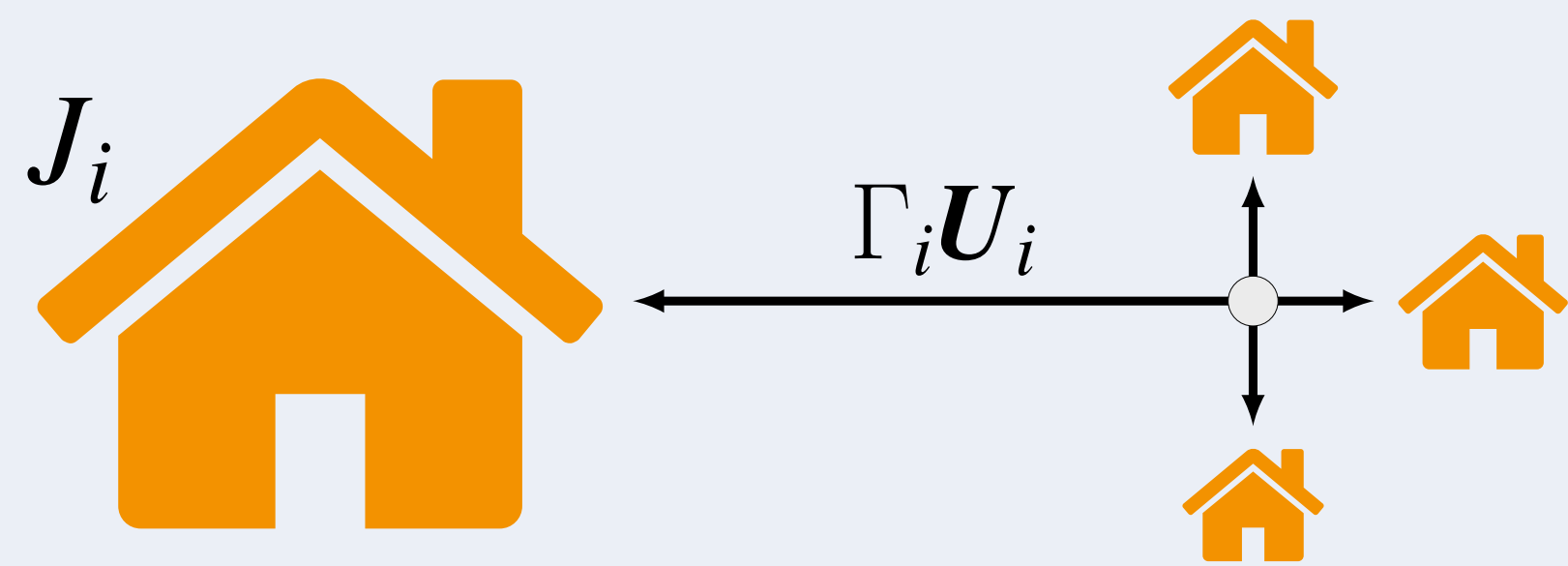




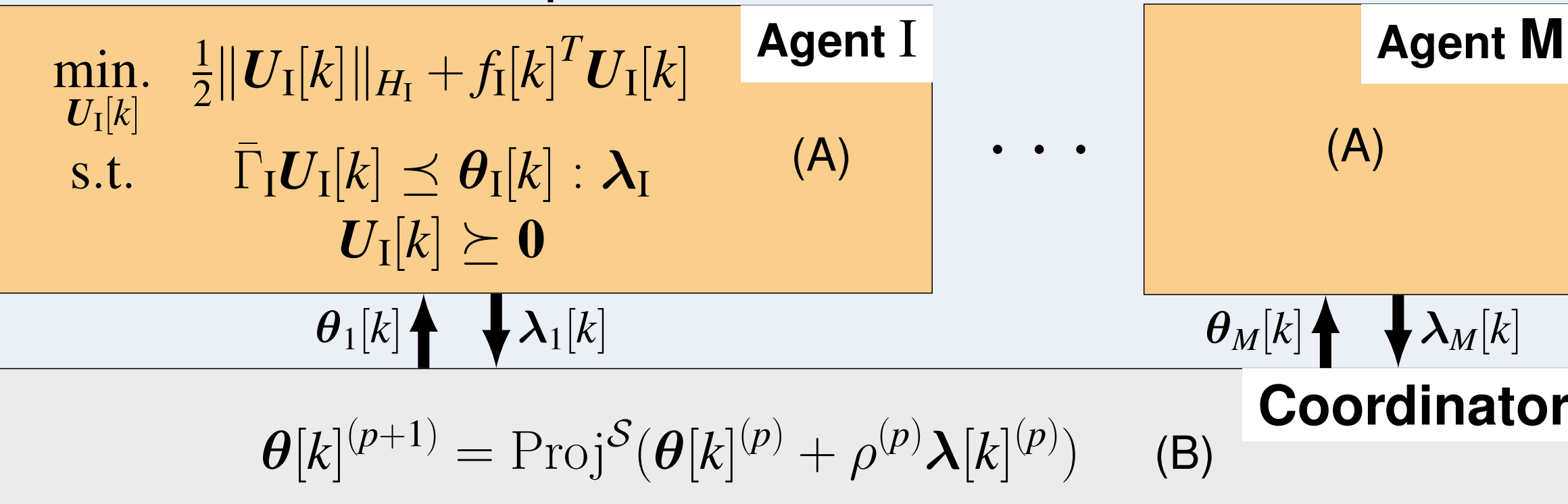
1. Challenge - False Data injection in dMPC exchange

