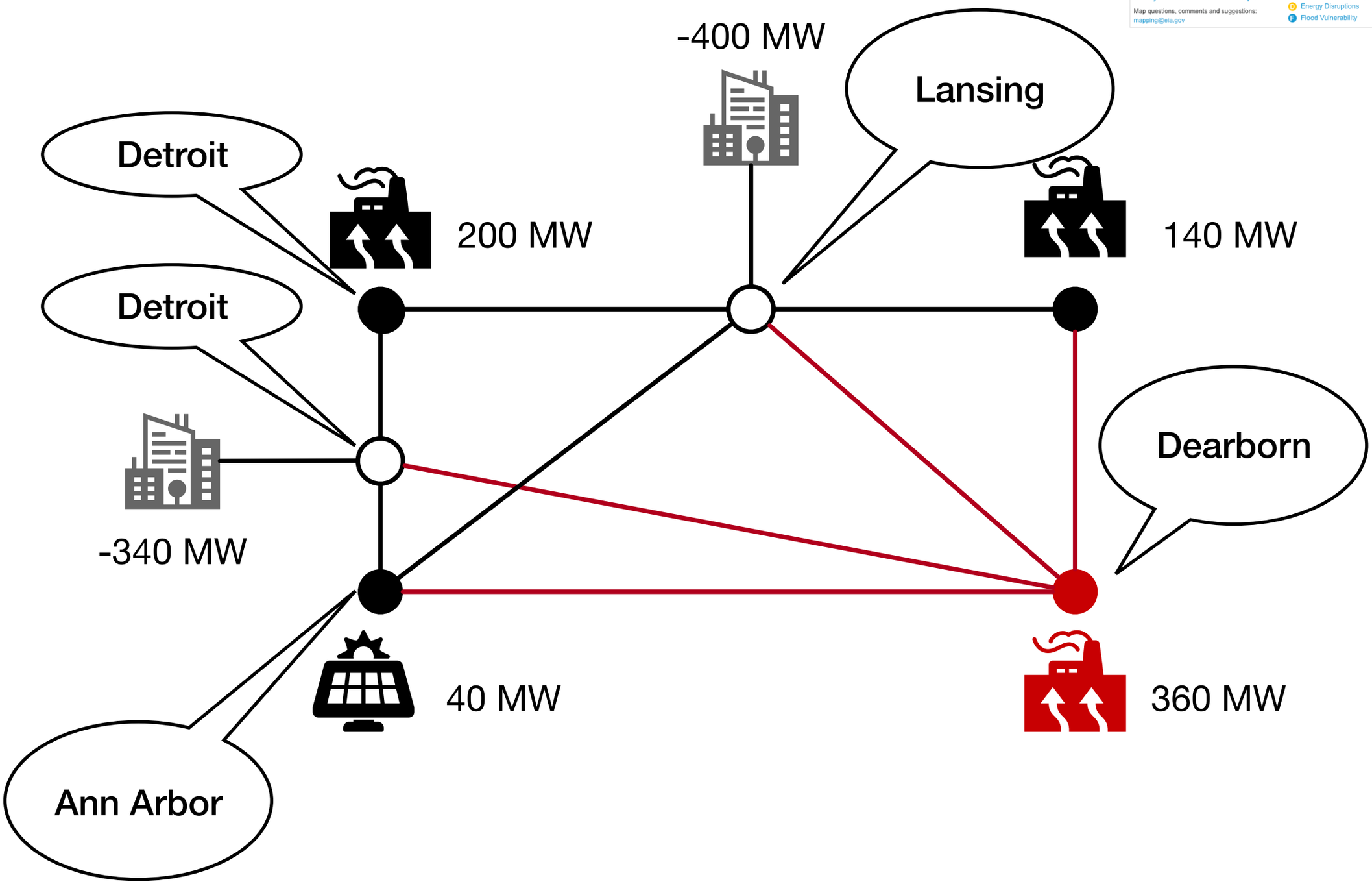
What can we infer?



Georgia Tech

With public map data and matching the topology ..





Georgia Tech

With public data and matching the generator capacities …

Coal

Plant	Location	Power (MW)
Belle River Power Plant	St. Clair	1395
D.E. Karn Generating Plant	Hampton Township	544
Eckert Power Plant	Lansing	240
Erickson Power Plant	Lansing	155
Escanaba Paper Company	Escanaba	54
J.B. Sims Power Plant	Grand Haven	80
J.H. Campbell Power Plant	Port Sheldon Township	1560
Monroe Power Plant	Monroe	3280
River Rouge Power Plant	River Rouge	358
Shiras Station	Marquette	78
St. Clair Power Plant	St. Clair	1378
Filer City Station	Filer City	70
Trenton Channel Power Plant	Trenton	536
White Pine Power Plant	White Pine	40

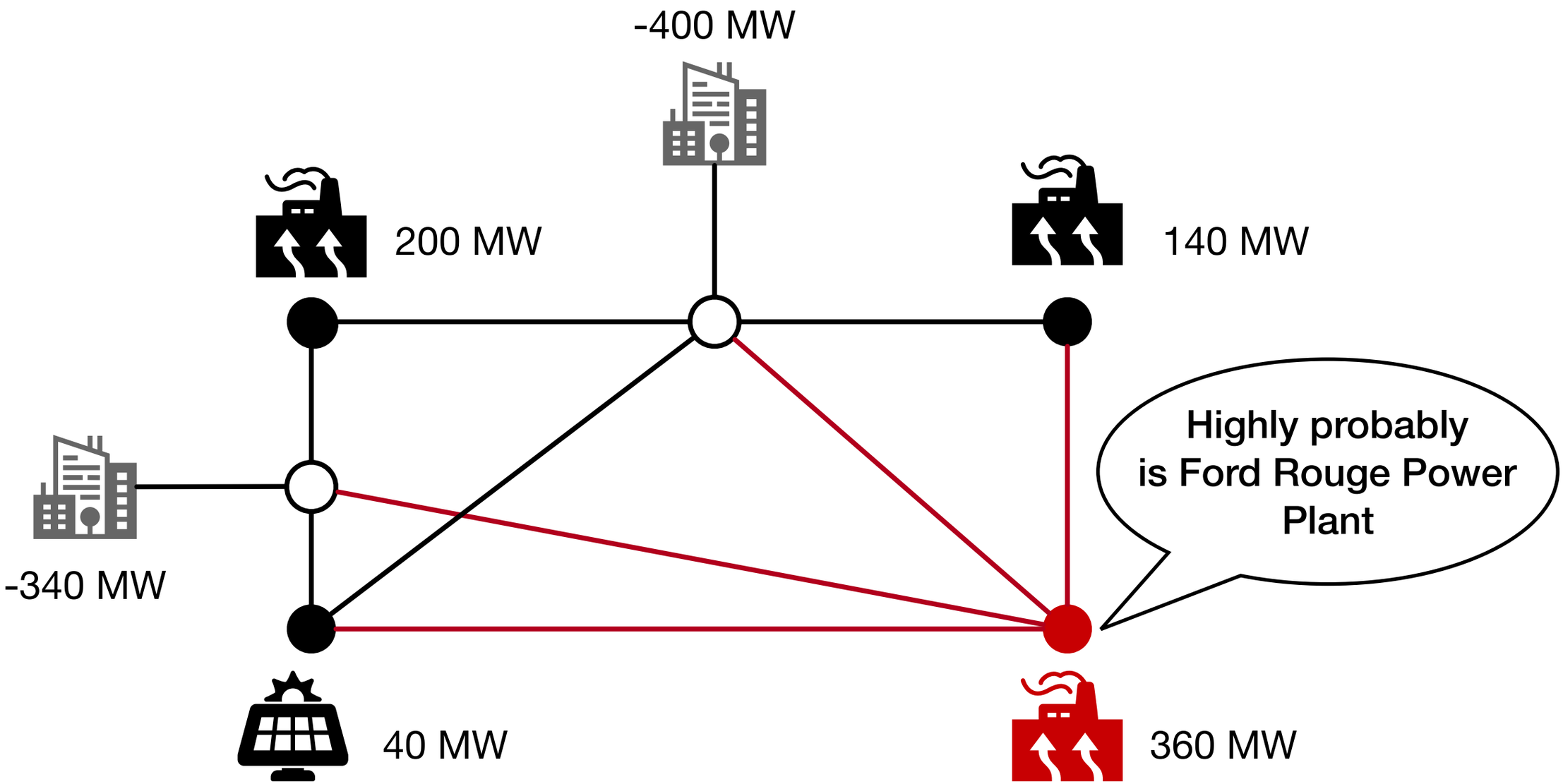
Nuclear

Plant	Location	Power (MW)
Enrico Fermi Nuclear Generating Station	Monroe	1098
Donald C. Cook Nuclear Power Plant	Bridgman	2110
Palisades Nuclear Power Plant	South Haven	800

Gas

Plant	Location	Power (MW)
A.J. Mihm Generating Station	L'Anse	54.9
Alpine Generating Facility	Elmira	440
48th Street Generation Station	Holland	142
Belle River Power Plant	East China Township, Michigan	256
Conners Creek Power Plant	Detroit	240
Dearborn Industrial Generation	Dearborn	710
Delray Peaking Facility	Detroit	127
Dean Peaking Station	East China Township, Michigan	336
F.D. Kuester Generating Station	Negaunee Township	128.1
Hancock	Commerce Township	141
Holland Energy Park	Holland	130
Kalamazoo River Generating Station	Comstock	68
Kinder Morgan Power	Jackson	564
Livingston Generating Station	Gaylord	156
Marquette Energy Center	Marquette	50
Michigan Power	Ludington	123
Midland Cogeneration Venture	Midland	1560
Mistersky Gas Power Plant	Detroit	154
New Covert Generating Facility	Covert, Michigan	1159
REO Town Cogeneration Plant	Lansing, Michigan	110
Renaissance Power	Carson City	660
River Rouge Power Plant	River Rouge	260
Sumpter Plant	Sumpter	340
T. B. Simon Power Plant	East Lansing	100
Thetford	Genesee	222
Wyandotte Municipal Power Plant	Wyandotte	73
Zeeland Generating Station	Zeeland	868

