# UC-Lab Center for Distribution System Cybersecurity

Mahnoosh Alizadeh, UCSB

March 2019

# Energy management schemes in distribution networks

- The rise of smart metering technologies, flexible loads and distributed generation resources (e.g., solar) has opened new doors to improve efficiency and reliability at the distribution level

# Energy management schemes in distribution networks

- The rise of smart metering technologies, flexible loads and distributed generation resources (e.g., solar) has opened new doors to improve efficiency and reliability at the distribution level

- Design control and market operation algorithms to coordinate smart loads and distribution generation

# Higher efficiency comes at the risk of higher vulnaribility

Heavy digitalization and connectivity through smart metering, IoT devices, smart appliances and communication networks significantly increases the attack surface of the grid at the distribution level

# Higher efficiency comes at the risk of higher vulnaribility

Heavy digitalization and connectivity through smart metering, IoT devices, smart appliances and communication networks significantly increases the attack surface of the grid at the distribution level

**Main reserach question**

Given these new vulnaribitilies, how can we design secure demand response architectures?

# Higher efficiency comes at the risk of higher vulnaribility

Heavy digitalization and connectivity through smart metering, IoT devices, smart appliances and communication networks significantly increases the attack surface of the grid at the distribution level

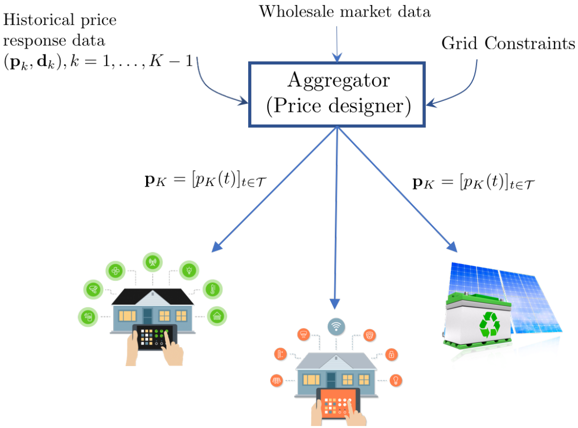
**Main reserach question**

Given these new vulnaribitilies, how can we design secure demand response architectures?

Let us first do a high-level review of demand response architectures

# Architecture #1: Centralized real-time pricing algorithms

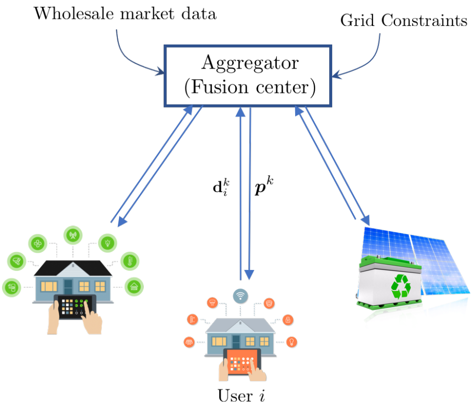
- At the beginning of each day, aggregator posts hourly varying prices
- Essentially an open loop strategy.




Price design based on learned price response from past interactions

# Architecture #2: Distributed coordination algorithms

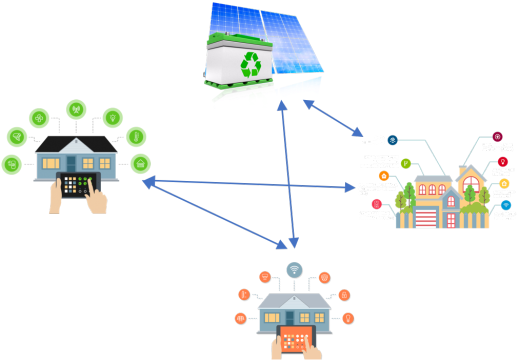
- Decentralized solutions allow users to coordinate to maximize welfare
- Aggregator acts as fusion center for decentralized algorithms




Based on Lagrangian dual decomposition alg $\rightarrow$ Pull demand and push updated electricity price (dual iterates) until convergence

# Architecture #3: Decentralized coordinated algorithms

- No fusion center, only communication with neighbors.



