Optimal Scaled Attacks on Consensus-based Formation Control

Sreejeet Maity SR. No: 19973

Under the supervision of

Dr. Vaibhav Katewa

भारतीय विज्ञान संस्थान

Robert Bosch Center for Cyber-Physical Systems
Indian Institute of Science, Bangalore

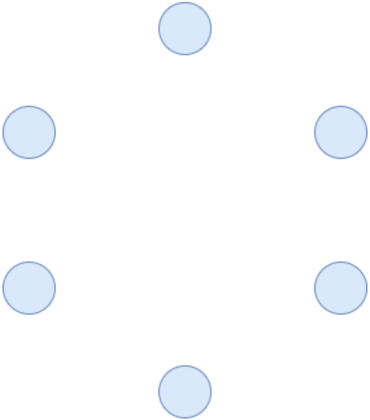
November 30, 2023

Contents

Current Section

Introduction

- What is Consensus ?
- Formation Control in Multi-agent Systems
- Can we club them together ?



Introduction

Figure 1: Consensus : What even are they ?

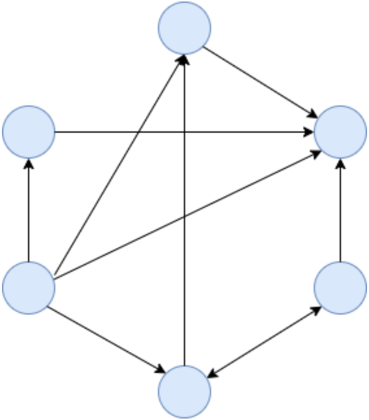


Figure 2: Consensus and the underlying Network Topology

Introduction

General Consensus Based Protocol

$$u_i^{(j)} = \dot{x}_i{}^{(j)} = \sum_{j \in N_i} a_{ij}(x_j^{(j)} - x_i^{(j)})$$

$$\dot{x} = -L \cdot x \tag{1}$$

Taking all the d dimensions,

$$\dot{x} = -L \otimes I_d \cdot x \tag{2}$$

Why are the axis decoupled ?

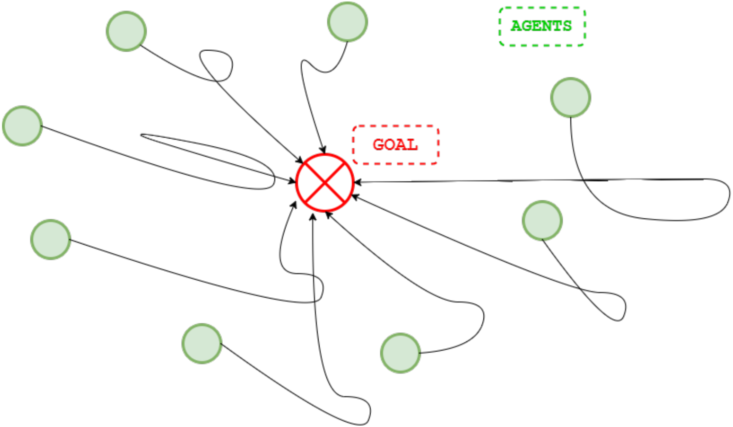


Figure 3: Why are the axis decoupled ?

Consensus Based Protocol for Formation Control

$$u_i^{(j)} = \dot{x}_i^{(j)} = \sum_{j \in N_i} a_{ij}(x_j^{(j)} - x_i^{(j)} - \delta_{ji}^{(j)}))$$

$$\dot{x} = -L \cdot x + \bar{\delta} \tag{3}$$

Taking all the d dimensions,

$$\dot{x} = -L \otimes I_d \cdot x + \bar{\delta} \tag{4}$$

Consensus Based Formation Protocol

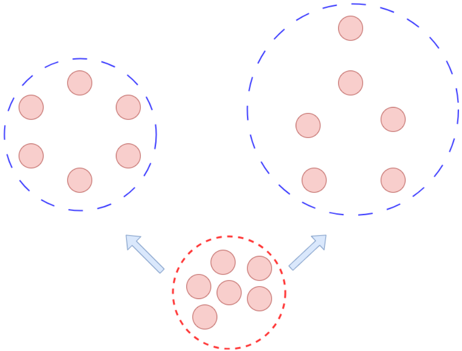


Figure 4: Formation Control in Multi-Agent Systems with 6 agents

Consensus Based Formation Protocol

w : Left-dominant eigenvector corresponding to $L, satisfying 1_n^T w = 1$.