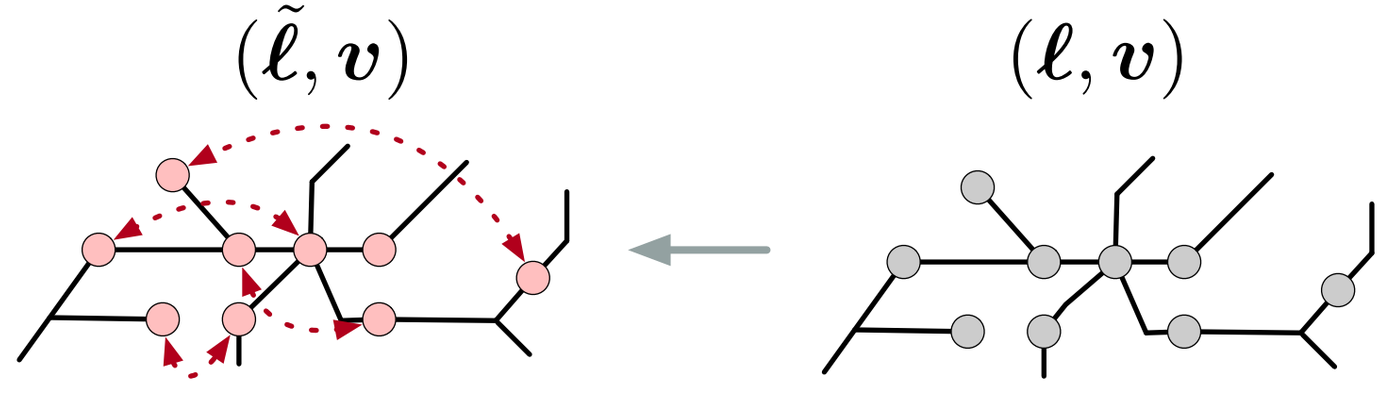
What can we infer?



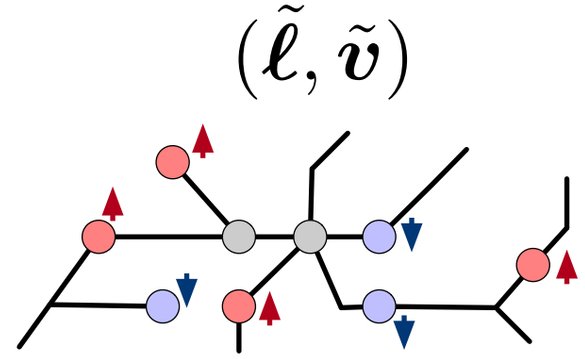
Georgia Tech

Privacy-preserving Obfuscation mechanism

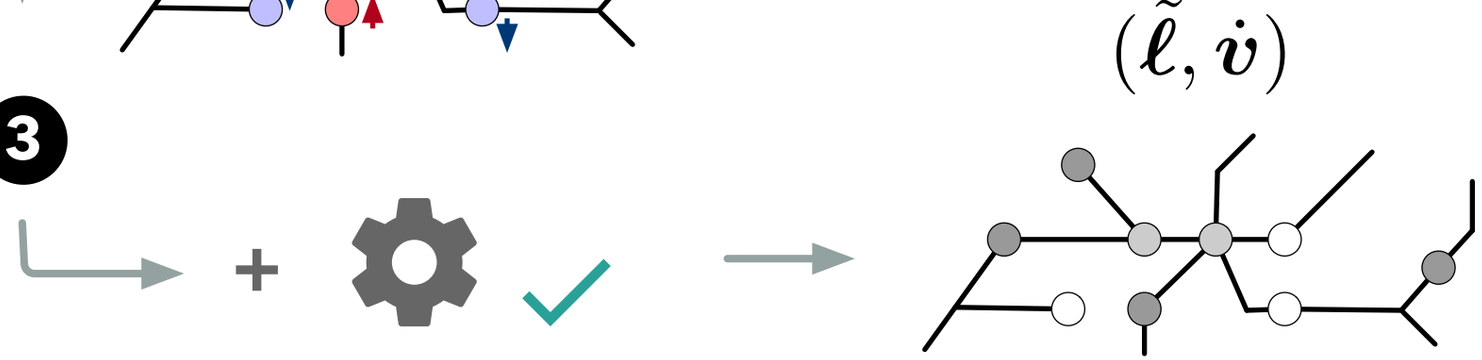
Location Obfuscation 1



Value Obfuscation 2



Fidelity Restoration 3



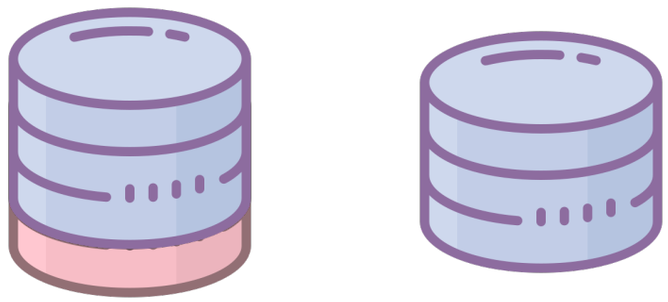
Georgia Tech

Overview

- Motivation
  - Critical Infrastructure Networks
- Background
  - Differential Privacy
- Privacy-preserving Obfuscation mechanism
  - Critical Infrastructure Networks Obfuscation Problem
  - POCIN Mechanism:
    - ➡Location Obfuscation, Value Obfuscation, and Fidelity Restoration
- Experimental Results
  - Power Network Obfuscation Problem
  - Traffic Network Obfuscation Problem
- Conclusion

Differential Privacy

For every pair of inputs that differs in one row



D_1 D_2

For every output O:

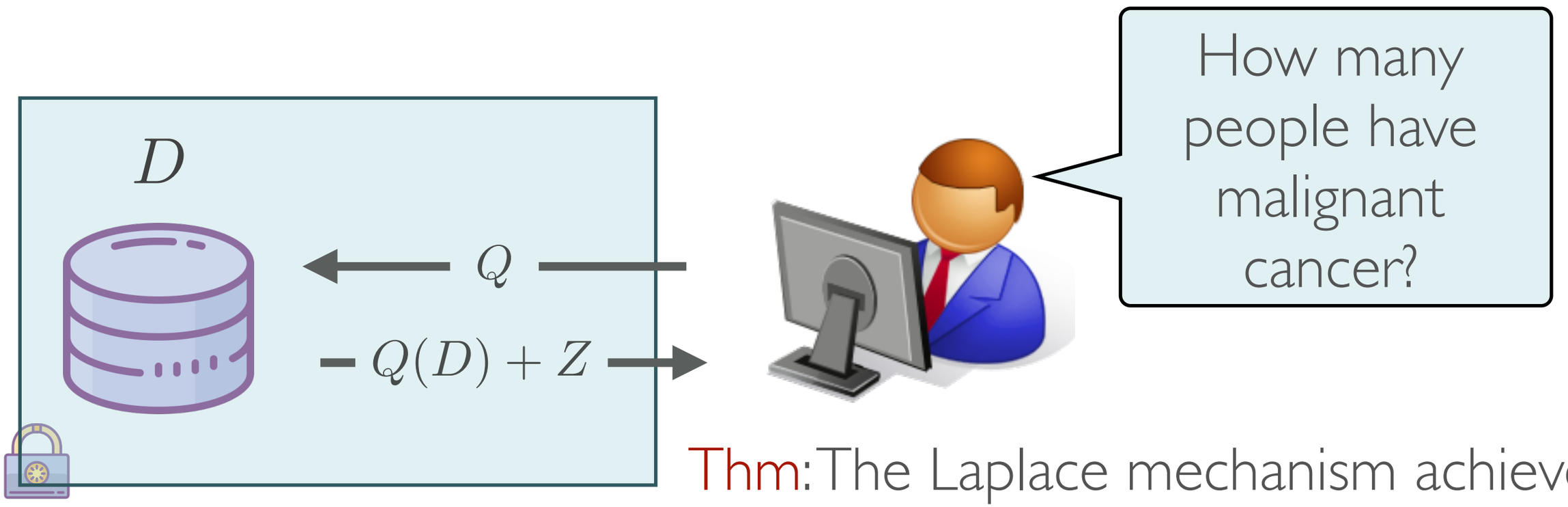
A randomized algorithm $\mathcal{A}$ is ε-differentially private if:

$$\frac{\Pr[\mathcal{A}(D_1) = O]}{\Pr[\mathcal{A}(D_2) = O]} \leq \exp(\epsilon)$$

Intuition: adversary should not be able to use output O to distinguish between any D_1 and D_2

Differential Privacy
Sensitivity Method & Privacy Properties

- Consider a query Q on the dataset D. The *sensitivity method* injects noise to the output Q(D) that depends on the sensitivity of the query:
- $$\Delta_Q = \max_{D_1 \sim D_2} \|Q(D_1) - Q(D_2)\|_1$$



Thm: The Laplace mechanism achieves ε-differential privacy

Georgia Tech

Overview

- Motivation
  - Critical Infrastructure Networks
- Background
  - Differential Privacy
- Privacy-preserving Obfuscation mechanism
  - Critical Infrastructure Networks Obfuscation Problem
  - POCIN Mechanism:
    - ➡Location Obfuscation, Value Obfuscation, and Fidelity Restoration
- Experimental Results
  - Power Network Obfuscation Problem
  - Traffic Network Obfuscation Problem
- Conclusion

Critical Infrastructure Networks Obfuscation Problem

- Two critical infrastructure network $\boldsymbol{G} = (\boldsymbol{I}, \boldsymbol{v})$, $\boldsymbol{G'} = (\boldsymbol{I'}, \boldsymbol{v'})$ are location-value indistinguishable:
  - $\boldsymbol{G} \sim_{Iv} \boldsymbol{G'} \Leftrightarrow \boldsymbol{I} \sim_{I} \boldsymbol{I'}$ or $\boldsymbol{v} \sim_{v} \boldsymbol{v'}$

- A randomized mechanism is $(\epsilon, \alpha_I, \alpha_V)$-indistinguishable if, for any pair of $\sim_{Iv}$-adjacent datasets, differential privacy holds.