Uses consensus protocols to estimate optimal market clearning prices based on local computation and collaborative message passing

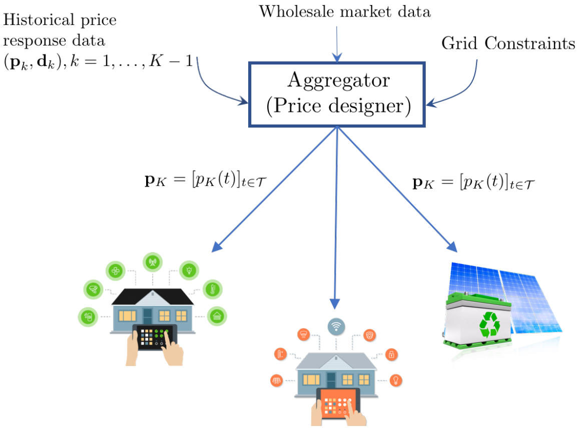
Let us focus on our progress in the **centralized scheme** first

Let us focus on our progress in the **centralized scheme** first

Suprisingly, this is not as well-studied as decentralized and distributed schemes

# Architecture #1: Real-time pricing algorithms

- At the beginning of each day, aggregator posts hourly varying prices
- Essentially an open loop strategy.




Price design based on learned price response from past interactions

# Architecture #1: Real-time pricing algorithms

**Main Question**

How to learn the price response of a population of customers to minimize running costs of an aggregator without endangering the distribution grid?

Challenges:

1. Stochastic and unknown nature of customer behavior
2. Variable daily aggregator cost due to changing conditions
3. Small size of the observation

# Problem setup

- Every day $t$, aggregator posts price $\mathbf{p_t} \in \mathcal{P} \rightarrow$ observes $\boldsymbol{\ell}^{\star}(\mathbf{p_t})$

# Problem setup

- Every day $t$, aggregator posts price $\mathbf{p_t} \in \mathcal{P} \rightarrow$ observes $\boldsymbol{\ell}^\star(\mathbf{p_t})$
- Daily context $\mathbf{d_t}$ drawn iid from a finite set $\mathcal{D}$

# Problem setup

- Every day $t$, aggregator posts price $\mathbf{p_t} \in \mathcal{P} \rightarrow$ observes $\boldsymbol{\ell}^\star(\mathbf{p_t})$
- Daily context $\mathbf{d_t}$ drawn iid from a finite set $\mathcal{D}$

**Aggregator's goal?**

$$\min_{\mathbf{p}_t} \sum_{t=1}^{T} g(\boldsymbol{\ell}^\star(\mathbf{p_t}), \mathbf{d_t})$$

s.t. grid safety constraints

# Problem setup

- Every day $t$, aggregator posts price $\mathbf{p_t} \in \mathcal{P} \to$ observes $\boldsymbol{\ell}^\star(\mathbf{p_t})$
- Daily context $\mathbf{d_t}$ drawn iid from a finite set $\mathcal{D}$

**Aggregator's goal?**

$$\min_{\mathbf{p}_t} \quad \sum_{t=1}^{T} g(\boldsymbol{\ell}^\star(\mathbf{p_t}), \mathbf{d_t})$$

s.t. grid safety constraints

# Problem setup

- Every day $t$, aggregator posts price $\mathbf{p_t} \in \mathcal{P} \rightarrow$ observes $\boldsymbol{\ell}^\star(\mathbf{p_t})$
- Daily context $\mathbf{d_t}$ drawn iid from a finite set $\mathcal{D}$

**Aggregator's goal?**

$$\min_{\mathbf{p}_t} \sum_{t=1}^{T} g(\boldsymbol{\ell}^\star(\mathbf{p_t}), \mathbf{d_t})$$

s.t. grid safety constraints

How do we model the load response to prices $\boldsymbol{\ell}^\star(\mathbf{p}_t)$?

$$\mathbb{E}[\boldsymbol{\ell}^\star(\mathbf{p}_t)] = \sum_{i=1}^{Q} a_i(\boldsymbol{\theta}, \mathbf{p}_t)\boldsymbol{\ell}_i^\star(\mathbf{p}_t)$$