- ▶ Decomposable quadratic objective $\sum_{i=1}^M J_i$
- ▶ Coupling constraint $\sum_{i=1}^M \Gamma_i U_i \leq U_{\max}$



Solution

Primal Decomposition based distributed MPC



Coordinator allocates θ_i
Agent has dissatisfaction λ_i

What happens if an agent lies about λ_i ?



2. Attack and consequences

- ▶ λ_i is the dissatisfaction of i to allocation θ_i
- ▶ Attacker increases λ_i using function $\gamma(\cdot)$
- ▶ \uparrow dissatisfaction == \uparrow allocation

Assumption

Attacker chooses an *invertible linear function*

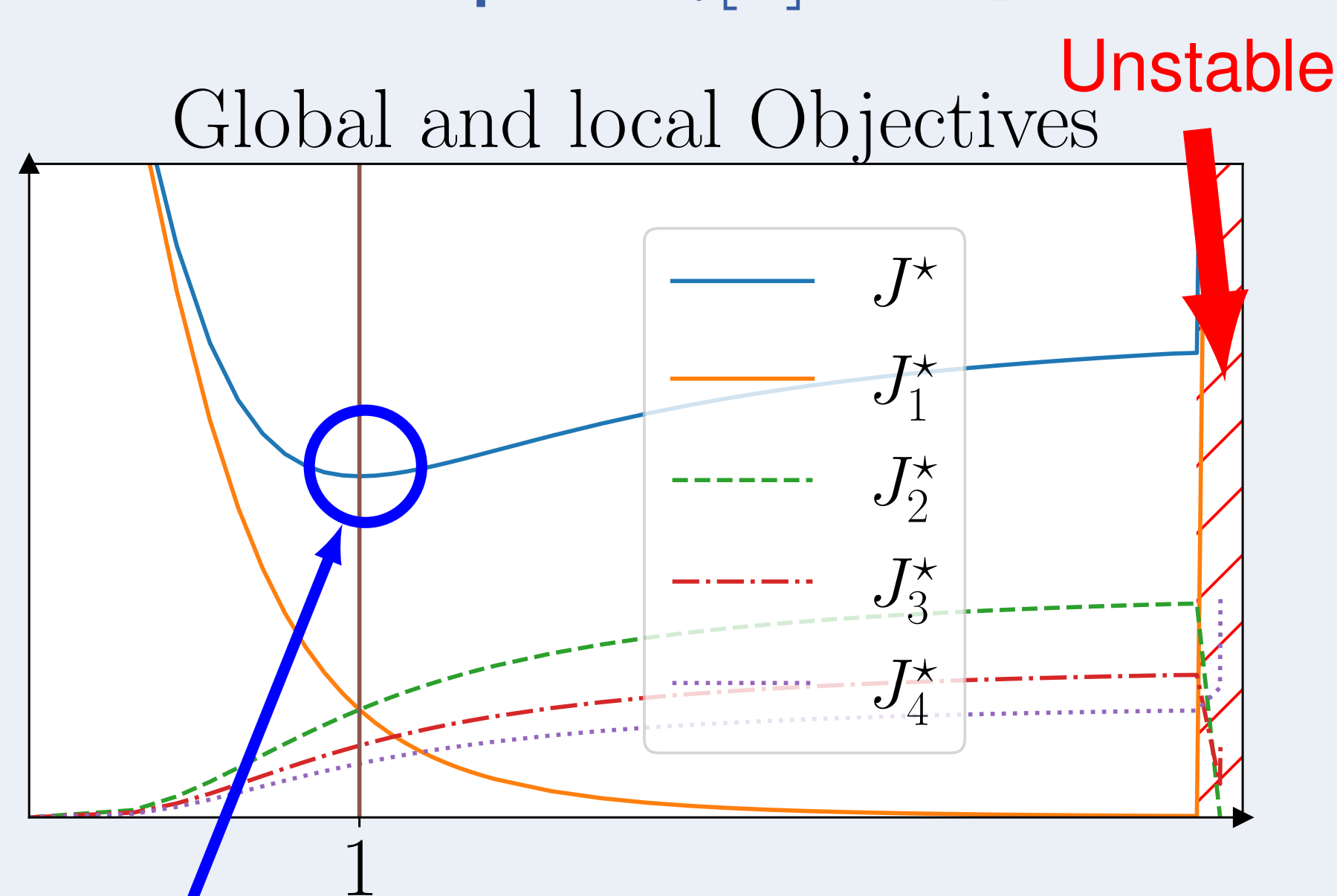
$$\tilde{\lambda}_i = \gamma_i(\lambda_i) = T_i[k] \lambda_i,$$