- Given a critical infrastructure network description $\boldsymbol{G}$, a problem P, and positive real values ϵ, α_I, and α_V, the privacy-preserving obfuscation problem produces $\boldsymbol{G^p}$ such that:

  1) Privacy: $\boldsymbol{G^p}$ is $(\epsilon, \alpha_I, \alpha_V)$-indistinguishable

  2) Fidelity: $\boldsymbol{G^p}$ admits a solution satisfying all the constraints of P and β-faithful to the objective of P (i.e. β percents to the original optimal solution of $\boldsymbol{G}$)

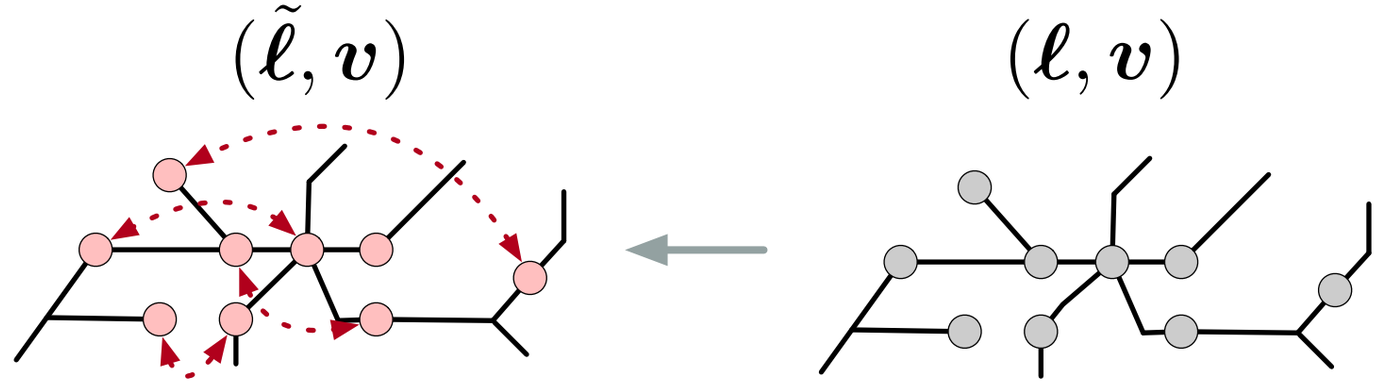
  3) Robustness: $\boldsymbol{G^p}$ minimizes the damage inflict by an attack function $\boldsymbol{A}$.

Overview

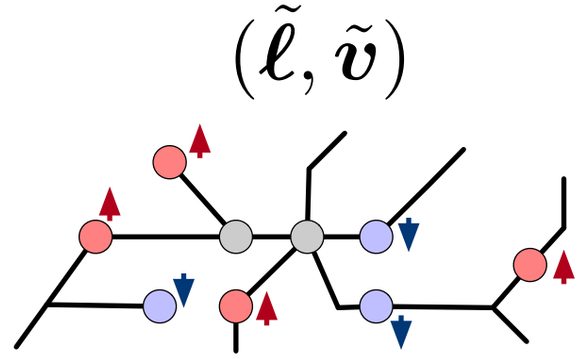
- Motivation
  - Critical Infrastructure Networks
- Background
  - Differential Privacy
- Privacy-preserving Obfuscation mechanism
  - Critical Infrastructure Networks Obfuscation Problem
  - POCIN Mechanism:
    - ➡Location Obfuscation, Value Obfuscation, and Fidelity Restoration
- Experimental Results
  - Power Network Obfuscation Problem
  - Traffic Network Obfuscation Problem
- Conclusion

