Hyergames for Control System Security

Arnab Bhattacharya
Research Scientist
Optimization and Control Group
Cyber Attacks on Feedback Control Systems

- Optimal control in closed-loop dynamical systems: Buildings
- Perturbations of system parameters via stealthy attacks
- Effect on efficiency: cost, operating constraint violation

**Objective:** Robust strategies against stealthy attacks for control systems
Game Theory

- Studies strategic interactions between rational agents
- Considers players, goals, moves, and observations
- Assumes **common perception** amongst agents
- Solves for equilibrium solution (collection of players’ best responses)

- Extensions required when there is
  - Information asymmetry
  - Partial observability (Perceptions/Beliefs)
Hypergames

- **(Mis) perceptions** about opponent strategies: Rationality + Information Asymmetry
- Perceptions of Perceptions (Nested optimization)
- Equilibrium Stability (Optimality conditions)

Two player game

$$G_{A,B} = (\{A, B\}, \{S_A, S_B\}, \{u_A, u_B\})$$

One-level Hypergame

$$H_{A,B} (A, B, G_{A,B}) = \{p(A, G_{A,B}), p(B, G_{A,B})\}$$

$$p(A, G_{A,B}) \neq p(B, G_{A,B})$$ (Both are unaware of the other's perceptions)

Two-level Hypergame

$$H_{A,AB} (A, AB, G_{A,B}) = \{p(A, G_{A,B}), p(AB, G_{A,B})\}$$

$$p(AB, G_{A,B}) \neq p(A, G_{A,B})$$ (A is aware that B has perceptions for A)

$$p(BA, G_{A,B}) = p(B, G_{A,B})$$ (B is unaware that A knows)
Static and Dynamic Optimization

Question: Can misperceptions in system parameters be an attack strategy?

- **Objective Function Manipulation**
  - Cost maximization by attacker

- **Constraint Manipulation**
  - System failure

- **Defender Anticipation of Attacker Strategies**
  - **Variant 1**: Attacker perturbs, defender unaware
  - **Variant 2**: Attacker perturbs, defender aware
  - **Variant 3**: Attacker knows defender knows about attacker perturbations (double bluff)

Defender Baseline Control Models

**Static**

\[
\min_{\mathbf{u}} \ J(\mathbf{u}, \theta) \\
g(\mathbf{u}, c) \leq 0
\]

**Dynamic**

\[
\min_{\mathbf{u}_t} \sum_{t=1}^{\tau} J(\mathbf{u}_t, \mathbf{x}_t, \theta) \\
x^t = f(x^{t-1}, \mathbf{u}_t, \alpha^t, \beta) \\
x^\tau - x^0 = 0 \\
g(x^t, \mathbf{u}_t, \alpha^t, \beta) \geq 0
\]
Objective Function Manipulation

- **Attacker’s model**
  - Attacker perturbs defender’s observation of the parameters $\hat{\theta} = \theta + \Delta \theta$.

  \[
  \max_{\Delta \theta} J(u^*, \theta) \quad \text{Attacker objective}
  \]

  \[
  \frac{1}{2} ||\Delta \theta||^2 \leq \delta_{\theta, \text{max}} \quad \text{Attack budget}
  \]

  \[
  \hat{u}^* = \arg \min_{\hat{u}} \left( J \left( \hat{u}, \hat{\theta} \right) : g(\hat{u}, c) \leq 0 \right) \quad \text{Attacker’s perception of defender problem}
  \]

- **Defender’s model**

  \[
  \min_u J(u, \hat{\theta}) \quad \text{Defender unaware of attacker manipulation}
  \]

  \[
  g(u, c) \leq 0
  \]
Constraint Manipulation

- Attacker perturbs constraint parameters

**Defender unaware, Attacker maximizes power (Power Max)**

\[
\max_{\Delta c} J(u^*, \theta) \\
\frac{1}{2} \|\Delta c\|^2 \leq \delta_{c,\text{max}} \\
\hat{c} = c + \Delta c \\
u^* = \arg\min_u (J(u, \theta) : g(u, \hat{c}) \leq 0)
\]

**Defender unaware, Attacker maximizes constraint violation (System Break)**

\[
\max_{\Delta c} \gamma^T g(u, c) \\
\frac{1}{2} \|\Delta c\|^2 \leq \delta_{c,\text{max}} \\
\hat{c} = c + \Delta c \\
u^* = \arg\min_u (J(u, \theta) : g(u, \hat{c}) \leq 0)
\]

Deviate maximally from operating envelope
## Static Optimization Results

\[
\min_{m, p} \theta_1 m + \theta_2 m^2 + \theta_3 p \\
\frac{1}{2} \left[ (m - c_m)^2 + (p - c_p)^2 - c_r^2 \right] \leq 0
\]

<table>
<thead>
<tr>
<th>Attacker Action</th>
<th>Defender Belief of Attacker Action</th>
<th>Power</th>
<th>Constraint Violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>No attack</td>
<td>Normal</td>
<td>13.97</td>
<td>-</td>
</tr>
<tr>
<td>Power Max</td>
<td>Normal</td>
<td>17.76</td>
<td>-</td>
</tr>
<tr>
<td>No Attack</td>
<td>Power Max</td>
<td>10.79</td>
<td>4.92</td>
</tr>
<tr>
<td>Break System</td>
<td>Normal</td>
<td>10.79</td>
<td>2.20</td>
</tr>
<tr>
<td>No Attack</td>
<td>Break System</td>
<td>17.76</td>
<td>-</td>
</tr>
<tr>
<td>Break System</td>
<td>Power Max</td>
<td>8.11</td>
<td>4.85</td>
</tr>
<tr>
<td>Power Max</td>
<td>Break System</td>
<td>22.21</td>
<td>-</td>
</tr>
</tbody>
</table>
Acknowledgements

Pacific Northwest National Laboratory is operated by Battelle for the U.S. Department of Energy under Contract No. DE-AC05-76RL01830.

Arnab Bhattacharya
Research Scientist
Pacific Northwest National Laboratory
arnab.bhattacharya@pnnl.gov
(509) 375-2441

Reference

Thank you
Repeated Game Extension

- Games of Timing
- Repeated Hypergame
- Learning and Monitoring Schemes

\[
\min_u J \left( u, \hat{\theta}(n) \right) \\
g(u, c) \leq 0
\]