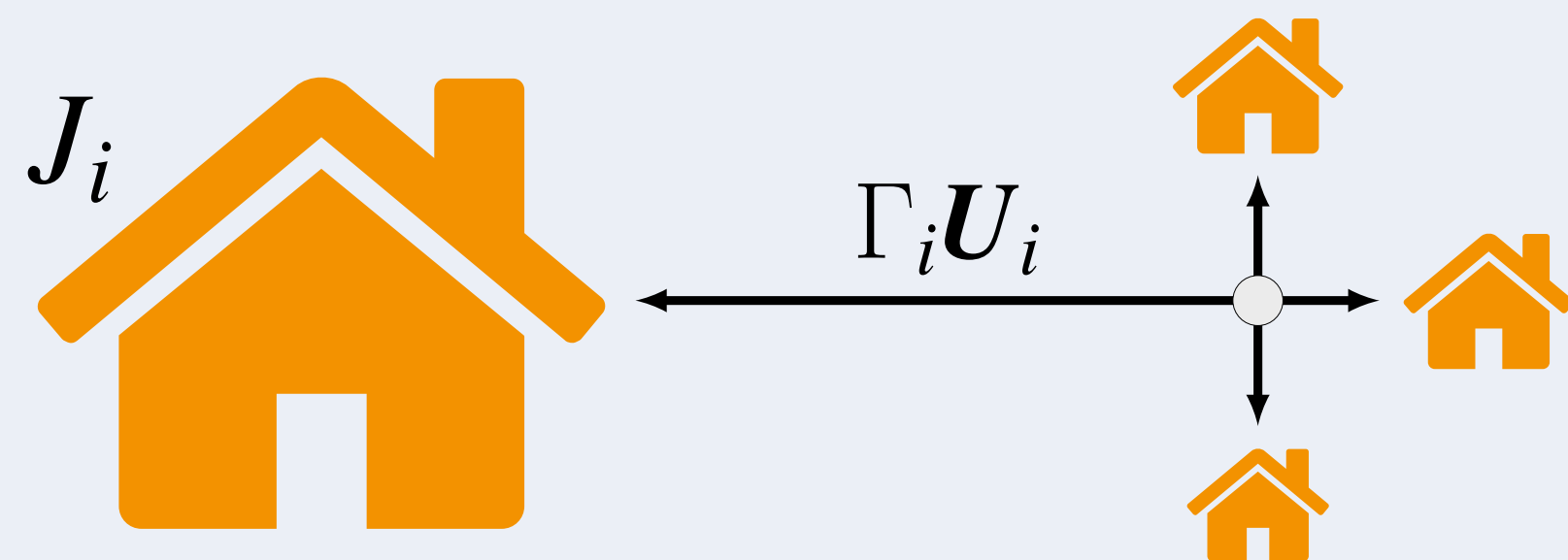




1. Challenge - False Data injection in dMPC exchange

- Global decomposable quadratic objective $\sum_{i=1}^M J_i$
- Global coupling constraint $\sum_{i=1}^M \Gamma_i U_i \leq U_{\max}$



$$\begin{aligned} \min_{U_1[k]} \quad & \frac{1}{2} \|U_1[k]\|_{H_1} + f_1[k]^T U_1[k] \\ \text{s.t.} \quad & \bar{\Gamma}_1 U_1[k] \preceq \theta_1[k] : \lambda_1 \\ & U_1[k] \succeq 0 \end{aligned} \quad \text{Agent 1} \quad (A)$$

...

$$\begin{aligned} \min_{U_M[k]} \quad & \frac{1}{2} \|U_M[k]\|_{H_M} + f_M[k]^T U_M[k] \\ \text{s.t.} \quad & \bar{\Gamma}_M U_M[k] \preceq \theta_M[k] : \lambda_M \\ & U_M[k] \succeq 0 \end{aligned} \quad \text{Agent M} \quad (A)$$

What happens if an agent lies?



$$\theta[k]^{(p+1)} = \text{Proj}^S(\theta[k]^{(p)} + \rho^{(p)} \lambda[k]^{(p)}) \quad (B)$$