Privacy-preserving Obfuscation mechanism

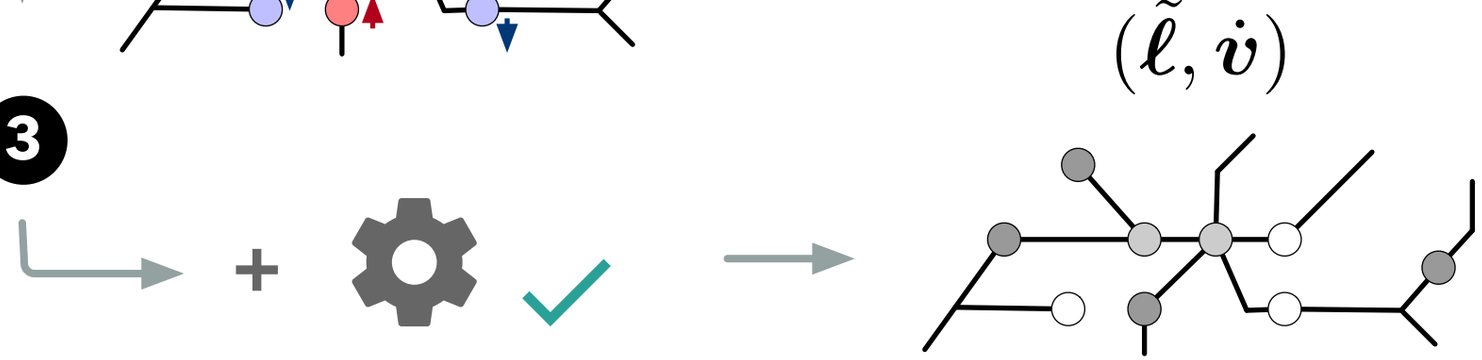
Location Obfuscation 1



Value Obfuscation 2



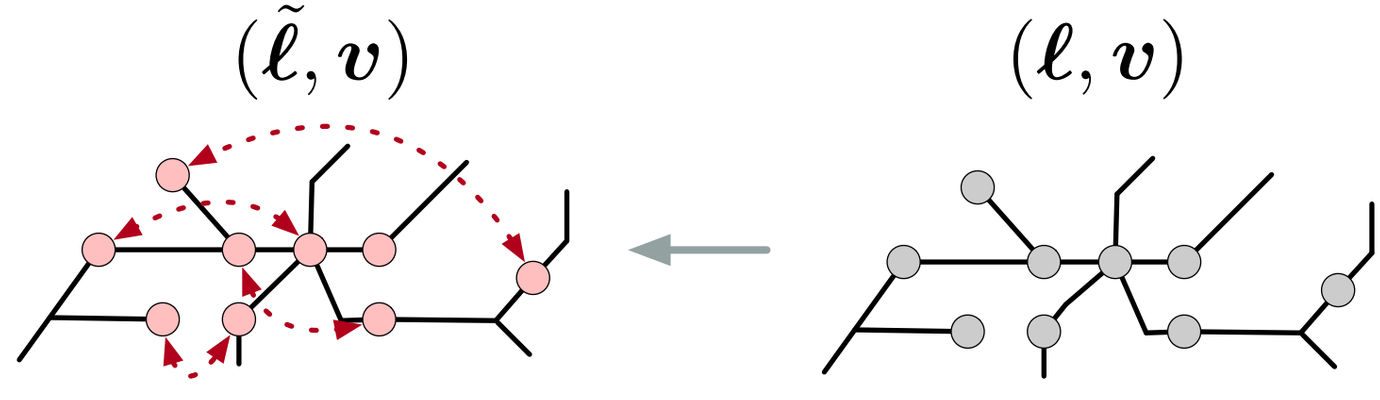
Fidelity Restoration 3



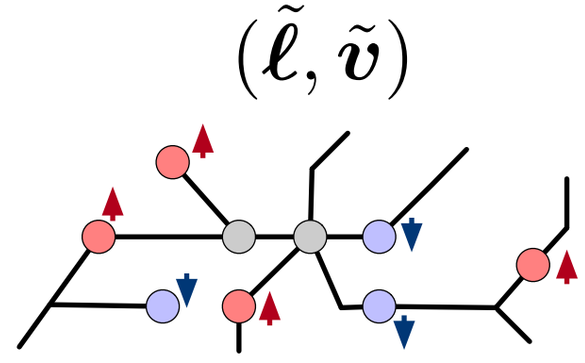
Georgia Tech

Privacy-preserving Obfuscation mechanism

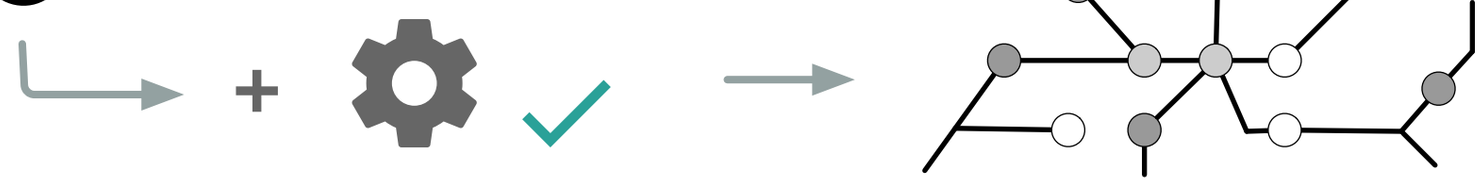
Location Obfuscation ❶



Value Obfuscation ❷

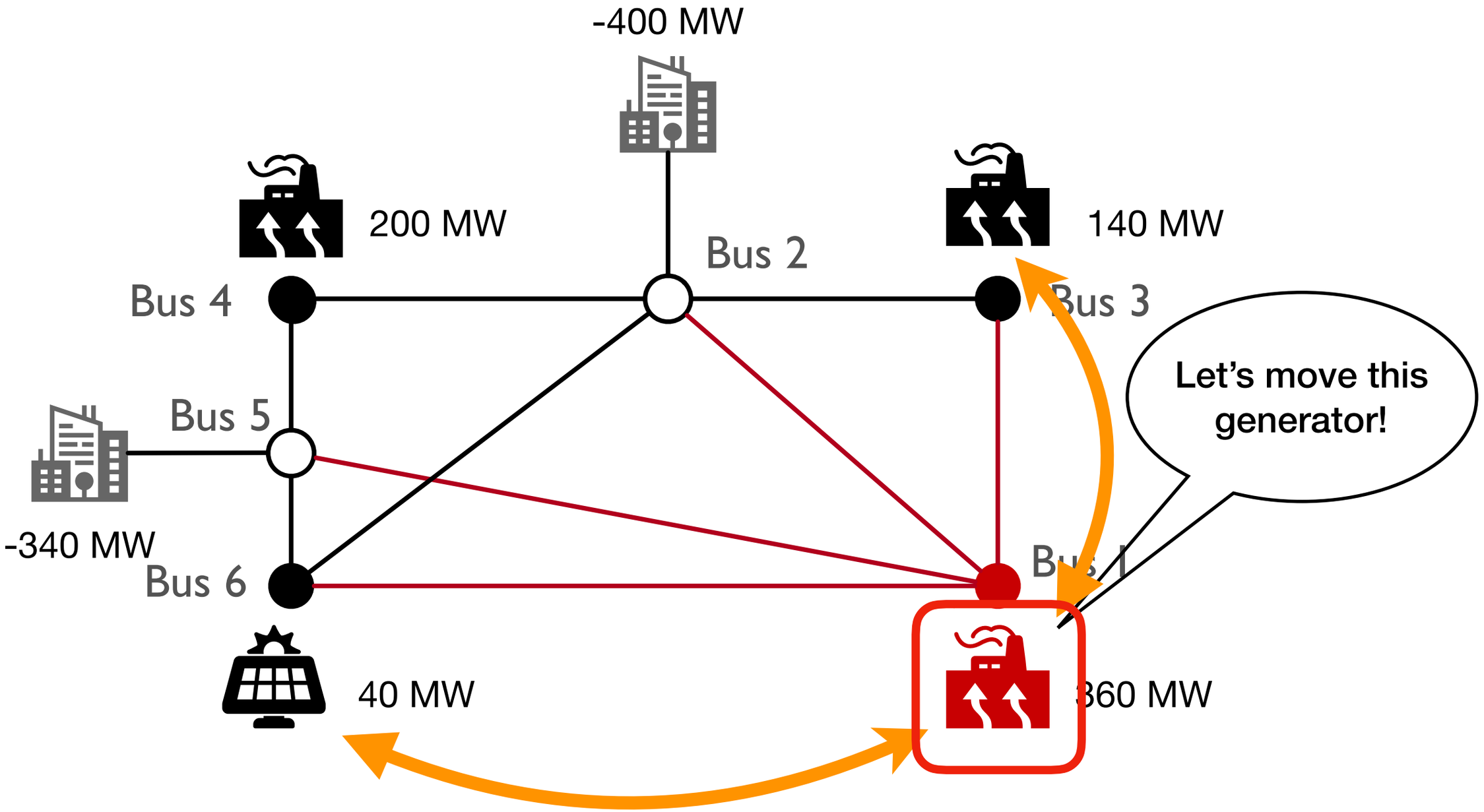


Fidelity Restoration ❸



Georgia Tech

What can we infer?

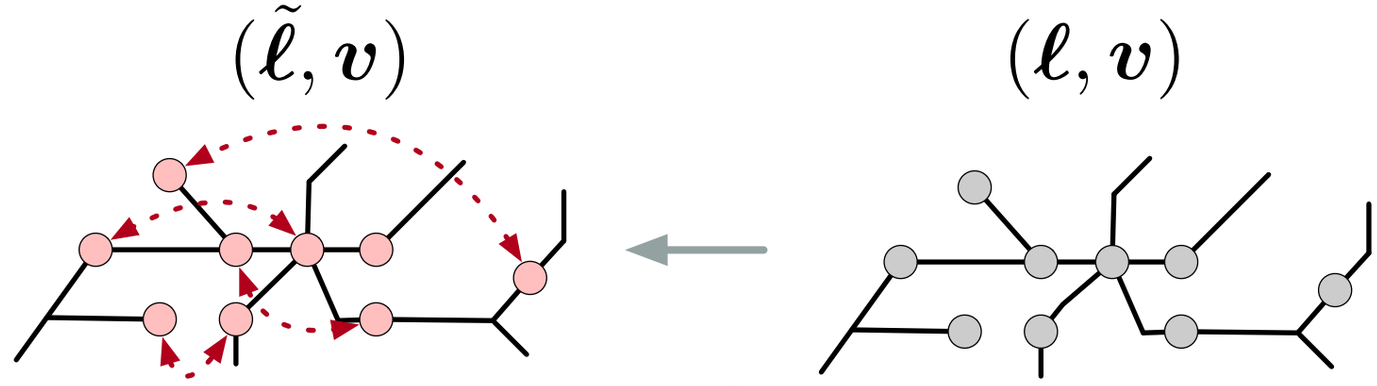


Thm: The Exponential mechanism [McSherry and Talwar, 2007] achieves α_l-location-indistinguishability

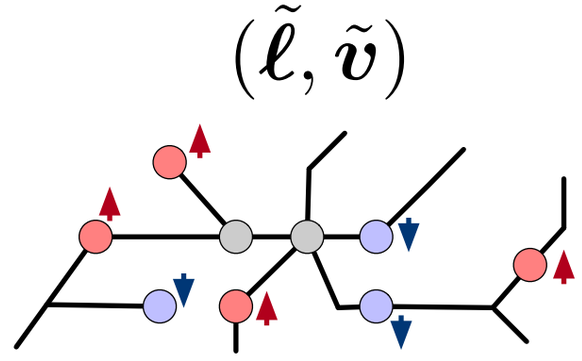
Georgia Tech

Privacy-preserving Obfuscation mechanism

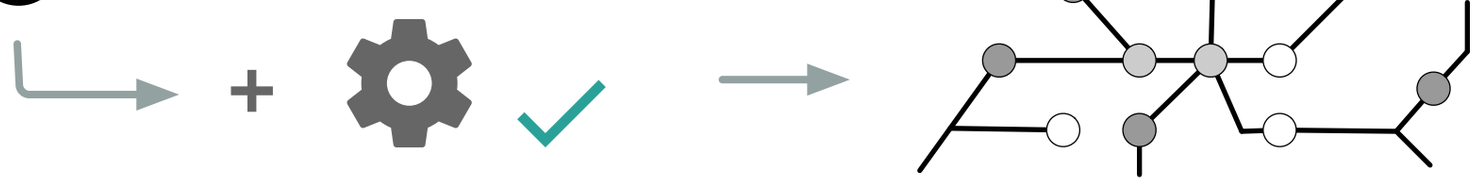
Location Obfuscation 1



Value Obfuscation 2

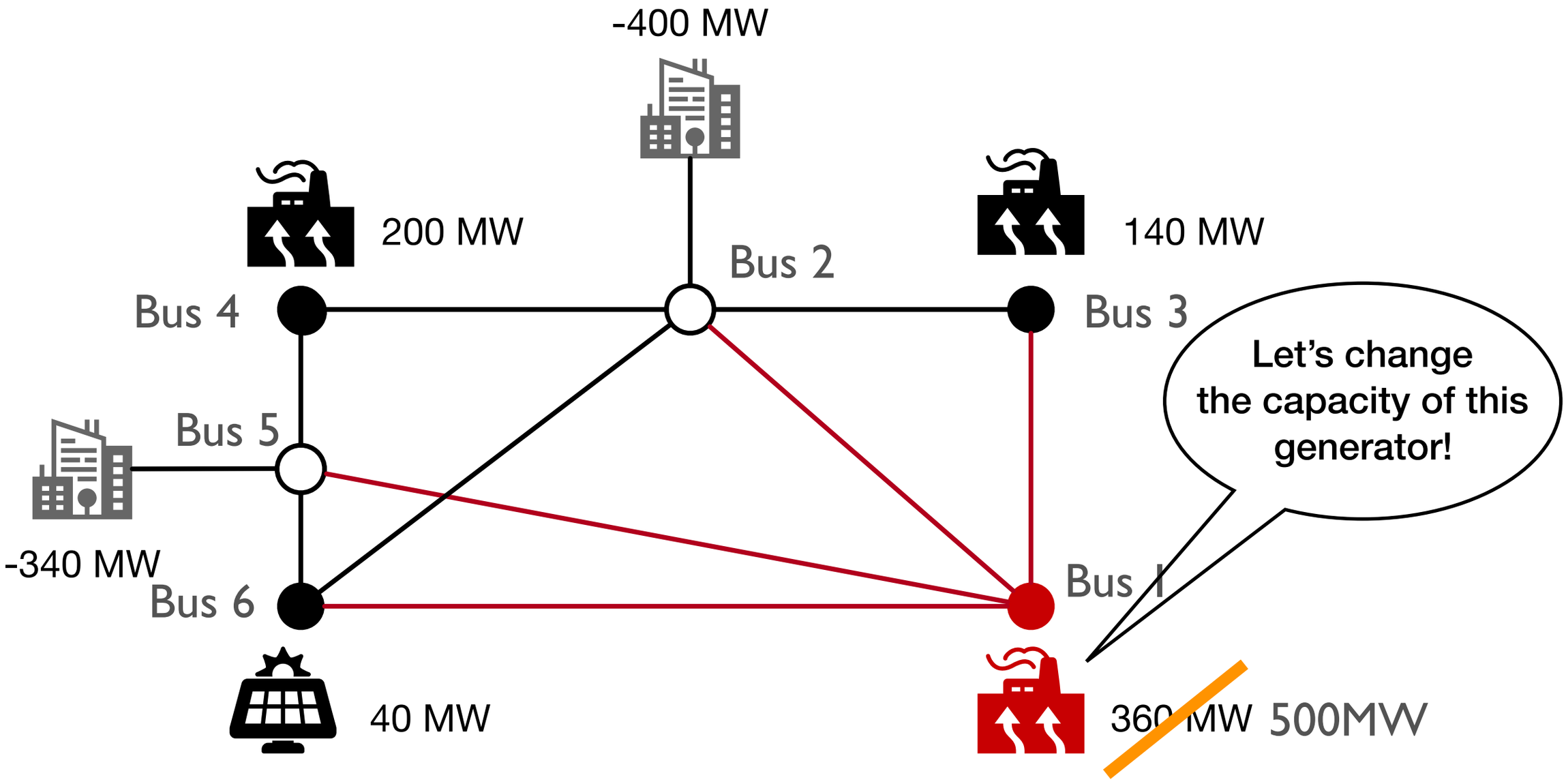


Fidelity Restoration 3



Georgia Tech

What can we infer?



