Expectation-Maximization Based Defense Mechanism for Distributed Model Predictive Control
Rafael Accacio Nogueira, Romain Bourdais, Simon Leglaive, Hervé Guéguen

To cite this version:
Rafael Accacio Nogueira, Romain Bourdais, Simon Leglaive, Hervé Guéguen. Expectation-Maximization Based Defense Mechanism for Distributed Model Predictive Control. 9th IFAC Conference on Networked Systems (NecSys22), Jul 2022, Zürich, Switzerland. hal-04628841

HAL Id: hal-04628841
https://hal.science/hal-04628841
Submitted on 28 Jun 2024
1. Challenge - False Data injection in dMPC exchange

- Decomposable quadratic objective: $\sum_{i=1}^{M} J_i$
- Coupling constraint: $\sum_{i=1}^{M} \Gamma_i U_i[k] \leq U_{\text{max}}$

Primal Decomposition based distributed MPC

Solution

Agent 1

$\min_{u_i[k]} \frac{1}{2} \|U_i[k]\|_{\Gamma_i}^2 + J_i[A_i] U_i[k]$

Agent M

$\min_{\theta_i} \frac{1}{2} \|U_i[k] - \theta_i\|_{\lambda_i}^2$

Update $\theta_i$, using past $\theta_i$ and all $\lambda_i$

Coordinator allocates $\theta_i$, Agent has dissatisfaction $\lambda_i$

What happens if an agent lies about $\lambda_i$?

2. Attack and consequences

- $\lambda_i$ is the dissatisfaction of $i$ to allocation $\theta_i$
- Attacker increases $\lambda_i$ using function $\gamma(\cdot)$
- $\uparrow$ dissatisfaction $\implies$ $\uparrow$ allocation

Remark
Attacker says it is satisfied only when it is Assumption
Attacker chooses an invertible linear function

$\lambda_i = \gamma(\lambda_i) = T_i[k] \lambda_i$

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

Example $T_i[k] = \tau_i I$

Global and local Objectives

Unstable

Optimal objective $\tau_i$

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 are QP

Explicit Solution with PWA form w.r.t $\theta_i$:

$\lambda_i[k] = -P_i^T[k] \theta_i[k] - s_i[k], \text{if } G_i^T[k] \theta_i[k] \leq b_i[k]$ (B)

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

Remark
Sensibilities $P_i^T$ are time invariant.

Another assumption
In Region 1 local constraints are active:

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

and $\theta_i = 0$ belongs to it

Attacker modifies sensibility $P_i[k] = T_i[k] P_i$

If we can know nominal $P_i$,

by estimating $P_i[k]$, we can find $T_i[k]^{-1}$:

$T_i[k]^{-1} = P_i^{-1} P_i^T[k]^{-1}$ (D)

But how can we estimate the $P_i^T[k]$?

Enter Expectation Maximization

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

EM needs minimally excited inputs $\theta_i$ and $\hat{\lambda}_i$.

- 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 $z \in Z = \{1, Z\}$
- Gaussian mixture (mean $B$ and $\Sigma \rightarrow 0$)
- Parameters $P = \{P_z | z \in Z\}$, with $P_z = (P_z^T, \Sigma_z, \pi_z)$.
- Observations $o \in \Omega = \{1, O\}$ of $(\theta_i, \lambda_i)$ stacked as $(\Omega, \Delta)$ with corresponding $Z$

Algorithm 1: Expectation Maximization

Initialize parameters $P_{\text{new}}$

repeat

$P_{\text{cur}} \leftarrow P_{\text{new}}$

E step:

Evaluate $\zeta_{\text{EM}}(P_{\text{cur}}) = P(\zeta, \theta_i, \lambda_i, P_{\text{cur}})$

M step:

Reestimate parameters using:

$P_{\text{new}} = \arg \max_P \zeta_{\text{EM}}(P_{\text{cur}})\log P(\Omega, \Delta, Z, P)$

until $P_{\text{cur}}$ converges

5. Secure dMPC

Modified negotiation (some additional steps):

1. Detection Phase
   - 1.1 Estimate sensibility $P_i[k]$
   - 1.2 Detect attack if $|P_i[k] - P_i[k]| \geq \epsilon_P$

2. Negotiation Phase
   - 2.1 If detected reconstruct $\lambda_i$
     - $\lambda_{\text{rec}} = T_i[k]^{-1} \hat{\lambda}_i$
     - (E)
   - 2.2 Use adequate $\lambda_i$ to update $\theta_i$

6. Example: Control of a heating network under power scarcity - 3 Scenarios (Nominal, Selfish, + Correction)

- Control applied in all houses for the 3 scenarios.
- $I$ to $IV$: scenarios
- District with 4 houses

Agents

- Nominal
- Selfish
- + Correction

Objective function

Global

Air temperature in house I ($^\circ C$)

Air temperature in house II ($^\circ C$)

Air temperature in houses I and II.

Control applied in all houses for the 3 scenarios.