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 1

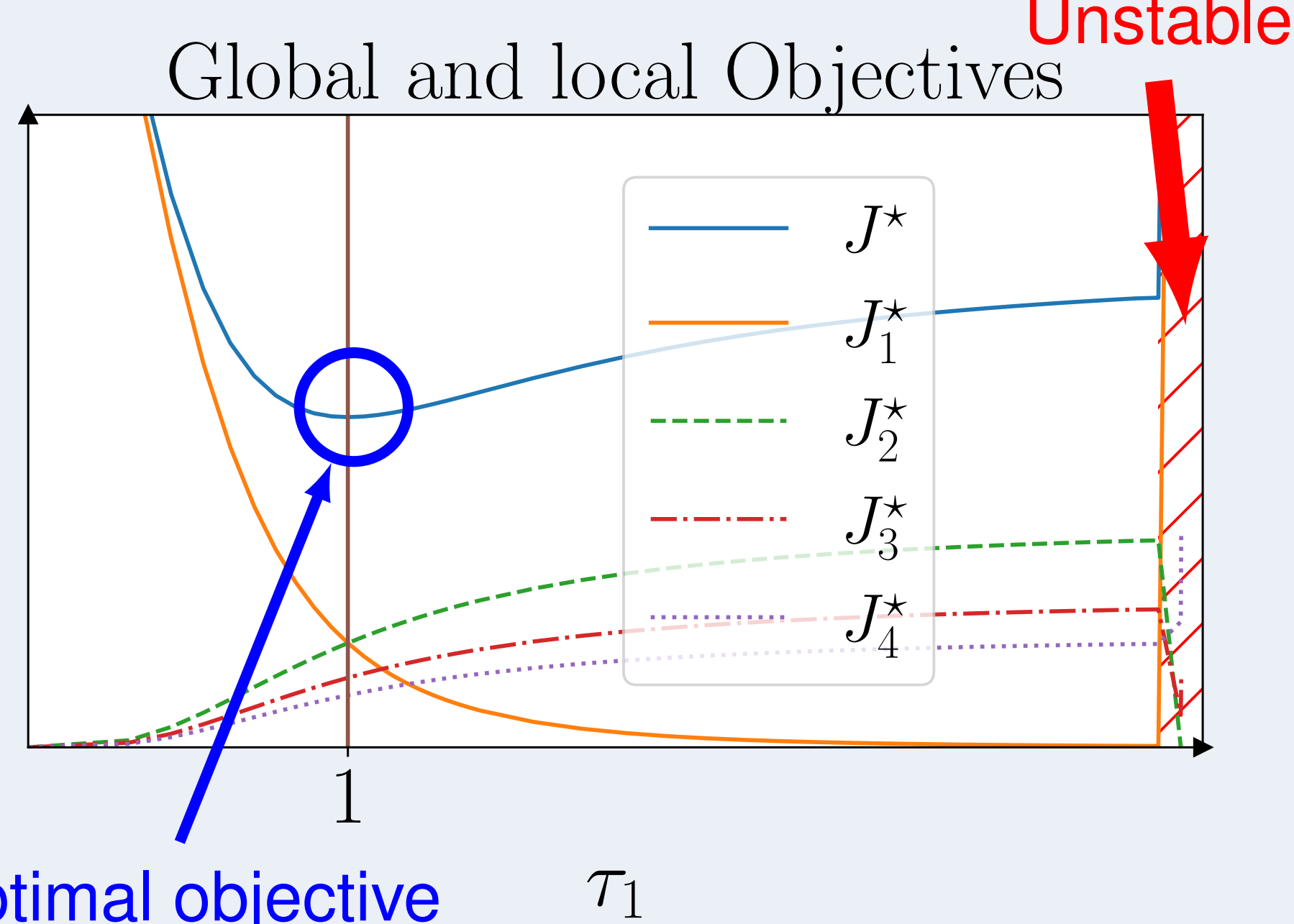
The attacker chooses a linear function

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

$\tilde{\lambda}_i = 0$ only if $\lambda_i = 0 \rightarrow T_i[k]$ is invertible.

