Synthesizing Grid Data with Cyber Resilience and Privacy Guarantees

Online Appendix

Shengyang Wu, Vladimir Dvorkin

1 Reformulation of (7)

The original formulation of (7) in the manuscript are as follows

$$C_{\text{att}}^{\text{RO}}(\mathbf{d}) = \underset{\mathbf{x}}{\text{minimize}} \;\; \mathbf{c}^\top \mathbf{x} \tag{1a}$$

$$\text{subject to} \quad \max_{\boldsymbol{\delta}_k \in \boldsymbol{\Delta}} \left[\mathbf{a}_k^\top \mathbf{x} + \mathbf{b}_k^\top (\mathbf{d} + \boldsymbol{\delta}_k) + e_k\right] \leqslant \mathbf{0}, \forall k, \tag{1b}$$

Constraint (1b) can be rewritten as:

$$\left[\begin{array}{lll} \max\limits_{\delta} & \mathbf{b}_k^\top \boldsymbol{\delta}_k & \\ \text{s.t.} & \underline{\boldsymbol{\delta}} \leqslant \boldsymbol{\delta}_k \leqslant \overline{\boldsymbol{\delta}} & : \overline{\boldsymbol{\mu}}_k, \underline{\boldsymbol{\mu}}_k \\ & \mathbf{1}^\top \boldsymbol{\delta}_k = 0 & : \lambda_k \end{array}\right] \leqslant -\mathbf{a}_k^\top \mathbf{x} - \mathbf{b}_k^\top \mathbf{d} - e_k \quad \forall k = 1, \ldots, K \tag{2}$$

We can get the Lagrangian function of the left-hand side problem as

$$\begin{aligned} \mathcal{L}(\overline{\boldsymbol{\mu}}_k, \underline{\boldsymbol{\mu}}_k, \lambda_k) &= -\mathbf{b}_k^\top \boldsymbol{\delta}_k + \underline{\boldsymbol{\mu}}_k^\top (-\boldsymbol{\delta}_k + \underline{\boldsymbol{\delta}}) + \overline{\boldsymbol{\mu}}_k^\top (\boldsymbol{\delta}_k - \overline{\boldsymbol{\delta}}) + \lambda_k^\top \mathbf{1}^\top \boldsymbol{\delta}_k \\ &= (-\mathbf{b}_k^\top - \underline{\boldsymbol{\mu}}_k^\top + \overline{\boldsymbol{\mu}}_k^\top + \lambda_k^\top \mathbf{1}^\top)\boldsymbol{\delta}_k + \underline{\boldsymbol{\mu}}_k^\top \underline{\boldsymbol{\delta}} - \overline{\boldsymbol{\mu}}_k^\top \overline{\boldsymbol{\delta}} \end{aligned} \tag{3}$$

The dual of problem for the left-hand side maximization problem (2) can be expressed as:

$$\begin{aligned} \underset{\overline{\boldsymbol{\mu}}_k, \underline{\boldsymbol{\mu}}_k, \lambda_k}{\text{maximize}} \quad & \underline{\boldsymbol{\mu}}_k^\top \underline{\boldsymbol{\delta}} - \overline{\boldsymbol{\mu}}_k^\top \overline{\boldsymbol{\delta}} \\ \text{subject to} \quad & -\mathbf{b}_k - \underline{\boldsymbol{\mu}}_k + \overline{\boldsymbol{\mu}}_k + \mathbf{1} \cdot \lambda_k = 0 \\ & \underline{\boldsymbol{\mu}}_k, \overline{\boldsymbol{\mu}}_k \geqslant 0, \; \lambda_k \in \text{FREE} \end{aligned} \tag{4}$$

Take (4) into (2), the whole formulation can be written as:

$$\underset{\mathbf{x}, \overline{\boldsymbol{\mu}}, \underline{\boldsymbol{\mu}}, \lambda}{\text{minimize}} \quad \mathbf{c}^\top \mathbf{x} \tag{5a}$$

$$\text{subject to} \quad \overline{\boldsymbol{\mu}}_k^\top \overline{\boldsymbol{\delta}} - \underline{\boldsymbol{\mu}}_k^\top \underline{\boldsymbol{\delta}} \leqslant -\mathbf{a}_k^\top \mathbf{x} - \mathbf{b}_k^\top \mathbf{d} - e_k \quad \forall k = 1, \ldots, K \tag{5b}$$

$$\mathbf{b}_k - \overline{\boldsymbol{\mu}}_k + \underline{\boldsymbol{\mu}}_k - \mathbf{1} \cdot \lambda_k = \mathbf{0} \quad \forall k = 1, \ldots, K \tag{5c}$$

$$\underline{\boldsymbol{\mu}}_k, \overline{\boldsymbol{\mu}}_k \geqslant 0, \; \lambda_k \in \text{FREE} \tag{5d}$$

$$\tag{5e}$$

which is the formulation (8) in the manuscript.