Theory and Algorithms for Safe and Resilient Multi-Agents Systems

Dimitra Panagou

Joint work with

James Usevitch, Kunal Garg and Ehsan Arabi

Aerospace Engineering, University of Michigan
Multi-Agent Planning and Control
Ground, marine, aerial, space vehicles

Safety and Resilience under Uncertainty
Towards advancing autonomy

Nonlinear Control and Estimation
Robust control, estimation and learning
Safety and Resilience Architecture

Safety Control

Agent
\[ \dot{x}_i = f(t, x_i, u_i) \]

Barrier Control

\[ \dot{x}_i, \hat{x}_i, \hat{x}_g \]

Physical Adversaries

Resilient Estimation

Information Filtering

Reference Estimate

State & Goal Estimate

\[ y_i[t] \]

\[ z_i[t] \]

Sensed information

Communicated information

Secure Communication

( Time- and spatially-varying k-circulant graphs )

Cyber Adversaries

\[ X_i[t] \]
• Resilient Multi-Agent Networks
  • Information Reconstruction
  • Formation Control

• Safety Control under Spatiotemporal Constraints
  • Finite-Time Stability (FTS) and Fixed-Time Stability (FxTS)
  • Fixed-Time Control Lyapunov Functions
    • QP approach
    • CLF approach (WeB18.5)

• Future Research
Earlier Resilience Results

- Network as a digraph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, $\mathcal{V} = \{1, \ldots, n\}$, $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$

- Up to $F$-local adversaries
  - Share malicious information and/or do not play consensus

- Resilient Communication Graphs
  - $r$-robustness and $(r,s)$-robustness

- Resilient Filtering: W-MSR algorithm
  - Principle: Each agent
    - sorts received information
    - filters out the $F$ highest and $F$ lowest values
  - Consensus if the network is
    - $(2F+1)$-robust or $(F+1,F+1)$-robust

- Challenges:
  - Checking $r$-robustness and $(r,s)$-robustness is NP-hard
  - Consensus to arbitrary reference values is not guaranteed
Our Resilience Results

- [1]: $k$-circulant graphs have $r$-robustness and $(r,s)$-robustness as functions of $k$
  - Resilient, scalable network topologies [CDC17]

- [2]: Resilient consensus to arbitrary reference values in time-invariant and time-varying graphs
  - Resilient Leader-Follower consensus [ACC18]

- [3]: Resilient formation control
  - In finite time under bounded control inputs [CDC18]

- [4]: Graph $r$-robustness and $(r,s)$-robustness as a MILP
  - More efficient than state-of-the-art methods [ACC19]
  - Approximate lower bounds of $r$- and $(r,s)$-robustness

- [5]: Resilient Barriers for Undirected Networks
  - J. Usevitch et. al. (Journal versions: [5], [6], [7])
• How can the formation be achieved in the presence of misbehaving agents?

• What are the communication topologies and information filters that ensure resilient consensus?

- Time invariant digraph $\mathcal{D} = (\mathcal{V}, \mathcal{E})$, $\mathcal{V} = \{1, \ldots, n\}$
- Agent states $p_i \in \mathbb{R}^n$, $i \in \mathcal{V}$

- $\xi_i \in \mathbb{R}^n \ \forall i \in \mathcal{V}$: Formation vectors (target locations)
- $\tau_i = p_i(t) - \xi_i \ \forall i \in \mathcal{V}$: Center of formation
Definition 1 (Resilient Directed Acyclic Graph (RDAG))

Digraph $\mathcal{D} = (\mathcal{V}, \mathcal{E})$ is RDAG with parameter $r \in \mathbb{N}$ if all of the following properties hold:

1. There exists partitioning of $\mathcal{V}$ into $S_0, \ldots, S_m \subseteq \mathcal{V}$, $m \in \mathbb{Z}$ such that $|S_0| \geq r$

2. For each $i \in S_j$, $1 \leq j \leq m$, $\mathcal{V}_i \subseteq \bigcup_{k=0}^{j-1} S_k$

3. For each $i \in S_j$, $1 \leq j \leq m$, $|\mathcal{V}_i| \geq r$

1) The size of the layer $S_0$ is at least $r$
2) In-neighbors are only from layers above
3) Each agent has at least $r$ in-neighbors
The norm-based W-MSR filtering modifies the above version by collecting and sorting the neighbors’ normed information from highest to lowest value, and removing only the F highest values.
Closed loop system:

\[
\dot{\tau}_i = u_i,
\]

\[
u_i(t) = \gamma_i(t) \sum_{j \in \mathcal{R}_i(t)} w_{ij}(t)(\tau_j - \tau_i)\|\tau_j - \tau_i\|^{\alpha-1}, \quad 0 < \alpha < 1
\]

where

- \( \gamma_i(t) = \frac{\sigma_i(t)}{\|u_i^p\|} \)
- Saturation function:

\[
\sigma_i(t) = \min\{\|u_i^p(t)\|, u_M\},
\]

\[
u_i^p(t) = \sum_{j \in \mathcal{R}_i(t)} w_{ij}(t)(\tau_j(t) - \tau_i(t))\|\tau_j(t) - \tau_i(t)\|^{\alpha-1}, \quad 0 < \alpha < 1
\]