$\delta^{X_i(0)}$ = $\mathbb{1}_n \delta_i^{(j)} - \delta^{(j)}$

The final position of the i^{th} agent (d-dimension) is given as follows :

$$x_i(\infty) = w^T[\bullet](X(0) + \delta^{X_i(0)}) \quad (5)$$

$$x_i(\infty) - x_j(\infty) = \delta_{ij} \quad (6)$$

Motivation

- Can an intruder attack one or more agents in some way ?
- Attack Design.
- Severity of the Attack.
- How much control the attacker should have over the agents ?

Current Section

Scale Attack Design for a M.R.S

- Attacks on agents/nodes.
- Attacked agents share/update itself with the scaled value of its original state.
- x_i shares $\alpha_i \cdot x_i$ with the other agents, and updates itself with that,

Scaled Attack Design for a M.R.S

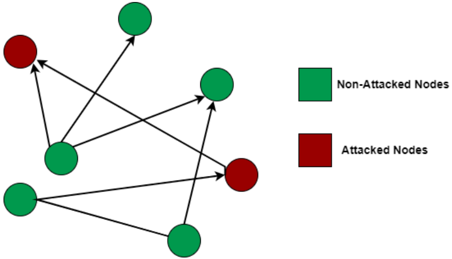


Figure 5: MAS with two attacked agent (coloured red) and 5 non-attacked agent(coloured green) trying to achieve a formation.

Scaled Attack : Changes in the governing Laplacian

- Attacks on agents/nodes

$$\dot{x} = -(LD \otimes I_d)x + \bar{\delta} \tag{7}$$

$$D = \begin{bmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{bmatrix}$$

Theorem 1

Theorem 1

*The attack protocol defined in (5) gives the following two results, namely **R1** and **R2**:*
(R1) *The eigenvalues $\mu_i(LD) \ > 0 \ \forall \ i \in \{2, n\}$ of the compromised system, and $\mu_1(LD)$ = 0.*
(R2) *Alternatively, $\mathbb{1}_{sgn\{[L \otimes I_d]_{ij}\} = sgn\{[LD \otimes I_d]_{ij}\} \geq 0} = 1$, where, $\mathbb{1}$ and sgn denote the standard indicator and sign function respectively.*

Proof.

(R1) By similarity transformation, μ_i (LD) = μ_i (DL) $\geq$ 0.
(R2) The diagonal entries of D $>$ 0. □

Final Position of the agents under the proposed attack

The final position of the i^{th} agent (d-dimension) is computed as follows:

$$\tilde{x}_i = \beta \left[\frac{\tilde{w}^T}{\alpha_i} [\bullet] \{ (\alpha \otimes \mathbb{1}_d) \odot X(0) + \delta^{X_i(0)} \} \right] \tag{8}$$

$$(\alpha_i \cdot \tilde{x}_i - \alpha_j \cdot \tilde{x}_j) = \beta \tilde{w}^T \mathbb{1}_n \delta_{ij} = \delta_{ij} \tag{9}$$

Final Position of the agents under the proposed attack

The final position of the i^{th} agent (d-dimension) is given as follows :

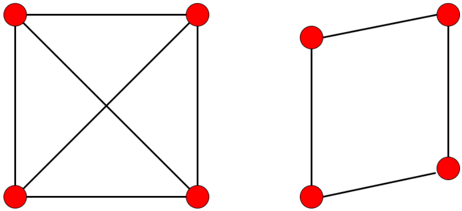


Figure 6: Desired and Final Formation for 4 agents, where 3 of those are attacked as per the protocol described in (5)

Attack Analysis: Spectral Properties

Theorem 2

Considering the attack scales as $\alpha_i \geq 0$, the second smallest eigenvalue (μ_2) of the compromised system (5) is lower bounded [1] and upper bounded as follows:

$$\mu_2 \leq \left(\sum_i \alpha_i \right) \lambda_n$$

Where, α_i are the scales associated with the i^{th} agent, and λ_n is the largest eigenvalue associated with the un-attacked case.