Remark

Attacker says it is satisfied only if it is

- ▶ Effects of cheating matrix $T_i[k]$
- ▶ Increase on global objective
- ▶ Destabilization

Example $T_i[k] = \tau_1 I$



Optimal objective

τ_1

Can we mitigate the effects?

YES! If we estimate $T_i[k]$ and invert it
But how?

3. Estimating cheating matrix $T_i[k]$

Local problems (A) are **QP**

Explicit Solution with PWA form w.r.t θ_i :

$$\lambda_i[k] = -P_i^n \theta_i[k] - s_i^n[k], \text{ if } G_i^n[k] \theta_i[k] \preceq b_i^n[k] \quad (C)$$

with $n \in \{1 : N\}$. $G_i^n[k]$ and $b_i^n[k]$ define regions.

Remark

Sensibilities P_i^n are time invariant.

Another assumption

In Region 1 **local constraints are active**:

$$\lambda_i[k] = -P_i^1 \theta_i[k] - s_i^1[k], \text{ if } G_i^1[k] \theta_i[k] \preceq b_i^1[k] \quad (D)$$

and $\theta_i = \mathbf{0}$ belongs to it

Attacker **modifies sensibility** $\tilde{P}_i[k] = T_i[k] \bar{P}_i$

If we can know **nominal** \bar{P}_i^1 ,
by estimating $\tilde{P}_i[k]$, we can find $T_i[k]^{-1}$:

$$\widehat{T_i[k]^{-1}} = \bar{P}_i^1 \widehat{\tilde{P}_i[k]}^{-1} \quad (E)$$

But how do we estimate $\tilde{P}_i^1[k]$?

Enter Expectation Maximization

- ▶ Classify data in regions (latent variables)
- ▶ Estimates parameters using weighted LS

EM needs minimally excited inputs θ_i and $\tilde{\lambda}_i$.

- ▶ During negotiation (time dependence)
- ▶ Solution: estimate in a separate phase
- ▶ Generate independent points near $\theta_i = \mathbf{0}$

Artificial Scarcity Sampling

4. Expectation Maximization

- ▶ Regions are indexed by $z \in \mathcal{Z} = \{1 : Z\}$
- ▶ Gaussian mixture (mean (C) and $\Sigma \rightarrow 0$)
- ▶ Parameters $\mathcal{P} = \{\mathcal{P}^z \mid z \in \mathcal{Z}\}$, with $\mathcal{P}^z = (\tilde{P}^z, \tilde{s}^z, \pi^z)$.
- ▶ Observations $o \in \mathcal{O} = \{1 : O\}$ of (θ_i, λ_i)