- Input satisfies bounds \( \|u_i\| \leq u_M \) \( \forall i \in \mathcal{V} \)

**Theorem 2**

Consider a digraph \( \mathcal{D} \) which is an RDAG with parameter \( 3F + 1 \), where \( S_0 = \mathcal{L} \) and \( \mathcal{A} \) is an \( F \)-local set. Under the proposed closed loop dynamics, \( \tau_i \) will converge to \( \tau_L \) in finite time for all normal agents \( i \in \mathcal{N} \).
Leaders:
- Determine trajectory for center of formation (COF)
- Encode COF trajectory into unique parameters
- Resiliently transmit parameters to out-neighbors

Followers:
- Receive and accept parameters only if resilience criteria satisfied
- Reconstruct unique trajectory of COF
- Add local formation offset to obtain local desired trajectory
- Track local trajectory
Multi-Source Resilient Propagation Algorithm [8]

- RDAG with parameter \(2F+1\)
- F-local misbehaving agent model
- Including misbehaving leaders
- \(S_0\) layer comprises of leaders only

- Example: RDAG with \(r=3\)
Multi-Source Resilient Propagation Algorithm [8]

- Leaders transmit message to out-neighbors
Multi-Source Resilient Propagation Algorithm [8]

- Leaders transmit message to out-neighbors
- Followers accept message if identically received from at least (F+1) in-neighbors
Multi-Source Resilient Propagation Algorithm [8]

- Leaders transmit message to out-neighbors
- Followers accept message if identically received from at least \((F+1)\) in-neighbors
- Accepted messages by followers transmitted to their out-neighbors, and so on
Safety and Resilience Architecture

Safety Control

Agent
\[ \dot{x}_i = f(t, x_i, u_i) \]

Barrier Control

Information Filtering

Reference Estimate

State & Goal Estimate

Resilient Estimation

Physical Adversaries

Secure Communication

(Time- and spatially-varying k-circulant graphs)

Cyber Adversaries

\[ x_i[t] \]

sensed information

communicated information
Spatiotemporal Control Synthesis: Overview

\[ S_i = \{ x \mid h_i(x) \leq 0 \} \]

\[ S = \{ x \mid h(x) \leq 0 \} \]

- **Safety (set invariance)**
  State trajectories must remain in a safe set

- **Performance (set attractivity)**
  State trajectories must reach desired sets within specified time intervals

**Spatiotemporal Control: Approach**

- **Synthesis tools:**
  Quadratic Programs (QPs) for FTS/FxTS/PTS [9, 10]
  Modified Sontag’s Formula for PTS (ACC20 Paper WeB18.5) [11]

- **Analysis tools:**
  FTS of Switched/Hybrid Systems [12]

- K. Garg, E. Arabi, and D. Panagou
Let \( \dot{x} = f(x) + g(x)u \) where \( x \in \mathbb{R}^n, u \in U \subset \mathbb{R}^m \)

Assume that:

- There exists a safe set \( S_s = \{ x \in \mathbb{R}^n \mid h(x) \leq 0 \} \) where \( h(x) \) is continuously differentiable
- There exist sets \( S_i = \{ x \in \mathbb{R}^n \mid h_i(x) \leq 0 \}, i \in \{0, 1, \ldots, N\} \) where \( h_i(x) \) are continuously differentiable
- \( S_s \cap S_0 \neq \emptyset, S_i \cap S_{i+1} \neq \emptyset \), for \( 0 \leq i \leq N - 1 \)
- There exist time intervals \( [t_i, t_{i+1}) \) such that \( t_{i+1} - t_i \geq \bar{T} \)

**Problem statement (Problem 1)**

Find a control input \( u(t) \in U = \{ A_u u \leq b_u \} \) such that for \( x(0) \in S_s \cap S_0 \),

- \( x(t) \in S_s, \ \forall t \geq 0 \),
- \( x(t) \in S_i, \ \forall t \in [t_i, t_{i+1}) \)
Let $\dot{x} = f(x)$ where $f$ is continuous, $f(0) = 0$