Thm: The Laplace mechanism achieves ε-differential privacy

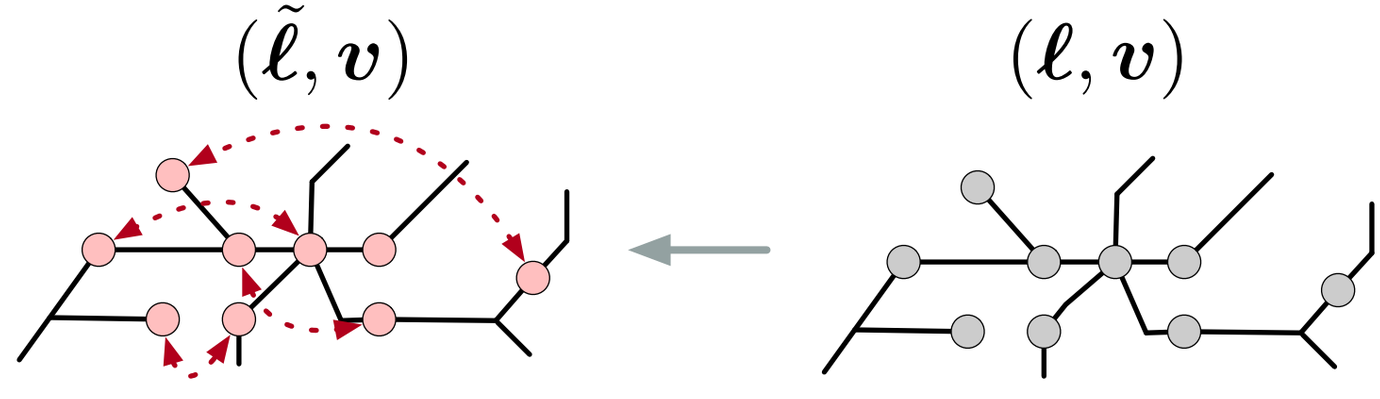
Corollary: achieves α_v-value-indistinguishability.

Georgia Tech

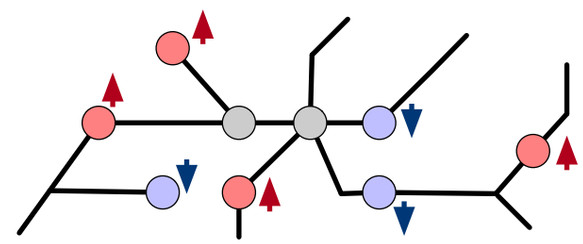
Privacy-preserving Obfuscation mechanis

Guarantee privacy!

Location Obfuscation 1

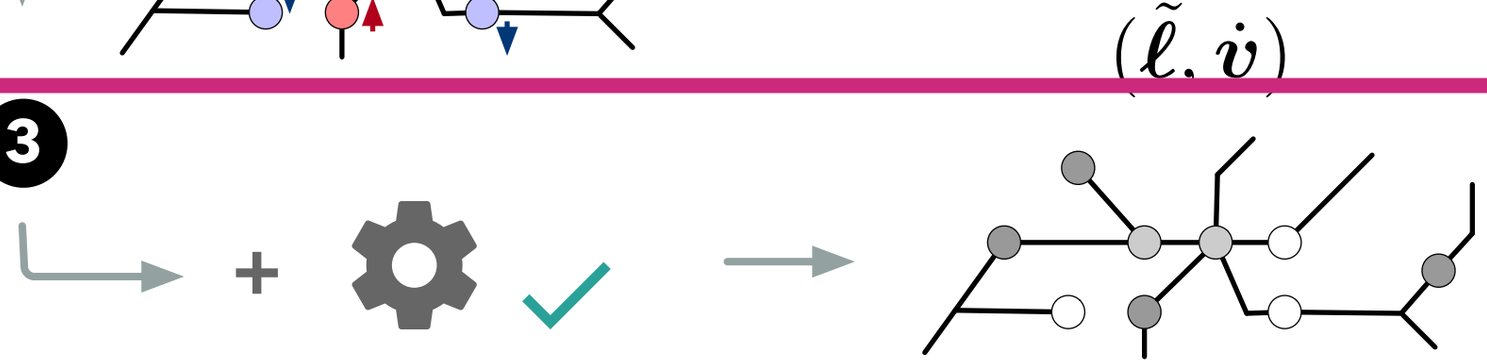


Value Obfuscation 2



Fidelity Restoration 3

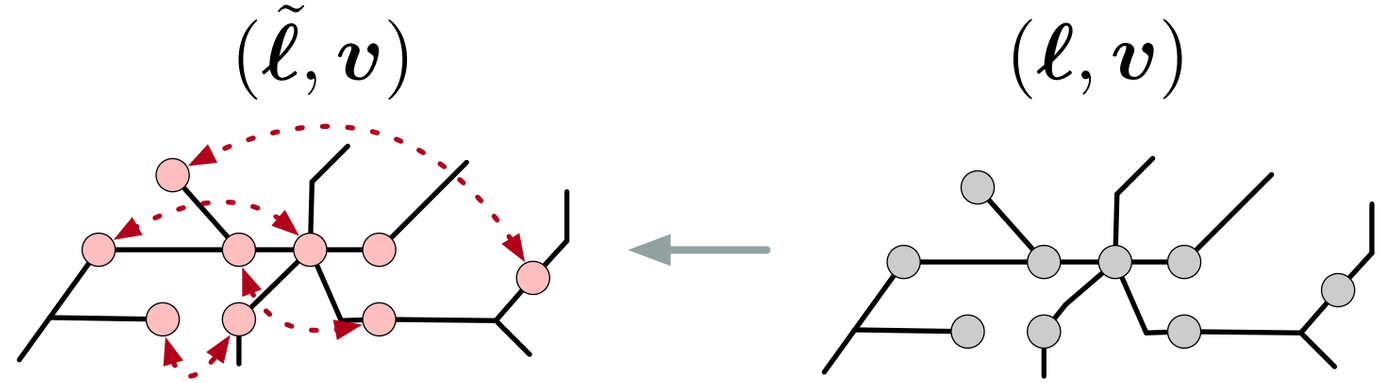
Post-processing immunity



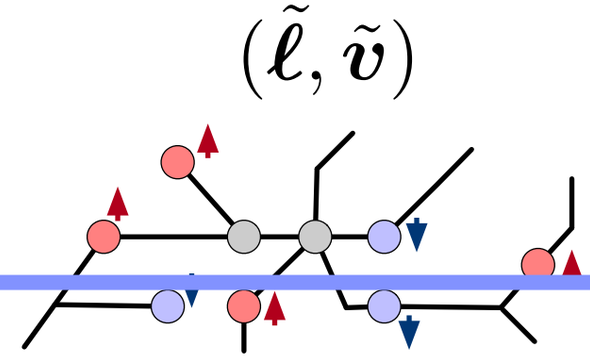
Georgia Tech

Privacy-preserving Obfuscation mechanism

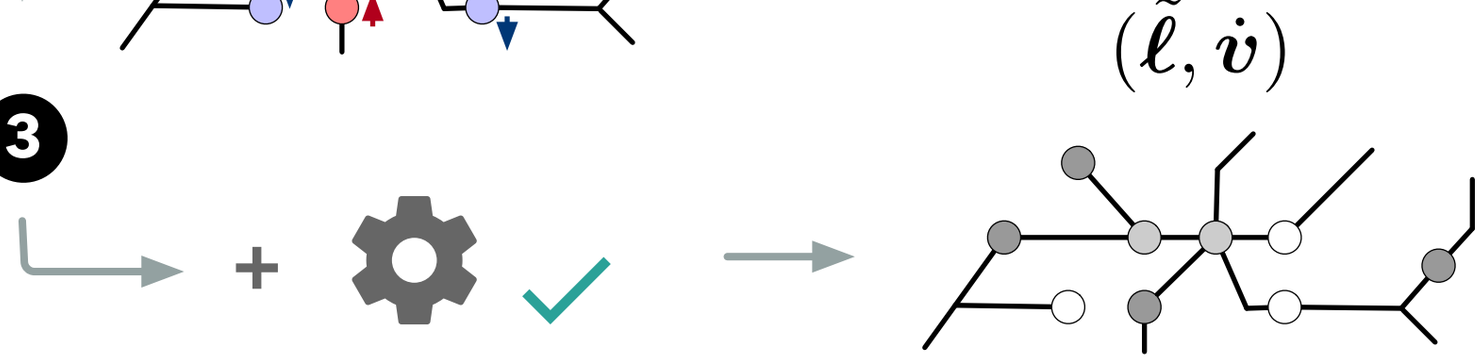
Location Obfuscation 1



Value Obfuscation 2



Fidelity Restoration 3



Georgia Tech

Privacy-preserving Obfuscation mechanism

Fidelity:

G^p admits a solution satisfying all the constraints of P and β-faithful to the objective of P