# Problem setup

- Every day $t$, aggregator posts price $\mathbf{p_t} \in \mathcal{P} \rightarrow$ observes $\boldsymbol{\ell}^\star(\mathbf{p_t})$
- Daily context $\mathbf{d_t}$ drawn iid from a finite set $\mathcal{D}$

**Aggregator's goal?**

$$\min_{\mathbf{p}_t} \sum_{t=1}^{T} g(\boldsymbol{\ell}^\star(\mathbf{p_t}), \mathbf{d_t})$$

s.t. grid safety constraints

How do we model the load response to prices $\boldsymbol{\ell}^\star(\mathbf{p}_t)$?

$$\mathbb{E}[\boldsymbol{\ell}^\star(\mathbf{p}_t)] = \sum_{i=1}^{Q} a_i(\boldsymbol{\theta}, \mathbf{p}_t)\boldsymbol{\ell}_i^\star(\mathbf{p}_t)$$

So based on the physical characteristics of the problem,
we have reduced the challenge to not knowing the parameter $\boldsymbol{\theta}$

# Background: multi-armed bandits

- We adopt a multi-armed bandit based solution for this problem

# Background: multi-armed bandits

- We adopt a multi-armed bandit based solution for this problem
- The name: imagine a gambler at a row of slot machines who has to decide which machines to play if he has $N$ coins.


- Stochastic payoffs with different expected value $\theta_i$ for slot machine $i$
- Goal: Maximize payoff over the $N$ limited plays $\rightarrow$ The strategy should not be focused solely on finding the highest paying machine
- Exploration-Exploitation tradeoff

# Background: multi-armed bandits

- We adopt a multi-armed bandit based solution for this problem
- The name: imagine a gambler at a row of slot machines who has to decide which machines to play if he has $N$ coins.

- Stochastic payoffs with different expected value $\theta_i$ for slot machine $i$
- Goal: Maximize payoff over the $N$ limited plays $\rightarrow$ The strategy should not be focused solely on finding the highest paying machine
- Exploration-Exploitation tradeoff
- Two well-known heuristics with performance guarantees: UCB and Thompson Sampling (confidence region vs. probability distribution)

# Real-time pricing based on multi-armed bandits

**Aggregator's problem**

$$\min_{\mathbf{p}_t} \; \mathbb{E}\left[\sum_{t=1}^{T} g(\boldsymbol{\ell}^\star(\mathbf{p_t}) + \text{noise}, \mathbf{d_t})\right]$$

s.t. grid safety constraints

where

$$\boldsymbol{\ell}^\star(\mathbf{p}_t) = \sum_{i=1}^{Q} a_i(\boldsymbol{\theta}, \mathbf{p}_t)\boldsymbol{\ell}_i^\star(\mathbf{p}_t)$$

# Real-time pricing based on multi-armed bandits

**Aggregator's problem**

$$\min_{\mathbf{p}_t} \; \mathbb{E}\left[\sum_{t=1}^{T} g(\boldsymbol{\ell}^\star(\mathbf{p_t}) + \text{noise}, \mathbf{d_t})\right]$$

s.t. grid safety constraints

where

$$\boldsymbol{\ell}^\star(\mathbf{p}_t) = \sum_{i=1}^{Q} a_i(\boldsymbol{\theta}, \mathbf{p}_t)\boldsymbol{\ell}_i^\star(\mathbf{p}_t)$$

We have considered both Thompson Sampling and UCB based solutions and we are making progress on providing performance guarantees (regret)

# Real-time pricing based on multi-armed bandits

## Aggregator's problem

$$\min_{\mathbf{p}_t} \ \mathbb{E}\left[\sum_{t=1}^{T} g(\boldsymbol{\ell}^{\star}(\mathbf{p_t}) + \text{noise}, \mathbf{d_t})\right]$$

s.t. grid safety constraints

where

$$\boldsymbol{\ell}^{\star}(\mathbf{p}_t) = \sum_{i=1}^{Q} a_i(\boldsymbol{\theta}, \mathbf{p}_t)\boldsymbol{\ell}_i^{\star}(\mathbf{p}_t)$$