Special cases: Weighted un-directed Graph

Lemma 1

In the scaled attack setup, we can write the following two statements (**S1** and **S2**) :

(S1):As per the attack mechanism on the proposed formation control protocol,$\|x_i^{LD_{i\alpha}}(\tau) - \delta_a^*\|_2^{LD_{i\alpha}} \leq \|x_i^L(\tau) - \delta_b^*\|_2^L \ \forall \quad i \in \{1, n\}$ and $\tau \in [t, \infty)$.
(S2) : The second smallest eigenvalue of the attacked system, $\mu_2 \geq \min(\alpha_i).\lambda_2$. Where, α_i is the scaled attack parameter and λ_2 is the second smallest eigenvalue of the non-attacked system.

Comparing the severity of two attacks using Lemma 3

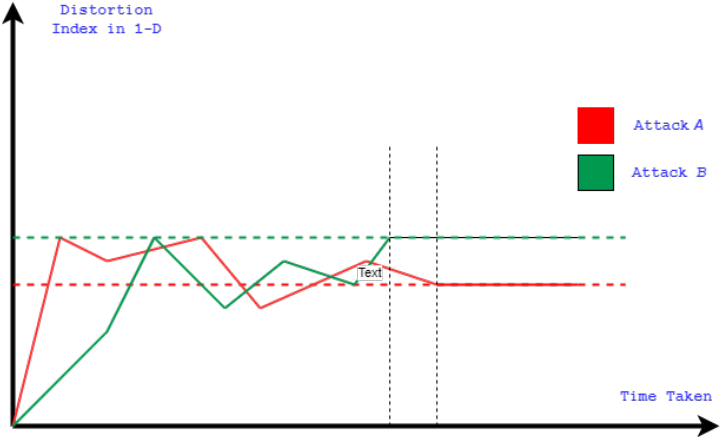


Figure 7: Two Attack $\mathscr{A}$ and $\mathscr{B}$ are compared using the results of Lemma 3

Attack Analysis: Extent of Distortion

The Distortion Metric(ε_{rel}) is defined as follows:

$$\varepsilon_{rel} = \sum_i \sum_j \|\tilde{x}_i - \tilde{x}_j - \delta_{ij}\|_2^2 = \sum_l \sum_i \sum_j (\tilde{x}_i^{(l)} - \tilde{x}_j^{(l)} - \delta_{ij}^{(l)})^2$$

We can also write :

$$\varepsilon_{rel} = {p^{(l)}}^T (\mathbb{I}_d \otimes Q) p^{(l)}$$

Where, $Q \in \mathbb{R}^{n \times n}$ and takes a special form of a fully connected Laplacian, and $p^{(l)} = [\tilde{x}_1^{(l)} - \delta_1^{(l)} \;\; \tilde{x}_2^{(l)} - \delta_2^{(l)} \;\; \dots \;\; \tilde{x}_n^{(l)} - \delta_n^{(l)}]$, and $p^{(l)} = \tilde{x}^{(l)} - \delta^{(l)}$

Choosing Optimal Scales for Maximizing Distortion

- Since, axis are decoupled, we will continue our analysis by taking $d = 1$

The optimization problem can be stated as follows :

$$\begin{aligned} \max_{\alpha} \quad & 2 \cdot {p^{(1)}}^T Q p^{(1)} \\ \text{s.t.} \quad & \alpha \in [\Delta_a, \Delta_b] \odot \mathbb{1}_n \end{aligned}$$