Bilevel program

$$P_{\mathrm{BL}} = \min_{(\dot{\boldsymbol{v}}, \boldsymbol{x})} \|\dot{\boldsymbol{v}} - \tilde{\boldsymbol{v}}\|_2 \tag{b1}$$

$$\text{s.t.: } |\mathcal{O}(\boldsymbol{x}^*, \dot{\boldsymbol{v}}) - \mathcal{O}^*| \leqslant \beta \tag{b2}$$

$$\boldsymbol{x}^* = \operatorname{argmin}_{\boldsymbol{x}} \ \mathcal{O}(\boldsymbol{x}, \dot{\boldsymbol{v}}) \quad \text{s.t.} \ \ g_i(\boldsymbol{x}, \dot{\boldsymbol{v}}) \leqslant 0 \ \forall i \in [k] \tag{b3}$$

Privacy-preserving Obfuscation mechanism

Fidelity:

G^p admits a solution satisfying all the constraints of P and β-faithful to the objective of P

Not too far from the obfuscated solution

Beta faithful to the original objective costs

Satisfying the constraints

$$P_{\mathrm{BL}} = \min_{(\dot{\boldsymbol{v}}, \boldsymbol{x})} \|\dot{\boldsymbol{v}} - \tilde{\boldsymbol{v}}\|_2 \tag{b1}$$

$$\text{s.t.: } |\mathcal{O}(\boldsymbol{x}^*, \dot{\boldsymbol{v}}) - \mathcal{O}^*| \leqslant \beta \tag{b2}$$

$$\boldsymbol{x}^* = \operatorname{argmin}_{\boldsymbol{x}} \ \mathcal{O}(\boldsymbol{x}, \dot{\boldsymbol{v}}) \quad \text{s.t.} \ \ g_i(\boldsymbol{x}, \dot{\boldsymbol{v}}) \leqslant 0 \ \forall i \in [k] \tag{b3}$$

Privacy-preserving Obfuscation mechanism

Fidelity:

G^p admits a solution satisfying all the constraints of P and β-faithful to the objective of P

Not too far from the obfuscated solution

Only use: *Public Information*

$$P_{\mathrm{BL}} = \min_{(\dot{\boldsymbol{v}}, \boldsymbol{x})} \|\dot{\boldsymbol{v}} - \tilde{\boldsymbol{v}}\|_2 \quad \text{(b1)}$$

$$\text{s.t.: } |\mathcal{O}(\boldsymbol{x}^*, \dot{\boldsymbol{v}}) - \mathcal{O}^*| \leqslant \beta \quad \text{(b2)}$$

$$\boldsymbol{x}^* = \operatorname{argmin}_{\boldsymbol{x}} \mathcal{O}(\boldsymbol{x}, \dot{\boldsymbol{v}}) \quad \text{(b3)}$$

$$\text{s.t. } g_i(\boldsymbol{x}, \dot{\boldsymbol{v}}) \leqslant 0 \; \forall i \in [k]$$

Beta faithful to the original objective costs

Satisfying the constraints

Privacy-preserving Obfuscation mechanism

Fidelity:

G^p admits a solution satisfying all the constraints of P and β-faithful to the objective of P

Not too far from the obfuscated solution

$$P_{\mathrm{BL}} = \min_{(\dot{\boldsymbol{v}}, \boldsymbol{x})} \|\dot{\boldsymbol{v}} - \tilde{\boldsymbol{v}}\|_2 \quad \text{(b1)}$$

$$\text{s.t.: } |\mathcal{O}(\boldsymbol{x}^*, \dot{\boldsymbol{v}}) - \mathcal{O}^*| \leqslant \beta \quad \text{(b2)}$$

$$\boldsymbol{x}^* = \operatorname{argmin}_{\boldsymbol{x}} \ \mathcal{O}(\boldsymbol{x}, \dot{\boldsymbol{v}}) \quad \text{s.t.} \ \ g_i(\boldsymbol{x}, \dot{\boldsymbol{v}}) \leqslant 0 \ \forall i \in [k] \quad \text{(b3)}$$

Theorem 4 *The error induced by POCIN on the CIN node values is bounded by the inequality:* $\|\dot{\boldsymbol{v}} - \boldsymbol{v}\|_2 \leqslant 2\|\tilde{\boldsymbol{v}} - \boldsymbol{v}\|_2$.

Solving the Fidelity Restoration Model

- General Bi-level Programs
  - NP-hard, even for just evaluating a solution

➡Solution:

- If subproblem is convex:
  - The subproblem can be approximated via *Karush-Kuhn-Tucker (KKT)* conditions → reduced to single-level
- If subproblem is linear:
  - The problem can be reformulated as a *mixed-integer program*
- Relaxation method:
  - *Relax the optimality condition* for the subproblem

Experimental Evaluations

- Two case studies:

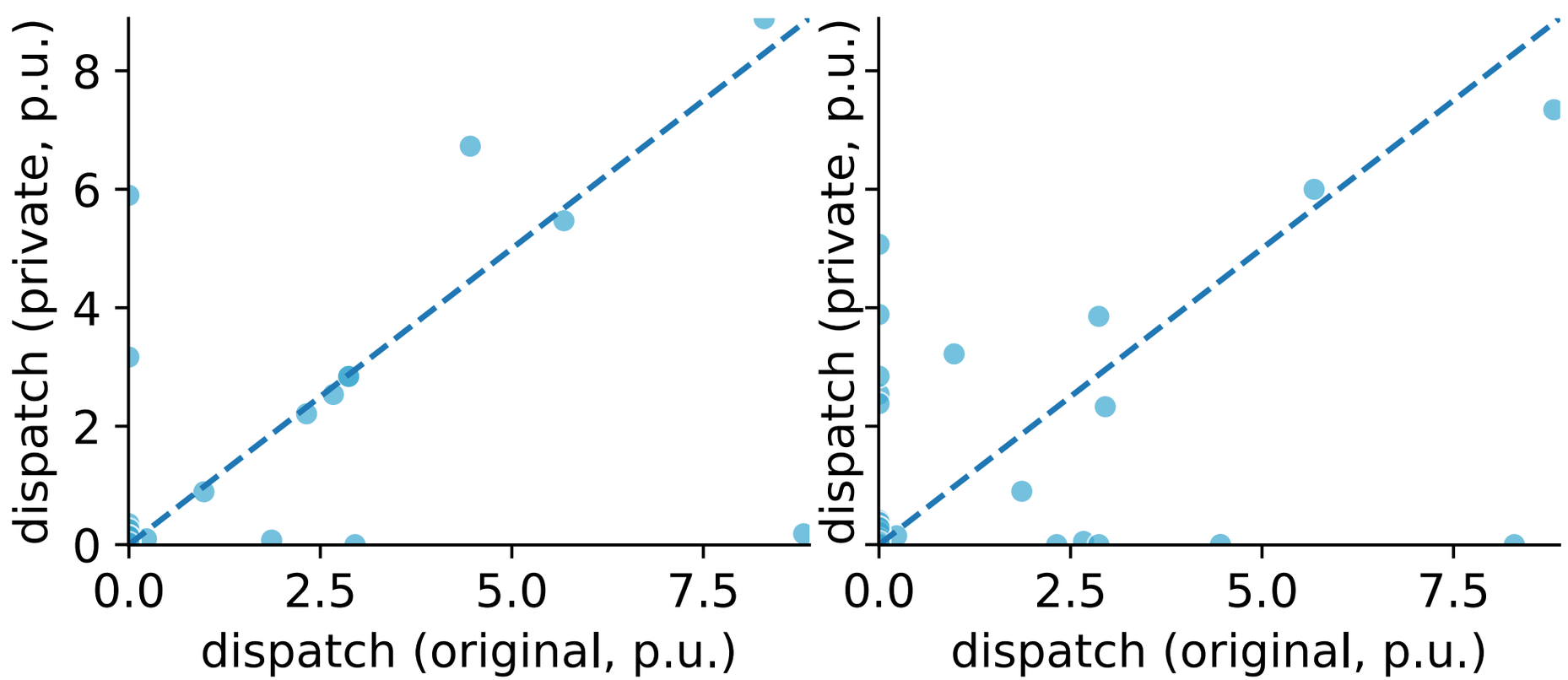
  1)Power Systems

  2)Traffic network & data

- Power Systems
  - Goal: Release the power network where:
    - Location of the generators are obfuscated (α_l =1% - 10%)
    - Capacities of the generators are obfuscated (α_v = 10MW)
    - The optimal AC power flow has to be similar (w.r.t β = 1%-10%)
  - Benchmark: various IEEE benchmarks Tools: Julia/PowerModels.jl
  - *Validate: Privacy, Fidelity, and Robustness criteria*

Privacy

Dispatch distance



Generator active dispatch: Original optimal solution vs Obfuscated optimal solution