We have considered both Thompson Sampling and UCB based solutions and we are making progress on providing performance guarantees (regret)

A. Moradipari, C. Silva, and M. Alizadeh, "Learning to Dynamically Price Electricity Demand Based on Multi-Armed Bandits"
(Thompson sampling performance without any safety constraints)

# How does Thompson Sampling work?

- A Bayesian approach that assumes a prior distribution $P(\boldsymbol{\theta})$ is available for the demand (e.g., through behavioral studies)

# How does Thompson Sampling work?

- A Bayesian approach that assumes a prior distribution $P(\boldsymbol{\theta})$ is available for the demand (e.g., through behavioral studies)

- We sample, in each round, a parameter $\boldsymbol{\theta}_t$ from this distribution
- We choose the best possible price $\mathbf{p}_t$ that minimizes cost assuming the true demand parameter is $\boldsymbol{\theta}_t$
- We observe a noisy version of the load response

$$\boldsymbol{\ell}^\star(\mathbf{p}_t) = \sum_{i=1}^{Q} a_i(\boldsymbol{\theta}, \mathbf{p}_t)\boldsymbol{\ell}_i^\star(\mathbf{p}_t)$$

- We update the distribution $P(\boldsymbol{\theta})$ based on our observation

# How does Thompson Sampling work?

- A Bayesian approach that assumes a prior distribution $P(\boldsymbol{\theta})$ is available for the demand (e.g., through behavioral studies)

- We sample, in each round, a parameter $\boldsymbol{\theta}_t$ from this distribution
- We choose the best possible price $\mathbf{p}_t$ that minimizes cost assuming the true demand parameter is $\boldsymbol{\theta}_t$
- We observe a noisy version of the load response

$$\boldsymbol{\ell}^\star(\mathbf{p}_t) = \sum_{i=1}^{Q} a_i(\boldsymbol{\theta}, \mathbf{p}_t)\boldsymbol{\ell}_i^\star(\mathbf{p}_t)$$

- We update the distribution $P(\boldsymbol{\theta})$ based on our observation

Question: How do we ensure grid safety?

# Reliability-aware MAB formulations

**Aggregator's problem**

$$\min_{\mathbf{p}_t} \sum_{t=1}^{T} g(\boldsymbol{\ell}^\star(\mathbf{p_t}), \mathbf{d_t})$$

$$\text{s.t.} \quad \mathbf{h}(\boldsymbol{\ell}^\star(\mathbf{p}_t), \mathbf{d}_t) \leq \mathbf{0} \qquad \text{(dist flow constraints)}$$

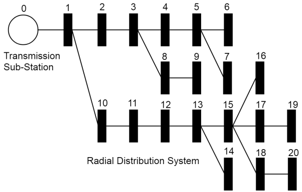
where

$$\boldsymbol{\ell}^\star(\mathbf{p}_t) = \sum_{i=1}^{Q} a_i(\boldsymbol{\theta}, \mathbf{p}_t)\boldsymbol{\ell}_i^\star(\mathbf{p}_t)$$

Potential approaches to ensure safety:

- Lagrangify the constraint (relaxation)
- Ensure the constraints hold with high probability

# Numerical experiment




$\ell^P_{i,t}$ : Active power demand at node $i$

$\ell^Q_{i,t}$ : Reactive power demand at node $i$

$s^P_{i,t}$ : Active power generation at node $i$

$s^Q_{i,t}$ : Reactive power generation at node $i$

$f^P_{i,t}$ : Active power flow on line $i$

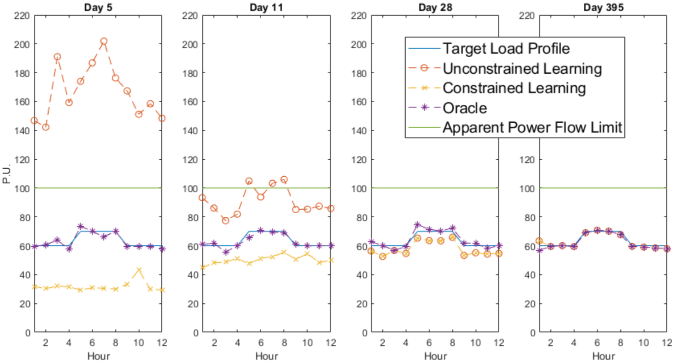
$f^Q_{i,t}$ : Reactive power flow on line $i$