Algorithm 1: Expectation Maximization

Initialize parameters \mathcal{P}_{new}

repeat

$\mathcal{P}_{\text{cur}} \leftarrow \mathcal{P}_{\text{new}}$

E step:

Evaluate $\zeta_{zo}(\mathcal{P}) = \mathbb{P}(z_o = z \mid \underline{\lambda}_o, \underline{\theta}_o; \mathcal{P})$

M step:

Reestimate parameters using:

$$\mathcal{P}_{\text{new}} = \arg \max_{\mathcal{P}} \mathbb{E}_{\zeta_{zo}(\mathcal{P}_{\text{cur}})} [\ln \mathbb{P}(\underline{\theta}, \underline{\lambda}, \underline{Z}; \mathcal{P})]$$

until \mathcal{P}_{cur} converges to a local maximum

5. Secure dMPC

Modified negotiation (some additional steps):

1. Detection Phase

1.1 Estimate sensibility $\hat{P}_i^1[k]$

- ▶ Artificial Scarcity Sampling + EM

1.2 Detect attack if $\|\hat{P}_i^1[k] - \bar{P}_i^1\|_F \geq \epsilon_P$

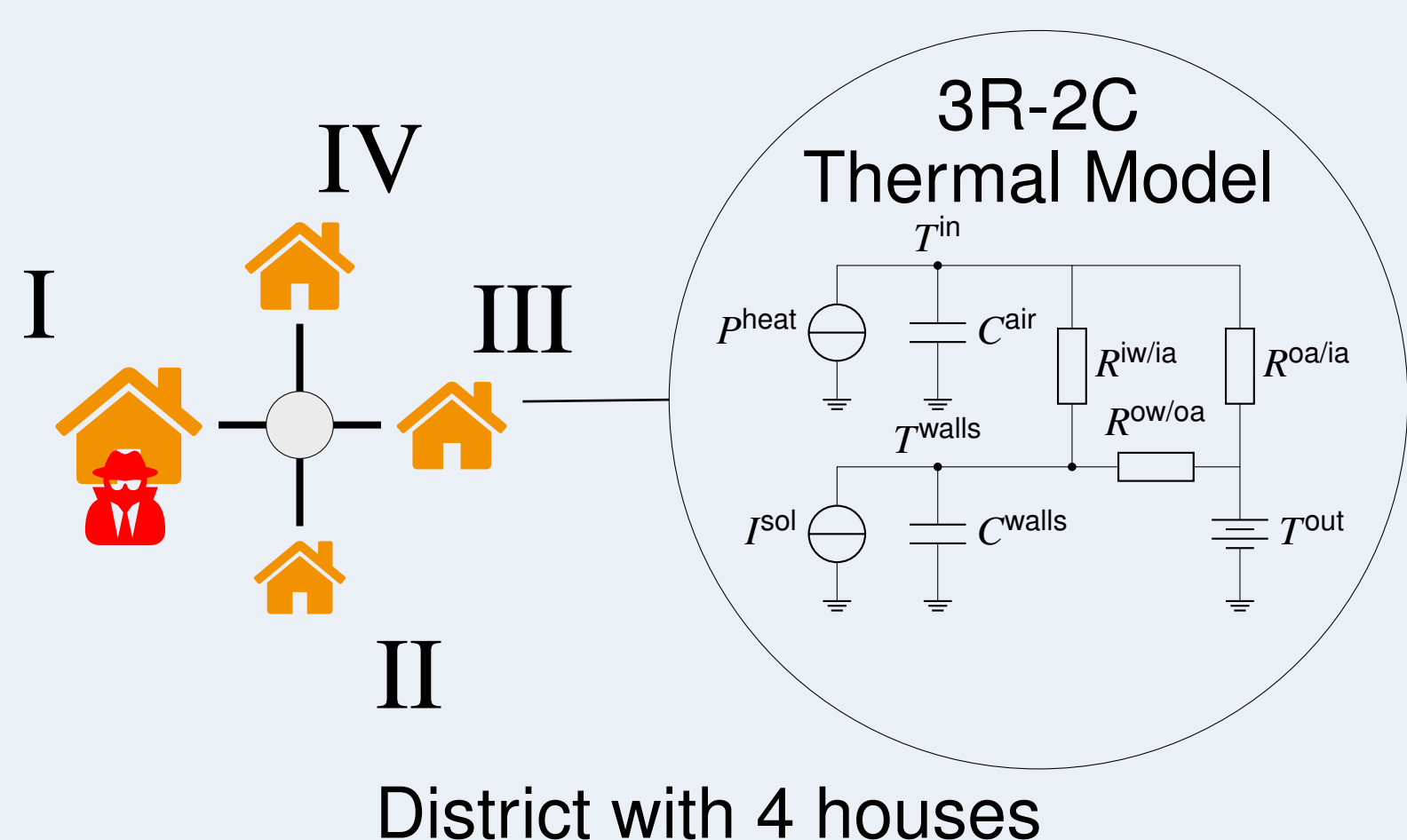
2. Negotiation Phase

2.1 If detected reconstruct λ_i

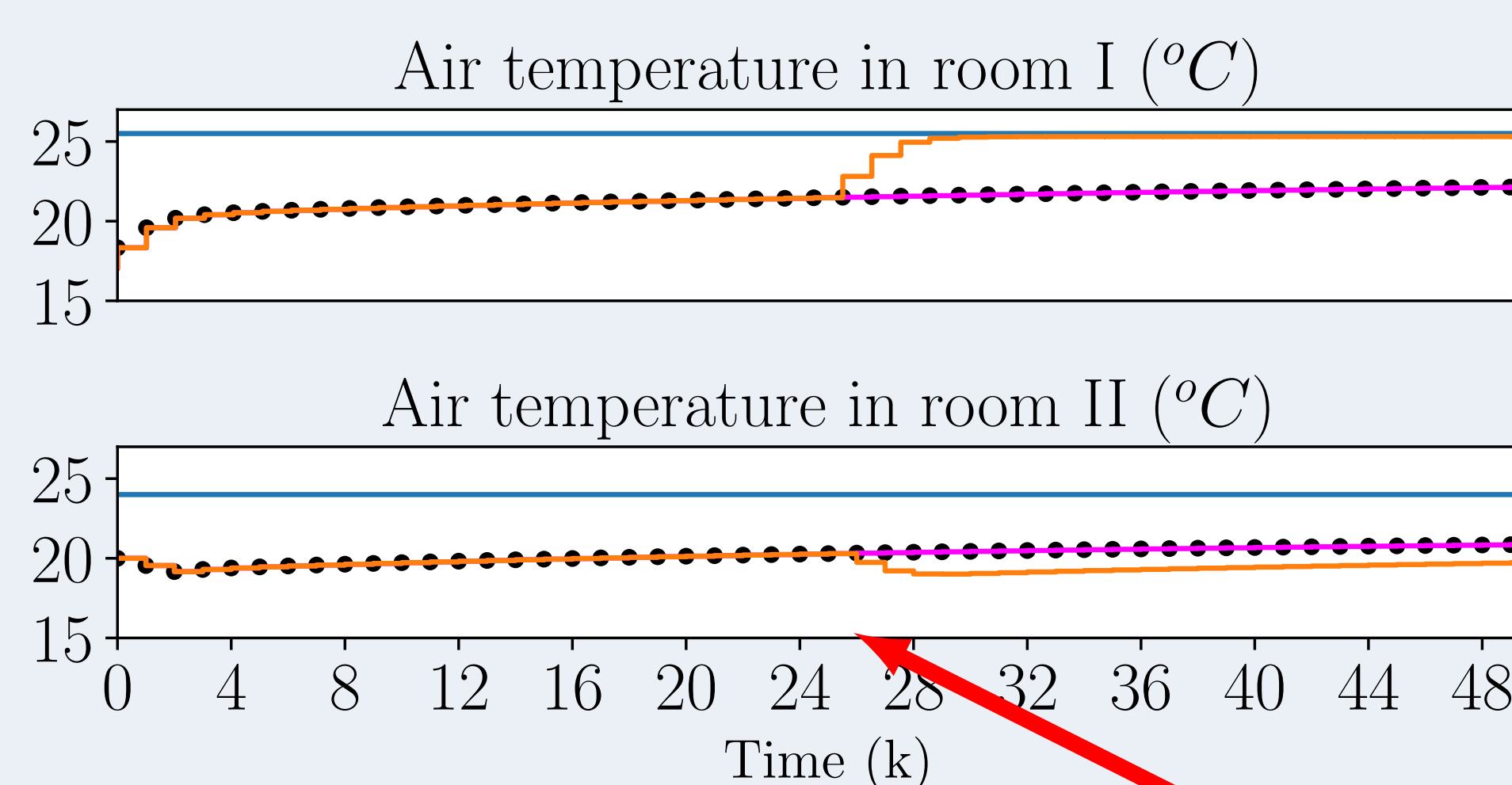
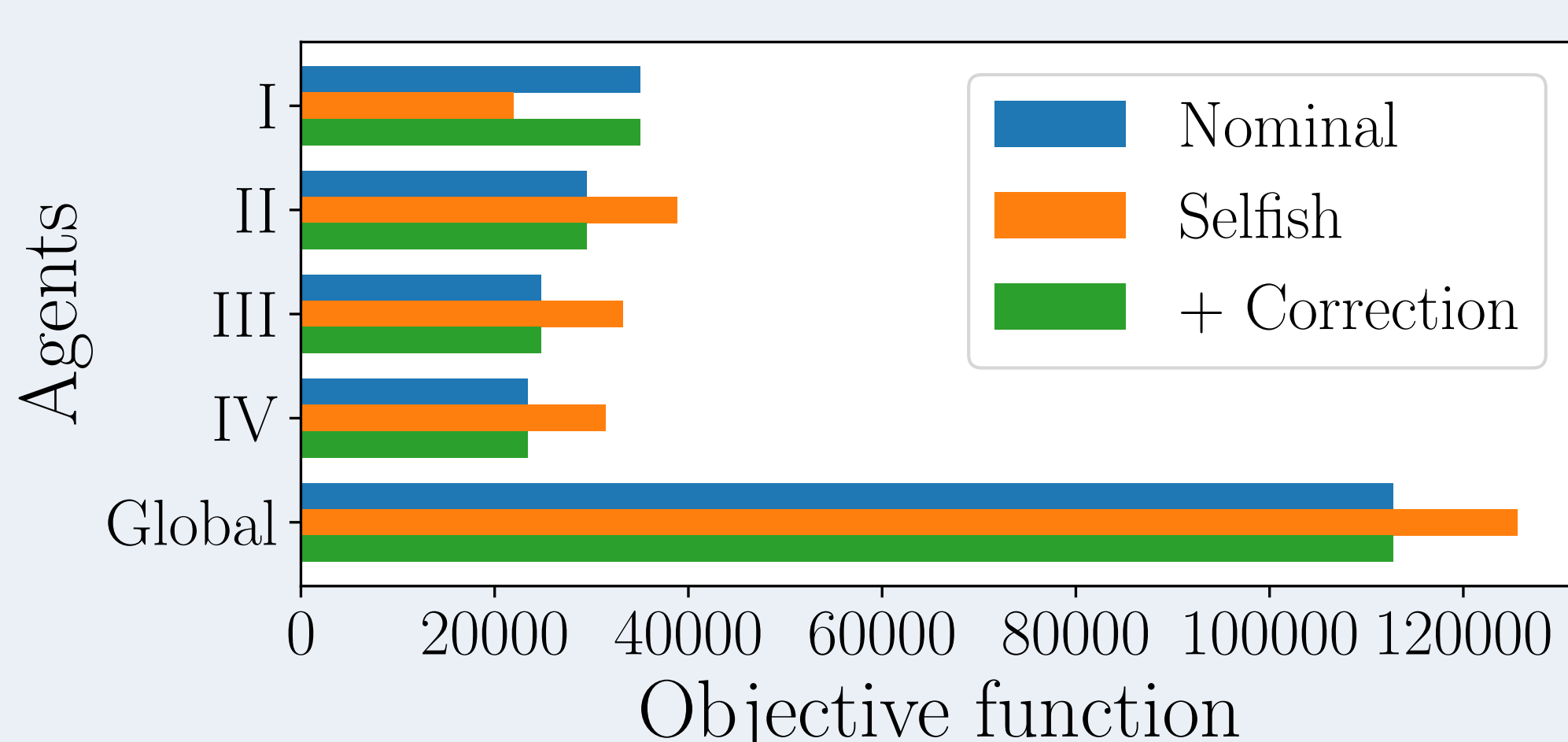
$$\lambda_{i\text{rec}} = \widehat{T_i[k]^{-1}} \tilde{\lambda}_i \quad (F)$$