Choosing Optimal Scales for Maximizing Distortion

Note : $\delta_i^{(j)}$'s are not unique but δ_{ij}'s are uniquely defined. The optimization can be equivalently re-stated as follows :

$$\begin{aligned} \max_{\alpha} \quad & 2 \cdot {x^{(1)}}^T (Qx^{(1)} + \mathscr{B}_1(\delta_{ij})) + \mathscr{B}_2(\delta_{ij}) \\ \text{s.t.} \quad & \alpha \in [\Delta_a, \Delta_b] \odot \mathbb{1}_n \end{aligned}$$

Where, $\mathscr{B}_1$, $\mathscr{B}_2$ are functions of δ_{ij}.
Where,

$$\tilde{x}_i^{(1)} = \beta \left[\frac{\tilde{w}^T}{\alpha_i} (\alpha \odot x(0)^{(j)}) + \frac{\tilde{w}^T}{\alpha_i} (\mathbb{1}_n \delta_i^{(1)} - \delta^{(1)}) \right] ; \beta = w^T \cdot D^{-1} \cdot \mathbb{1}_n$$

Special $Case_1$: M- Twin attacks

- Attacking m ($\leq N$) agents with only one scale $alp\bar{h}a$

The optimization can be equivalently re-stated as follows :

$$\begin{aligned} \max_{\bar{\alpha}} \quad & \mathscr{F}\left(\frac{1}{\bar{\alpha}}\right) \\ \text{s.t.} \quad & \bar{\alpha} \in [\Delta_a, \Delta_b] \end{aligned}$$

Where, $\mathscr{F}$ is a fractional Polynomial.

Solution of Special $Case_1$: M- Twin attacks

$$\mathscr{L} = \mathscr{F}\left(\frac{1}{\bar{\alpha}}\right) + \lambda_1 \left(\bar{\alpha} - \Delta_a\right) + \mu_1 \left(\bar{\alpha} - \Delta_b\right)$$

Case 1: When λ_1 or $\mu_1 \neq 0$, from the K.K.T conditions, the extreme points are Δ_a or Δ_b.
Case 2: When both λ_1 and μ_1 0, the constrained problem turns into an un-constrained problem.
In that case we need to find the roots of $\dot{\mathscr{F}}$ = 0 and check the sign of $\ddot{\mathscr{F}}$ to figure out the maxima scale value($\bar{\alpha}^*$).

Special $Case_2$: General Agreement Case

In general agreement, we put $\delta_{ij} = 0$

$$x^{(1)} = \beta D^{-1} \left[w^T x(0)^{(1)} \cdot \mathbb{1}_n \right] \tag{10}$$

Since, δ_{ij} is taken as 0, the optimization problem becomes equivalent to

$$\begin{aligned} \max_{\alpha} \quad & 2 \cdot {x^{(1)}}^T Q x^{(1)} \\ \text{s.t.} \quad & \alpha \in [\Delta_a, \Delta_b] \odot \mathbb{1}_n \end{aligned}$$

Solution of the Special $Case_2$: General Agreement

We start with the Lagrangian :

$$\mathscr{L} = 2(w^T x(0)^{(1)})^2 \beta^2 \mathbb{1}_n^T D^{-1} Q D^{-1} \mathbb{1}_n + \sum_i \lambda_i (\alpha_i - \Delta_a) + \sum_i \mu_i (\alpha_i - \Delta_b)$$

The K.K.T conditions give us the following two cases :

Case 1: 2^n possible extreme points given λ_i and μ_i $\forall i, j \in \{1, n\}$ are active.

Solution of the Special $Case_2$: General Agreement

Case 2: When they are not active, the unconstrained version gives us :

$$\frac{\partial \mathcal{L}}{\partial \alpha} = 4\bar{C}^2\beta^2 QD^{-1}\mathbb{1}_n + 2\bar{C}^2\mathbb{1}_n^T D^{-1}QD^{-1}\mathbb{1}_n\beta\dot{\beta} = 0$$

Here, $\bar{C} = w^T x(0)^{(1)}$ Hence, the number of points for which maxima needs to be checked are > 2^n, which makes it hard to solve the problem analytically.