$S^{max}_i$ : Apparent Power Limit of line $i$

$n_f$ : Likelihood of power flow constraint violations

$\mathbf{P}[(f^P_{i,t})^2 + (f^Q_{i,t})^2 \leq (S^{max}_i)^2] \geq 1 - n_f$

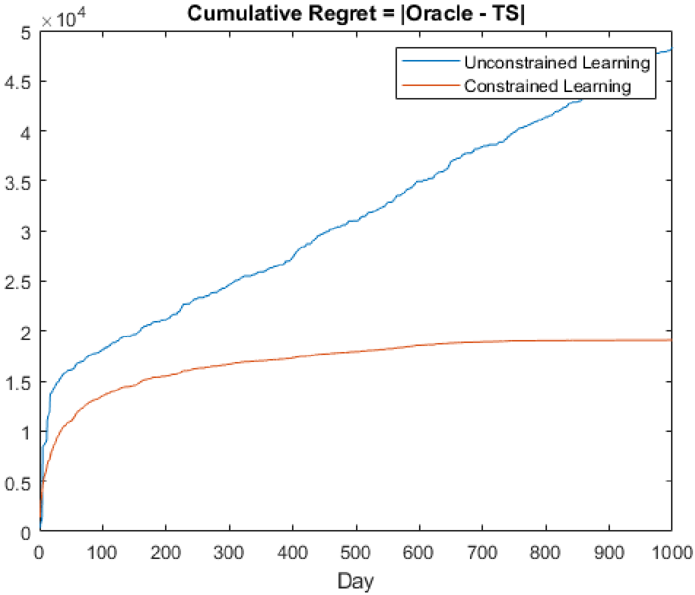
# Numerical experiment: case 1




Apparent Power Line Flow Limit violation ratios:

- Constrained case: 0.0017
- Unconstrained case: 0.1177

# Numerical experiment: case 2



Will discuss how this helps security in future work presentation

Will discuss how this helps security in future work presentation

Let's briefly look at the **distributed scheme** now
Ramtin will discuss the decentralized scheme

# Economic distpatch of distributed energy resources

- Individual agents are selfish price takers. They maximize payoff.
- Price responsive demand:

$$\max_{\mathbf{d}_j} \; U_j(\mathbf{d}_j) - \mathbf{p}^T \mathbf{d}_j$$

- Generators:

$$\max_{\mathbf{g}_v} \; \mathbf{p}^T \mathbf{g}_v - C_v(\mathbf{g}_v)$$

# Economic distpatch of distributed energy resources

- Individual agents are selfish price takers. They maximize payoff.
- Price responsive demand:

$$\max_{\mathbf{d}_j} \; U_j(\mathbf{d}_j) - \mathbf{p}^T \mathbf{d}_j$$

- Generators:

$$\max_{\mathbf{g}_v} \; \mathbf{p}^T \mathbf{g}_v - C_v(\mathbf{g}_v)$$

**Welfare maximization (economic dispatch) problem**

$$\begin{aligned} \max_{\mathbf{d},\mathbf{g}} \; & \sum_{j \in \mathcal{J}} U_j(\mathbf{d}_j) - \sum_{v \in \mathcal{V}} C_v(\mathbf{g}_v) \\ \text{s.t.} \; & \mathbf{1}^T \mathbf{d} = \mathbf{1}^T \mathbf{g} \qquad \text{(demand supply balance)} \\ & \mathbf{H}(\mathbf{d} - \mathbf{g}) \preceq \mathbf{c} \quad \text{(line capacity)} \end{aligned}$$

Constraints can be replaced with convexified distribution OPF models

# Market prices

## Welfare maximization (economic dispatch) problem

$$
\begin{aligned}
\max_{\mathbf{d},\mathbf{g}} \quad & \sum_{j \in \mathcal{J}} U_j(\mathbf{d}_j) - \sum_{v \in \mathcal{V}} C_v(\mathbf{g}_v) \\
\text{s.t.} \quad & \mathbf{1}^T\mathbf{d} = \mathbf{1}^T\mathbf{g} \qquad \text{(demand supply balance)} \\
& \mathbf{H}(\mathbf{d} - \mathbf{g}) \preceq \mathbf{c} \quad \text{(line capacity)}
\end{aligned}
$$

Why would selfish users follow the solution of this optimization problem?