- Effects
 - 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 1

Sensibilities P_i^n are time invariant.

Assumption 2

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

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

Assumption 3

$\theta_i = 0$ belongs to Region 1

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

If we can know **nominal** \bar{P}_i^1 , 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 $\tilde{P}_i[k]$?

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 $\theta_i = 0$
 - 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 $\zeta_{zo}(\mathcal{P}) = \mathbb{P}(z_o = z \mid \lambda_o, \theta_o; \mathcal{P})$

M step:

Reestimate parameters using:

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

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

5. Secure dMPC

Modified negotiation (some additional steps):

1. Detection Phase

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

- Artificial Scarcity Sampling + EM

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

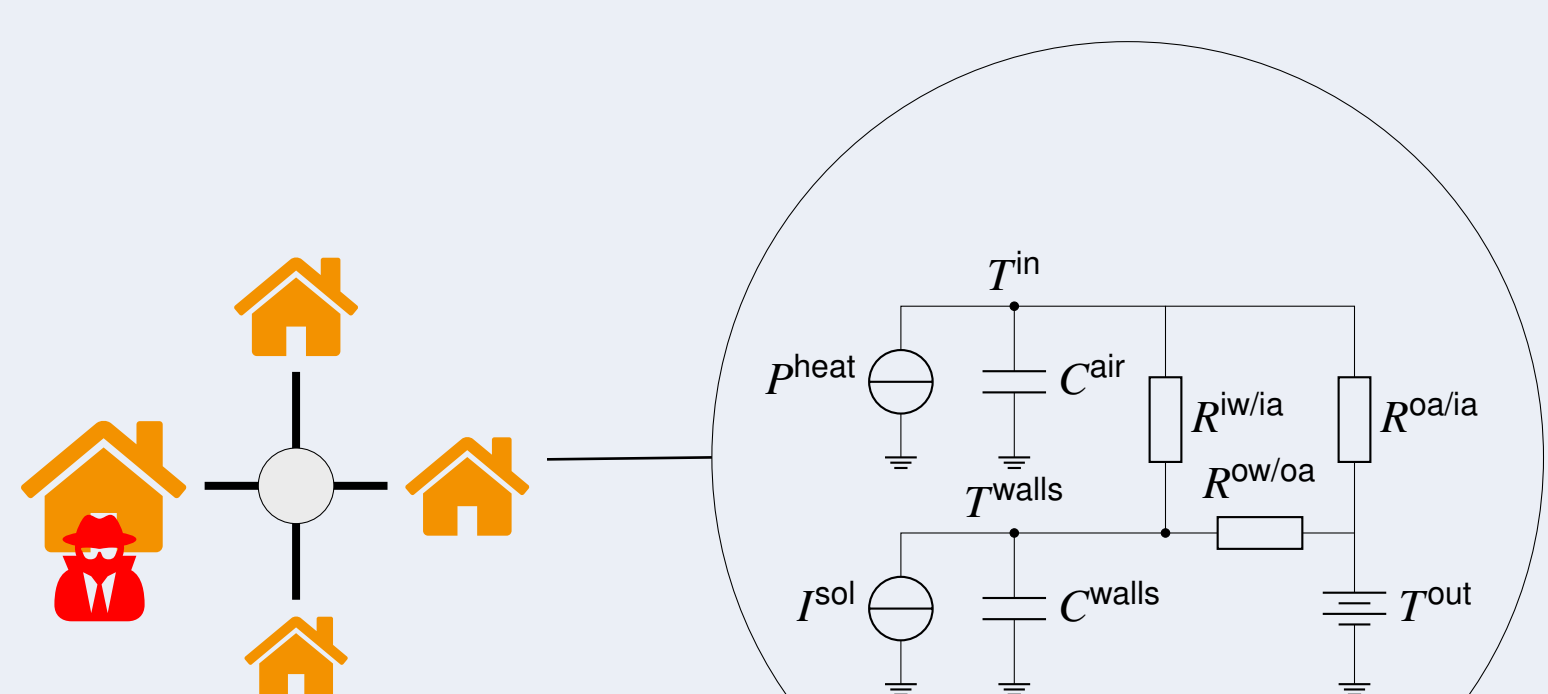
2. Negotiation Phase

2.1 If detected reconstruct λ_i

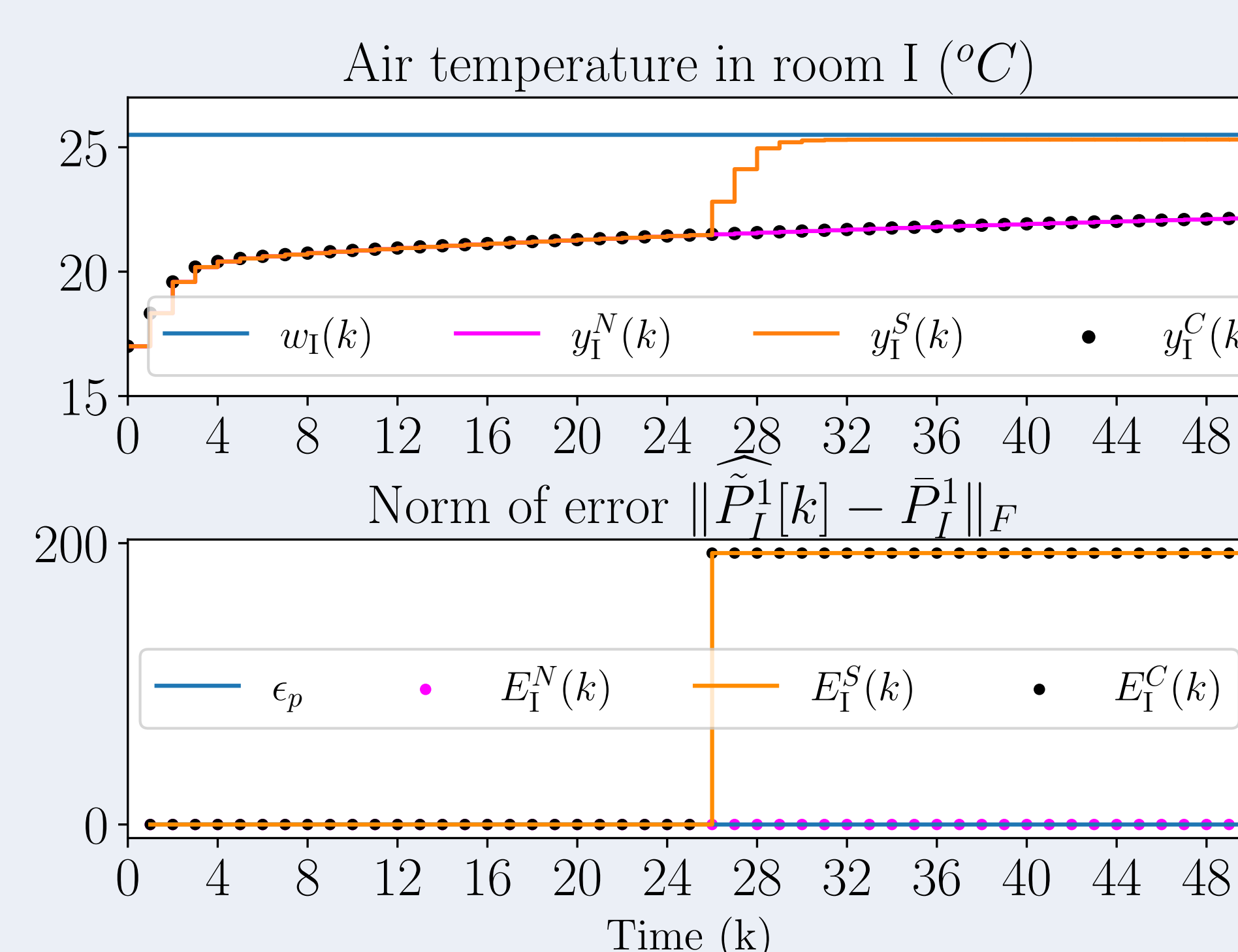
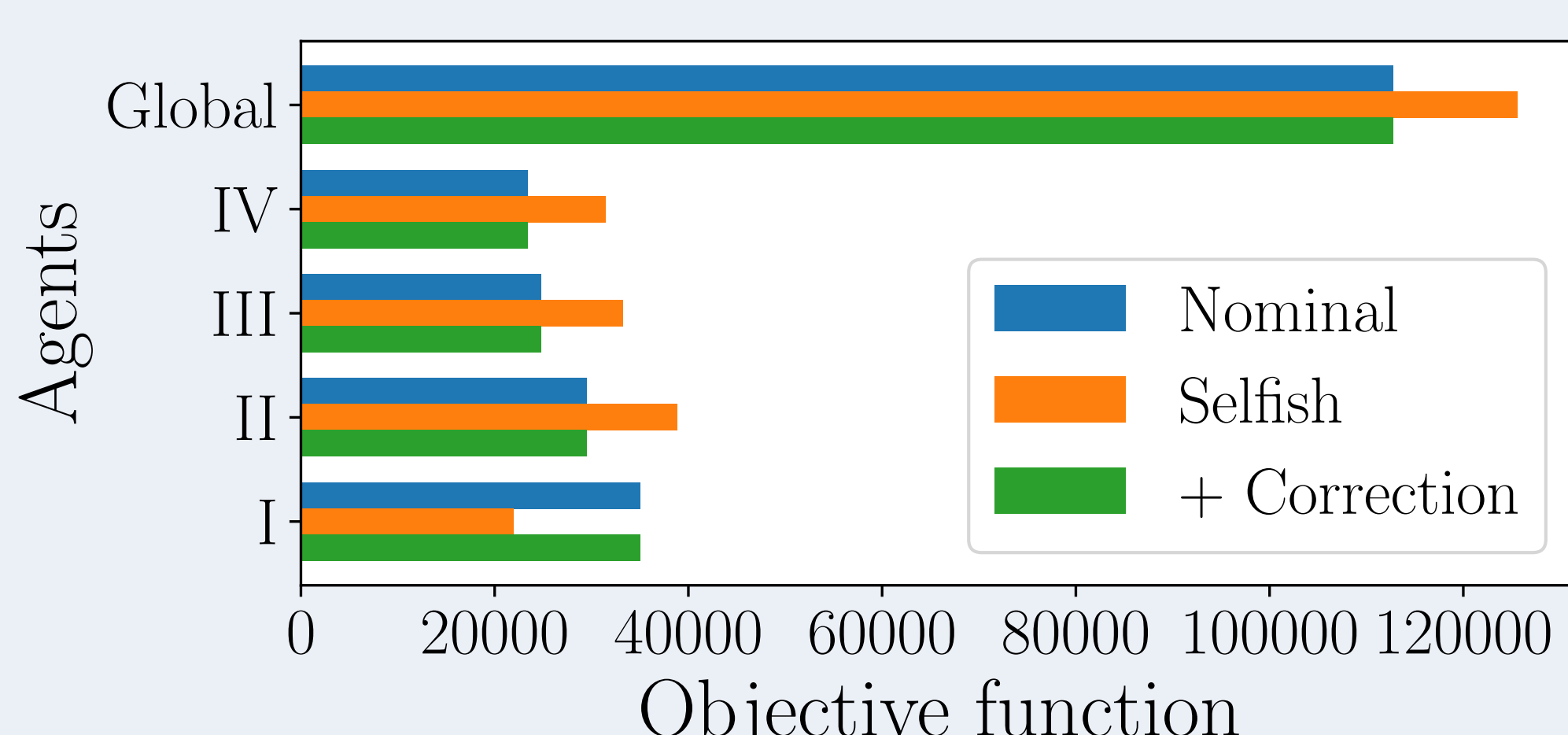
$$\lambda_{i\text{rec}} = \widehat{\tilde{P}_i[k]}^{-1} \tilde{\lambda}_i \quad (F)$$