Optimal Resilient Topology Design: Scaled attack

The Optimization Problem takes the following form :

$$\begin{aligned} \min_{W} \quad & 2 \cdot \sum_{l} {p^{(l)}}^{T} Q p^{(l)} \\ \text{s.t.} \quad & 0 \leq w_i \leq 1 \;\; \forall i \in \{1, n\}, \\ & \sum_{i=1}^{n} w_i = 1 \end{aligned}$$

Here, also we will present our analysis for $l = 1$.

Optimal Resilient Topology Design: Scaled attack

$$\tilde{x}_i^{(1)} = \beta\left[\frac{\tilde{w}^T}{\alpha_i}(\alpha \odot x(0)^{(j)}) + \frac{\tilde{w}^T}{\alpha_i}K_i^1\right]$$

Given α_i's are already chosen, the above expression can clearly be written as this :

$$\tilde{x}_i^{(1)} = \beta\left[\sum_l \gamma_l^i \cdot w_l\right]$$

Taking the steady state difference between the i^{th} agent and the j^{th} agent we get :

$$\tilde{x}_i^{(1)} - \tilde{x}_j^{(1)} = \beta\left[\sum_l \gamma_l^i \cdot w_l - \sum_l \gamma_l^j \cdot w_l\right]$$

$$= \beta\left[\sum_l \gamma_l^{ij} \cdot w_l\right] \;\; ; \;\; \gamma_l^{ij} = \gamma_l^i - \gamma_l^j$$

Optimal Resilient Topology Design: Scaled attack

Theorem 3

The Distortion Metric ε_{rel} is bounded by:

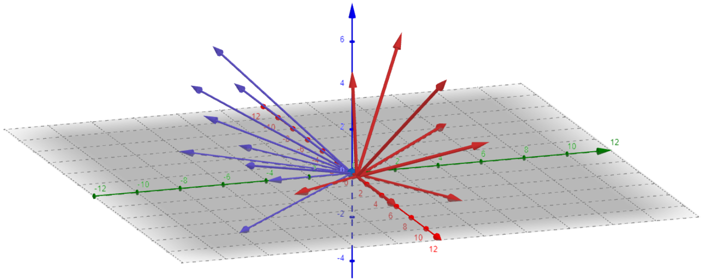
$$2\underline{K}_{\gamma^{ij}} \cdot \sum_i \sum_j cos^2(\theta_{\gamma^{ij} w}) \leq n \cdot \varepsilon_{rel} \leq 2n \cdot \bar{K}_{\gamma^{ij}} \cdot \sum_i \sum_j cos^2(\theta_{\gamma^{ij} w})$$

Assuming there exists w^* for which both the bounds are minimized, the optimal topology L^* is given by solving the synthesis problem ${w^*}^T L^* = 0$ and $\mathbb{1}_n^T w^* = 1$.

A Sub-Optimal Characterization

Aprroach

- $\gamma = \{(i,j) \in \{1,n\} | \gamma_{ij}\}$ be partitioned into 2-nearest neighbor sets (γ_1 and γ_2) such that $\gamma = \gamma_1 \oplus \gamma_2$.
- Considering,$\bar{\gamma}_1$ and $\bar{\gamma}_2$ as the average of the two chosen sets, we just need to choose $w^* = \mathscr{K} \cdot (\bar{\gamma}_1 \times \bar{\gamma}_2)$
- w^* is perpendicular to this generated 2-nearest set vectors (γ_1, γ_2).



Relative distortion error and its relation to connectivity

Definition 4

Connectivity of a graph $G = (V, \mathscr{E})$ is defined as the number of edges the graph has (in other words, $|\mathscr{E}|$). We say graph $G_1 = (V, \mathscr{E}_1)$ is more connected as compared to $G_2 = (V, \mathscr{E}_2)$ if and only if $|\mathscr{E}_1| > |\mathscr{E}_2|$.We change our formal measure of distortion to introduce the relative distortion error. $\|.\|_2^H$ and $\|.\|_2^L$ represents Euclidean norm in higher and lower connectivity, respectively. The modified relative distortion error is as follows :

$$\varepsilon_{rel}^{HL} = \sum_i \sum_j (\|\tilde{x}_i^H - \tilde{x}_j^H - \delta_{ij}\|_2^H - \|\tilde{x}_i^L - \tilde{x}_j^L - \delta_{ij}\|_2^L)$$