# Market prices

## Welfare maximization (economic dispatch) problem

$$\max_{\mathbf{d},\mathbf{g}} \sum_{j \in \mathcal{J}} U_j(\mathbf{d}_j) - \sum_{v \in \mathcal{V}} C_v(\mathbf{g}_v)$$

$$\text{s.t.} \quad \mathbf{1}^T\mathbf{d} = \mathbf{1}^T\mathbf{g} \qquad \text{(demand supply balance)}$$

$$\mathbf{H}(\mathbf{d} - \mathbf{g}) \preceq \mathbf{c} \quad \text{(line capacity)}$$

Why would selfish users follow the solution of this optimization problem?

## "Pricing" the constraints → Locational Marginal Prices

Based on the Lagrange multipliers of the first and second constraint, we can define the market clearing prices at each bus that maximize welfare:

$$\mathbf{p} = \gamma \mathbf{1} + \mathbf{H}^T \boldsymbol{\mu}$$

# Market prices

## Welfare maximization (economic dispatch) problem

$$\max_{\mathbf{d},\mathbf{g}} \sum_{j \in \mathcal{J}} U_j(\mathbf{d}_j) - \sum_{v \in \mathcal{V}} C_v(\mathbf{g}_v)$$

$$\text{s.t.} \quad \mathbf{1}^T \mathbf{d} = \mathbf{1}^T \mathbf{g} \qquad \text{(demand supply balance)}$$

$$\mathbf{H}(\mathbf{d} - \mathbf{g}) \preceq \mathbf{c} \quad \text{(line capacity)}$$

Why would selfish users follow the solution of this optimization problem?

## "Pricing" the constraints $\rightarrow$ Locational Marginal Prices

Based on the Lagrange multipliers of the first and second constraint, we can define the market clearing prices at each bus that maximize welfare:

$$\mathbf{p} = \gamma \mathbf{1} + \mathbf{H}^T \boldsymbol{\mu}$$

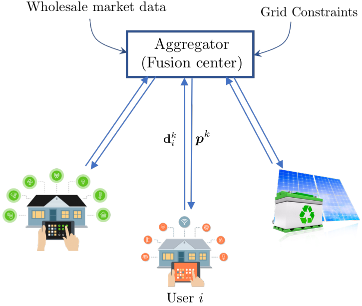
But no single entity knows $U_j(d_j)$ (and potentially $C_v(g_v)$)! So what should we do?

# Decentralized calculation of prices

## Welfare maximization (economic dispatch) problem

$$
\begin{aligned}
\max_{\mathbf{d},\mathbf{g}} \quad & \sum_{j\in\mathcal{J}} U_j(\mathbf{d}_j) - \sum_{v\in\mathcal{V}} C_v(\mathbf{g}_v) \\
\text{s.t.} \quad & \mathbf{1}^T\mathbf{d} = \mathbf{1}^T\mathbf{g} \qquad \text{(demand supply balance)} \\
& \mathbf{H}(\mathbf{d}-\mathbf{g}) \preceq \mathbf{c} \quad \text{(line capacity)}
\end{aligned}
$$

In dual decomposition the constraints are "priced" and then the dual problem is solved $\rightarrow$ dual problem solved via decentralized schemes