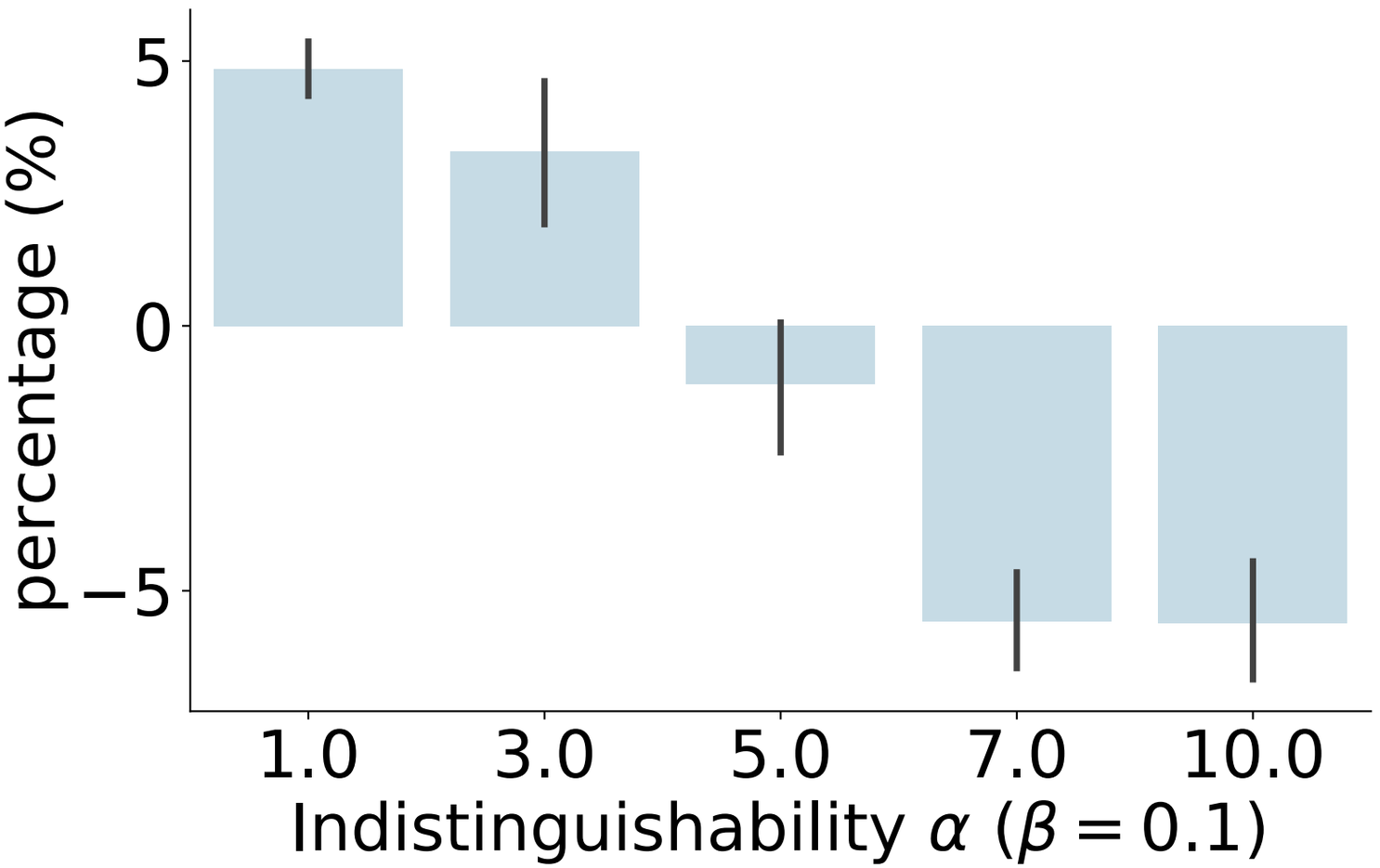
Georgia Tech

Without Fidelity Restoration

	α				
Network instance	1	3	5	7	10
nesta_case14_ieee	6	6	6	6	6
nesta_case30_ieee	0	0	0	0	0
nesta_case57_ieee	12	10	6	12	12
nesta_case118_ieee	0	0	0	0	0

Percentage (%) of instances converges to a feasible AC power flow on various α_l (over 50 different seeds)

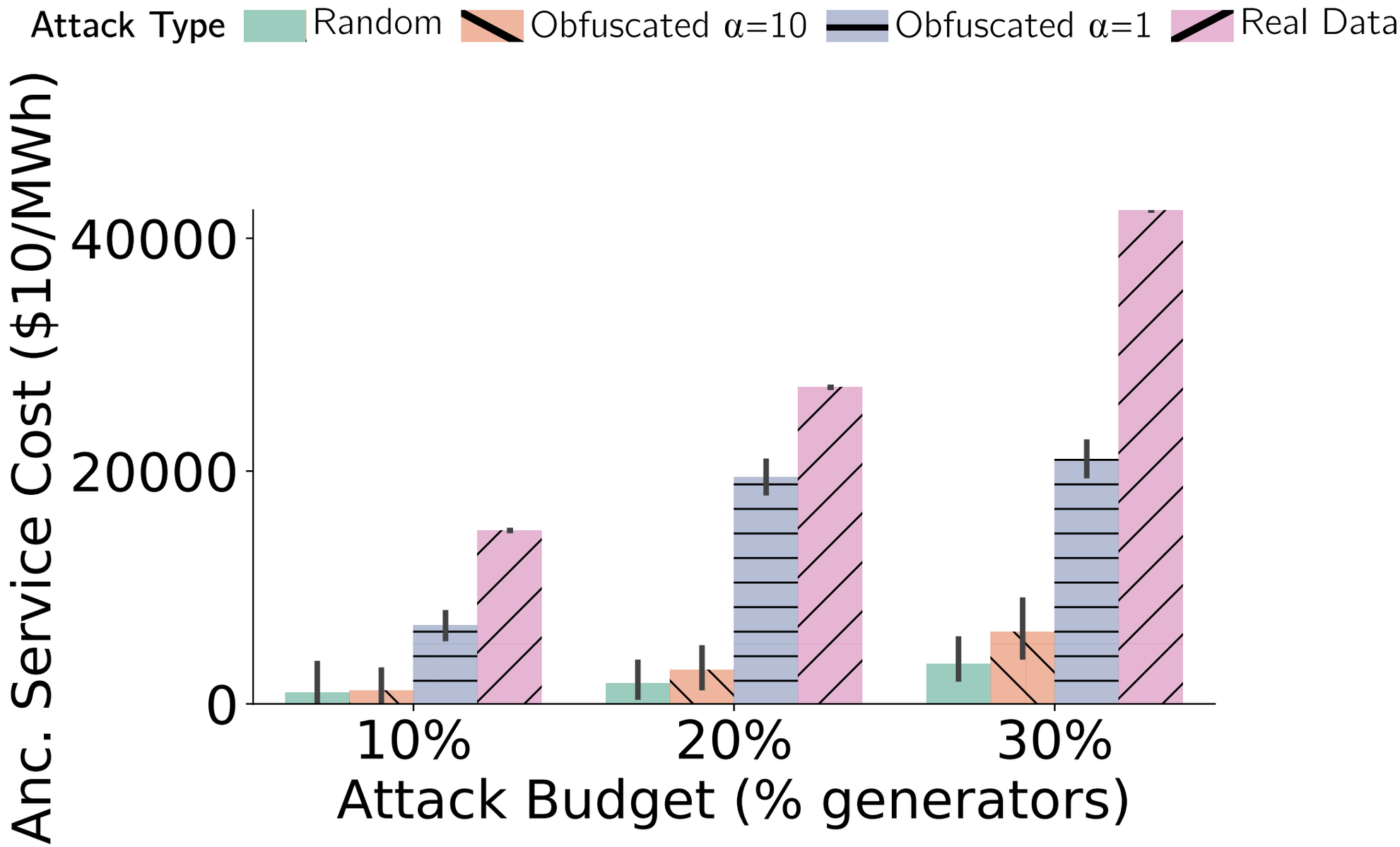
Fidelity



Percentage difference on the objective costs: original network vs Obfuscated network

Georgia Tech

Robustness



IEEE-118 bus - Estimated Recovery Cost on the objective costs: original network vs Obfuscated network (over 50 runs)

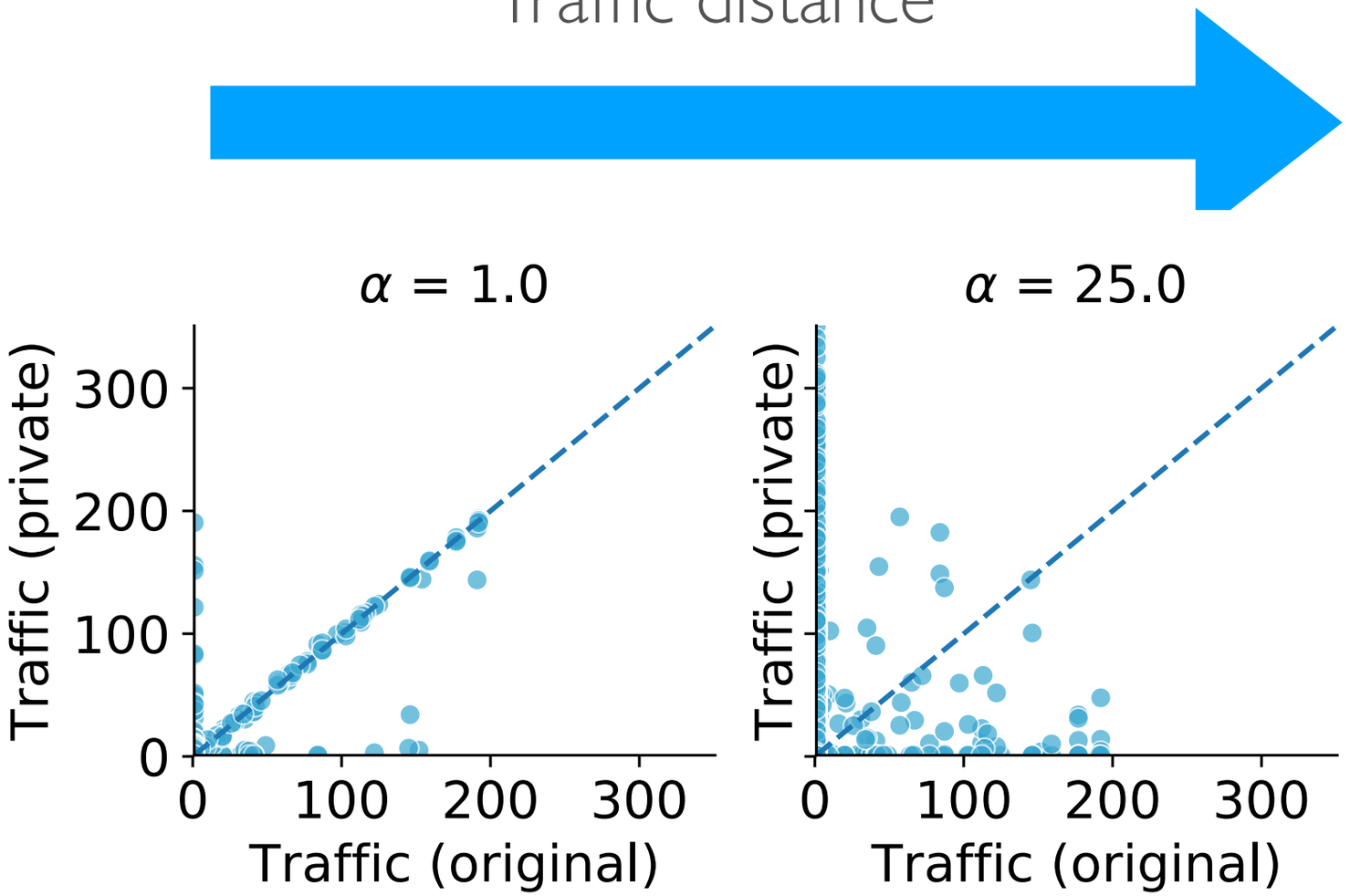
Georgia Tech

Experimental Evaluations

- Traffic Network Obfuscation Problem
  - Goal: Release the traffic data
    - Location of the roads are obfuscated (α_l : 1% - 25%)
    - Traffic data of each road are obfuscated (α_v)
    - Preserve the shortest trip durations of commuters (w.r.t β =10%)
  - Benchmark: Ann Arbor traffic data with 8000 real trips
  - Simplification: Travel times = distance + weight constant * traffic
  - Tools: Julia
  - *Validate: Privacy, Fidelity, and Robustness criteria*