2.2 Use adequate λ_i to update θ_i (B)

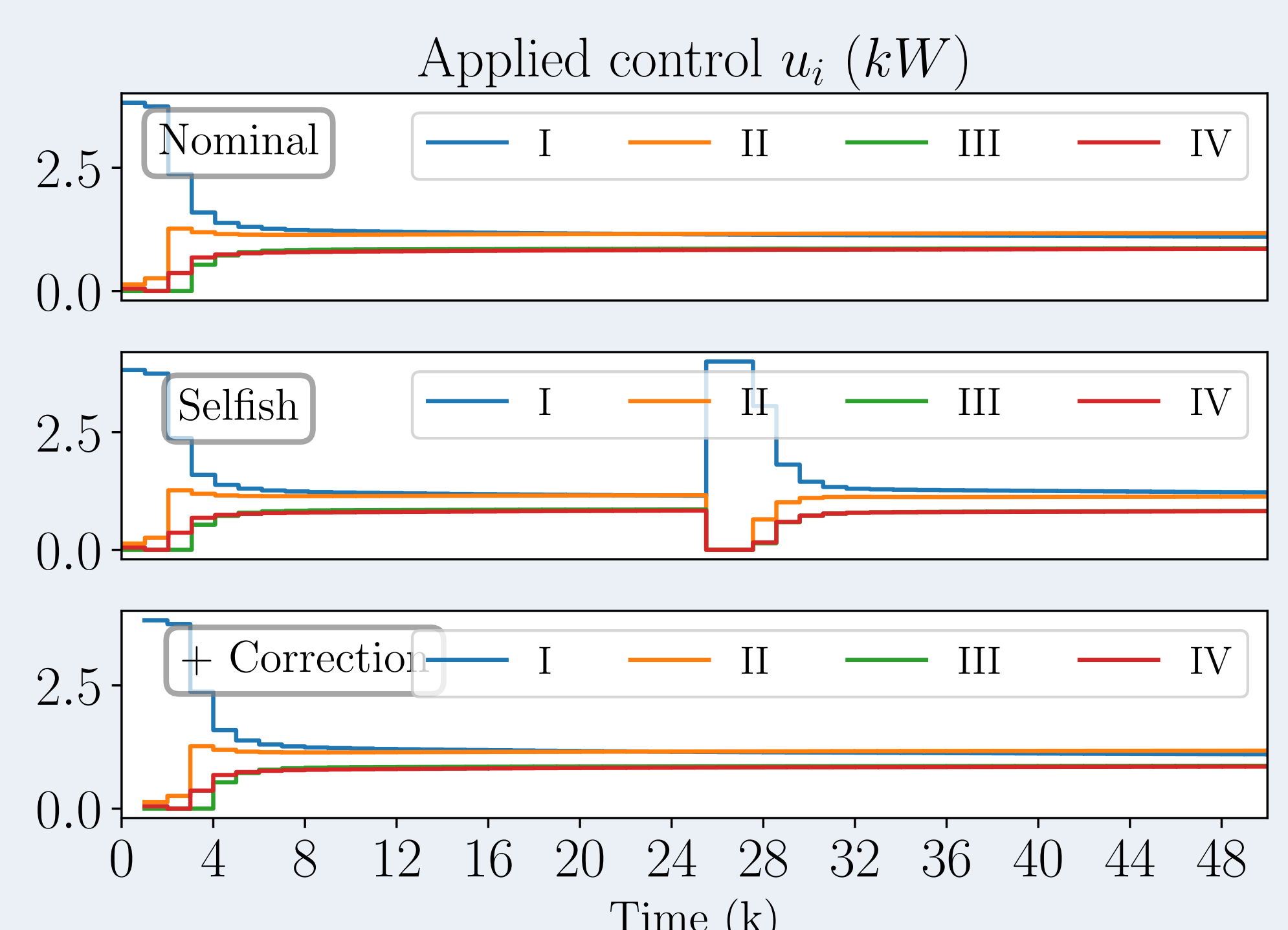
6. Example | 4 distinct rooms | 3 scenarios (Nominal, Selfish, Selfish + Correction)



3R-2C Thermic Model.



Air temperature in room I and the decision variable $E_I[k]$ for three scenarios: nominal (N), selfish behavior (S), and selfish behavior with correction (C).



Control applied in all rooms for the 3 scenarios.