# Distributed calculation of prices

### Welfare maximization (economic dispatch) problem

$$\max_{\mathbf{d},\mathbf{g}} \sum_{j\in\mathcal{J}} U_j(\mathbf{d}_j) - \sum_{v\in\mathcal{V}} C_v(\mathbf{g}_v)$$

$$\text{s.t.}\quad \mathbf{1}^T\mathbf{d} = \mathbf{1}^T\mathbf{g} \qquad \text{(demand supply balance)}$$

$$\mathbf{H}(\mathbf{d}-\mathbf{g}) \preceq \mathbf{c} \qquad \text{(line capacity)}$$

### Dual-decomposition based approach:

- Fusion center updates $\mathbf{p}^{(k)} = \gamma^{(k)}\mathbf{1} + \mathbf{H}^T\boldsymbol{\mu}^{(k)}$ (say using dual subgradient methods)
- Given prices, each individual user solves:

$$\max_{\mathbf{d}_j^{(k)}} U_j(\mathbf{d}_j^{(k)}) - \mathbf{p}^T\mathbf{d}_j^{(k)}, \qquad \max_{\mathbf{g}_v^{(k)}} \mathbf{p}^{(k)\,T}\mathbf{g}_v^{(k)} - C_v(\mathbf{g}_v^{(k)})$$

and shares $\mathbf{d}_j^{(k)}$ and $\mathbf{g}_v^{(k)}$ with fusion center

# The attack surface for distributed schemes

## Dual-ascent based approach

- Fusion center updates $\mathbf{p}^{(k)} = \gamma^{(k)}\mathbf{1} + \mathbf{H}^T\boldsymbol{\mu}^{(k)}$ (say using dual subgradient methods)
- Given prices, each individual user solves:

$$\max_{\mathbf{d}_j^{(k)}} \; U_j(\mathbf{d}_j^{(k)}) - \mathbf{p}^T\mathbf{d}_j^{(k)}, \quad \max_{\mathbf{g}_v^{(k)}} \; {\mathbf{p}^{(k)}}^T\mathbf{g}_v^{(k)} - C_v(\mathbf{g}_v^{(k)})$$

and shares $\mathbf{d}_j^{(k)}$ and $\mathbf{g}_v^{(k)}$ with fusion center

Alternatively, we can also perform a gradient descent/ascent on the primal/dual variables (a primal/dual approach)

# The attack surface for distributed schemes

## Dual-ascent based approach

- Fusion center updates $\mathbf{p}^{(k)} = \gamma^{(k)}\mathbf{1} + \mathbf{H}^T\boldsymbol{\mu}^{(k)}$ (say using dual subgradient methods)
- Given prices, each individual user solves:

$$\max_{\mathbf{d}_j^{(k)}} \; U_j(\mathbf{d}_j^{(k)}) - \mathbf{p}^T\mathbf{d}_j^{(k)}, \quad \max_{\mathbf{g}_v^{(k)}} \; \mathbf{p}^{(k)\,T}\mathbf{g}_v^{(k)} - C_v(\mathbf{g}_v^{(k)})$$

and shares $\mathbf{d}_j^{(k)}$ and $\mathbf{g}_v^{(k)}$ with fusion center

Alternatively, we can also perform a gradient descent/ascent on the primal/dual variables (a primal/dual approach)

A man-in-the-middle attack may easily drive the algorithm to diverge, resulting in an unstable system

# The attack surface for distributed schemes

## Dual-ascent based approach

- Fusion center updates $\mathbf{p}^{(k)} = \gamma^{(k)}\mathbf{1} + \mathbf{H}^T\boldsymbol{\mu}^{(k)}$ (say using dual subgradient methods)
- Given prices, each individual user solves:

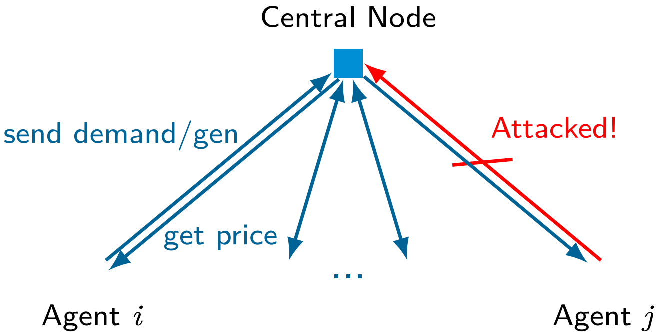
$$\max_{\mathbf{d}_j^{(k)}} \; U_j(\mathbf{d}_j^{(k)}) - \mathbf{p}^T\mathbf{d}_j^{(k)}, \quad \max_{\mathbf{g}_v^{(k)}} \; \mathbf{p}^{(k)\,T}\mathbf{g}_v^{(k)} - C_v(\mathbf{g}_v^{(k)})$$