2.2 Use adequate λ_i to update θ_i (B)

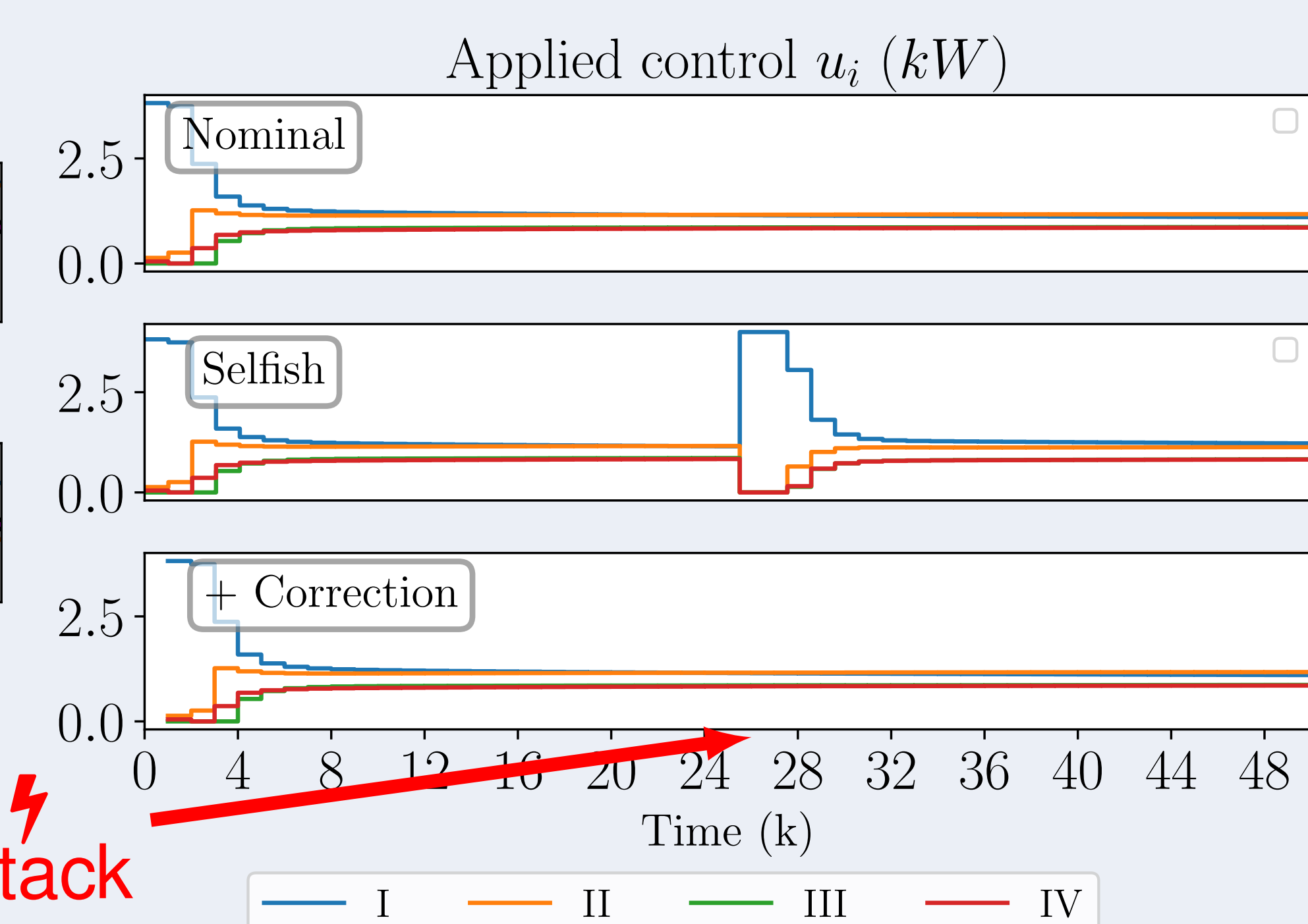
6. Example: distributed control for a heating network under power scarcity



District with 4 houses



Air temperature in houses I and II.



Control applied in all houses for the 3 scenarios.