Privacy

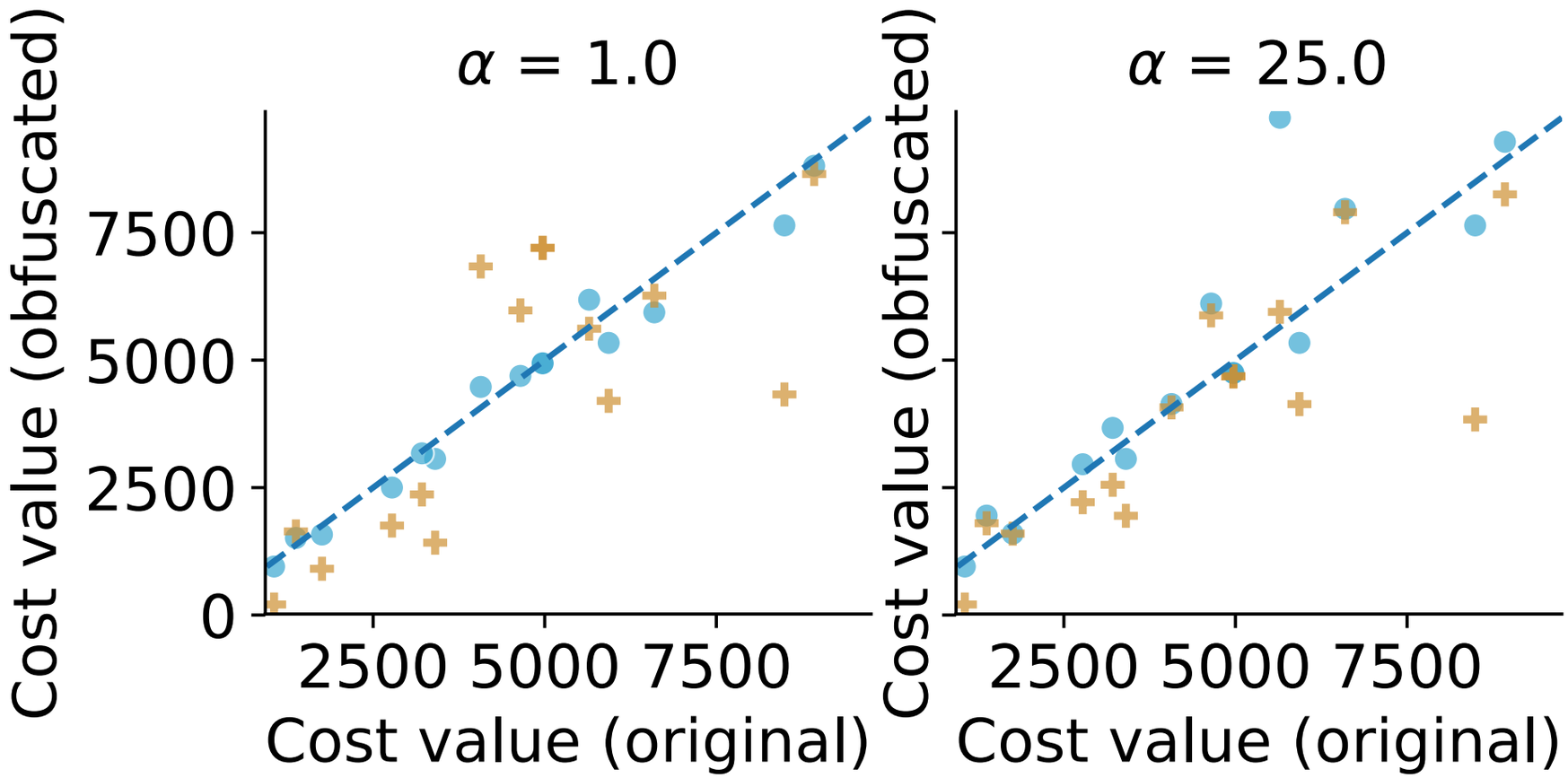
Traffic distance



Traffic costs: original network vs obfuscated network

Georgia Tech

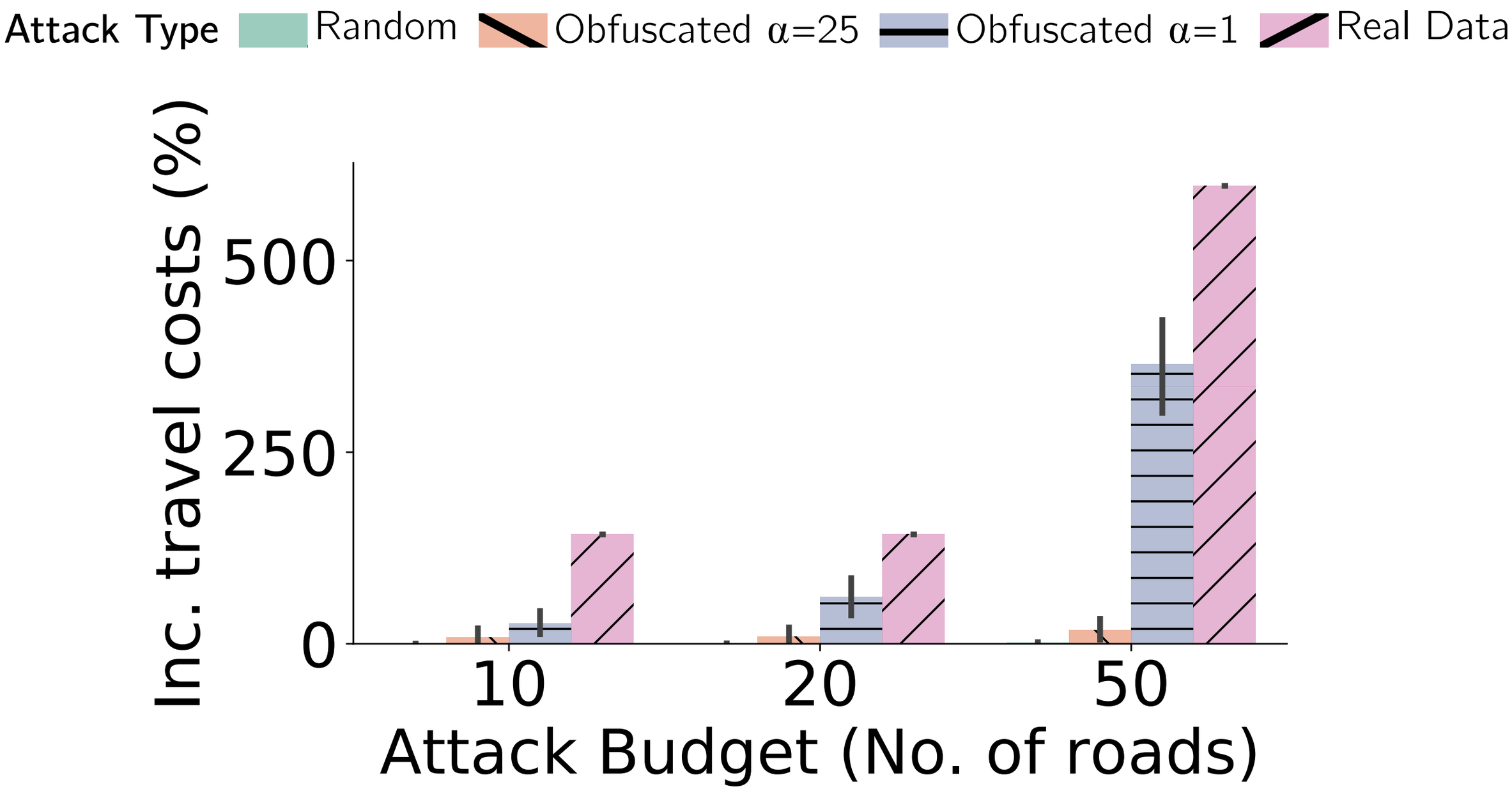
Fidelity



Travel costs (based on distance and traffic weights):
original network vs obfuscated network

Georgia Tech

Robustness



Increase travel costs (%):
original network vs obfuscated network (over 50 runs)

Georgia Tech

Conclusions

- Presented:
  - A privacy-preserving scheme for release of Critical Infrastructure Networks.
- The scheme:
  - Obfuscate values and locations of sensitive network elements using differential privacy and bi-level programs
  - Preserves the properties of an optimization problem of interests
- Experimental results:
  - Two domain: Power System & Traffic Networks, with real data
  - Validate the effectiveness to deceive malicious agents

Ask us any additional question at the poster session

Thank you!

fioretto@gatech.edu
wmak@gatech.edu
pvh@isye.gatech.edu