and shares $\mathbf{d}_j^{(k)}$ and $\mathbf{g}_v^{(k)}$ with fusion center

Alternatively, we can also perform a gradient descent/ascent on the primal/dual variables (a primal/dual approach)

A man-in-the-middle attack may easily drive the algorithm to diverge, resulting in an unstable system $\rightarrow$ true for any NUM formulation

# Attack-resilient network utitlity maximization?



# Attack-resilient network utitlity maximization?

Assume some of the $d_i$ iterates are adverserially chosen by an attacker in the following classical problem:

$$\begin{aligned}
&\min_{d_i \in \mathbb{R}^d, \forall i} \frac{1}{N} \sum_{i=1}^{N} U_i(d_i) \\
&\text{s.t.} \quad g_t\left(\frac{1}{N}\sum_{i=1}^{N} d_i\right) \leq 0, \ t = 1, ..., T, \\
&\qquad\quad d_i \in \mathcal{C}_i, \ \forall i.
\end{aligned}$$

# Attack-resilient network utitlity maximization?

Assume some of the $d_i$ iterates are adverserially chosen by an attacker in the following classical problem:

$$\begin{aligned}
&\min_{d_i \in \mathbb{R}^d, \forall i} \frac{1}{N} \sum_{i=1}^{N} U_i(d_i) \\
&\text{s.t.} \quad g_t\left(\frac{1}{N}\sum_{i=1}^{N} d_i\right) \leq 0, \;\; t = 1, ..., T, \\
&\qquad\quad d_i \in \mathcal{C}_i, \;\; \forall i.
\end{aligned}$$

Important observation: the dual ascent iteration would depend only on the emperical mean $\overline{d}^{(k)} = \frac{1}{N}\sum_{i=1}^{N} d_i^{(k)}$.

# Attack-resilient network utitlity maximization?

Assume some of the $d_i$ iterates are adverserially chosen by an attacker in the following classical problem:

$$\begin{aligned} \min_{d_i \in \mathbb{R}^d, \forall i} \ & \frac{1}{N} \sum_{i=1}^{N} U_i(d_i) \\ \text{s.t.} \quad & g_t\left(\frac{1}{N}\sum_{i=1}^{N} d_i\right) \leq 0, \ t = 1, ..., T, \\ & d_i \in \mathcal{C}_i, \ \forall i. \end{aligned}$$

Important observation: the dual ascent iteration would depend only on the emperical mean $\overline{d}^{(k)} = \frac{1}{N}\sum_{i=1}^{N} d_i^{(k)}$.

**The trick**

Apply recent techniques from robust statistics to estimate the correct mean for unaffected agents in the presence of byzantine attacks.

# Overall idea

- Under Byzantine attack $\rightarrow$ impossible to optimize the original problem since the contribution from attacked agents becomes unknown to the fusion center $\rightarrow$ Focus only on trustworth agents:

$$\begin{aligned} \min_{d_i \in \mathbb{R}^d, \forall i \in \mathcal{H}} \ & \frac{1}{|\mathcal{H}|} \sum_{i \in \mathcal{H}} U_i(d_i) \\ \text{s.t.} \quad & g_t\left(\frac{1}{N}\sum_{i=1}^{N} d_i\right) \leq 0, \ t = 1, ..., T, \\ & d_i \in \mathcal{C}_i, \ \forall i \in \mathcal{H}. \end{aligned}$$

Note that the identity of the trustworthy agents ($\mathcal{H}$) are unknown

We will show that the robustified distributed method converges geometrically to a neighborhood of the optimal solution, where the radius of the neighborhood is proportional to the fraction of affected agents

Thank you!