Similar Networks

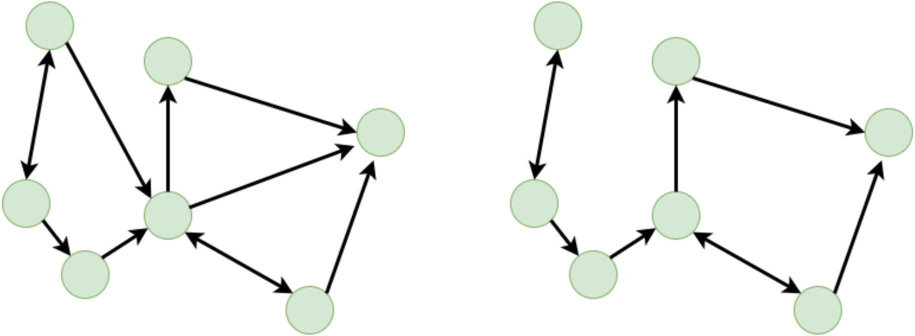


Figure 9: Two Similar Networks with 9 and 6 links respectively.

Lower Bound on Fiedler Eigenvectors considering Similar Networks

Theorem 5

Given two graph laplacians L_h and L_l , the euclidean distance between the left dominant eigenvectors($\tilde{w}_H, \tilde{w}_L$) satisfying $\mathbb{1}_n^T \tilde{w}_H(\succcurlyeq 0) = \mathbb{1}_n^T \tilde{w}_L(\succcurlyeq 0) = 1$ and $\tilde{w}_H^T L_h = \tilde{w}_L^T L_l = \mathbb{0}_n^T$ is bounded by $\|\tilde{w}^H - \tilde{w}^L\|_2 \geq \frac{1}{r} \sum_{n=1}^{r} \frac{|\sum_{i=1}^{m} \tilde{w}_i \sigma_{in}|}{\|C_n\|_2}$.

Where, $\|C_n\|_2$ is the euclidean norm of the n^{th} column of L_h and σ_{ij} is the change in the ij^{th} entry of G and H.

Current Section

Experiments

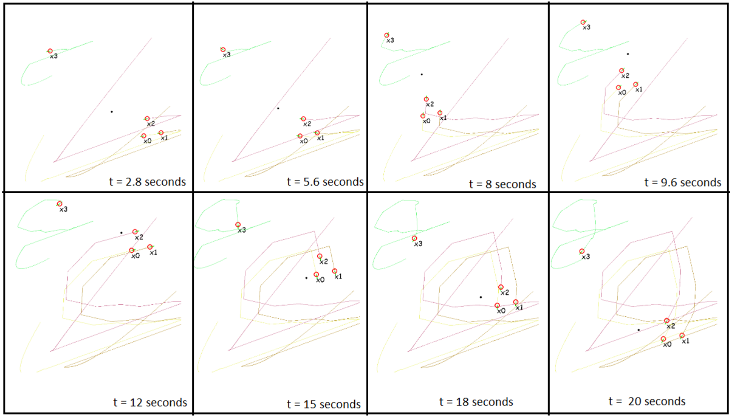


Figure 10: Scaled Attack in Multi-agent Formation Control

Current Section

Conclusions and future work

- Analytical solving the original distortion optimization problem.
- Coming up with refined sub-optimal methods for practical solutions.
- Generalize this problem to time-varying Networks.
- Bounds on the eigenvector

Current Section

References

[1] Abraham Berman, Xiao-Dong Zhang "Lower bounds for the eigenvalues of Laplacian matrices"

[2] Beard, R.W.: Consensus seeking in multiagent systems under dynamically changing interaction topologies. IEEE Trans. Autom. Control 50(5), 655-661

Current Section

Acknowledgement

To ALL those who have MATTERED since the beginning of TIME ...

Thank You