**Finite-Time and Fixed-Time Stability**

### Finite-time Stability (FTS) (Bhat and Bernstein, 2000)

**Theorem 1.** Suppose there exists a positive definite function $V$ for system (1) such that

$$\dot{V}(x) \leq -cV(x)^\beta,$$

with $c > 0$ and $0 < \beta < 1$. Then, the origin of (1) is FTS with settling time function

$$T(x(0)) \leq \frac{V(x(0))^{1-\beta}}{c(1-\beta)}.$$

### Fixed-time Stability (FxTS) (Polyakov, 2012)

**Theorem 1 (2).** Suppose there exists a positive definite function $V$ for system (1) such that

$$\dot{V}(x) \leq -aV(x)^p - bV(x)^q$$

with $a, b > 0$, $0 < p < 1$ and $q > 1$. Then, the origin of (1) is FxTS with continuous settling time $T$ that satisfies

$$T \leq \frac{1}{a(1-p)} + \frac{1}{b(q-1)}.$$

**Prescribed-time Stability (PTS)**

Time of convergence $T$ can be chosen arbitrarily by the user. Also called predetermined or predefined.
Reciprocal Control Barrier Functions (Ames et al, TAC 2017)

**Definition:** Let $\dot{x} = f(x) + g(x)u$, where $f(x), g(x)$ are locally Lipschitz $x \in \mathbb{R}^n, u \in U \subset \mathbb{R}^m$

A continuously differentiable function $B : \text{Int}(C) \to \mathbb{R}$ is called a **Reciprocal Control Barrier Function (RCBF)** for the set $C$ if there exist class K functions $\alpha_1, \alpha_2, \alpha_3$ such that for all $x \in \text{Int}(C)$

$$\frac{1}{\alpha_1(h(x))} \leq B(x) \leq \frac{1}{\alpha_2(h(x))}$$

$$\inf_{u \in U} \left[ L_f B(x) + L_g B(x)u - a_3(h(x)) \right] \leq 0$$

Let the set $K_{rcbf}(x) = \{u \in U : L_f B(x) + L_g B(x)u - a_3(h(x)) \leq 0\}$

Then any locally Lipschitz $u : \text{Int}(C) \to U$ such that $u(x) \in K_{rcbf}(x)$ will render $\text{Int}(C)$ a forward invariant set.
Let the following CLF-CBF QP

\[
\mathbf{u}^*(x) = \arg\min_{u=(u,\delta)\in \mathbb{R}^m \times \mathbb{R}} \frac{1}{2} \mathbf{u}^T H(x) \mathbf{u} + F(x)^T \mathbf{u}
\]

s.t.

\[
\begin{align*}
L_f V(x) + L_g V(x) u + c V(x) - \delta &\leq 0 \\
L_f B(x) + L_g B(x) u - \alpha(h(x)) &\leq 0
\end{align*}
\]

**Theorem** [Ames et al, TAC 2017]:

Suppose that:

- the vector fields \( f \) and \( g \) of the control system,
- the gradients of the RCBF \( B \) and CLF \( V \),
- the cost function terms \( H(x) \) and \( F(x) \) in (CLF-CBF QP)

are all locally Lipschitz. Suppose furthermore that

\[ L_g B(x) = 0 \] for all \( x \in \text{Int}(C) \).

Then the solution, \( \mathbf{u}^*(x) \), of (CLF-CBF QP) is locally Lipschitz continuous for \( x \in \text{Int}(C) \). Moreover, a closed-form expression can be given for \( \mathbf{u}^*(x) \).
• Resilient Multi-Agent Networks
  • Information Reconstruction
  • Formation Control

• Spatiotemporal Control Synthesis
  • Finite-Time Stability (FTS) and Fixed-Time Stability (FxTS)
  • Fixed-Time Control Lyapunov Functions
    • QP approach
    • CLF approach (WeB18.5)

• Future Research
Let $\dot{x} = f(x) + g(x)u$ where $x \in \mathbb{R}^n, u \in U \subset \mathbb{R}^m$

**Definition:** The continuously differentiable function $V : \mathbb{R}^n \to \mathbb{R}$ is called a **Fixed-Time Control Lyapunov Function** wrt a set $S$ (FxT-CLF-S) of the system with parameters $a_1, a_2, b_1, b_2$ if

i) It is positive definite wrt a closed set $S$, i.e.,

- $V(x) > 0$ for $x \notin S$
- $V(x) = 0$ for $x \in \partial S$

ii) $\inf_u[L_fV(x) + L_gV(x)u] \leq -a_1(V(x))^{b_1} - a_2(V(x))^{b_2}, \forall x \notin \text{Int}(S)$

where $a_1, a_2 > 0, b_1 > 1, 0 < b_2 < 1$ satisfy

$$\frac{1}{a_1(b_1 - 1)} + \frac{1}{a_2(1 - b_2)} \leq \bar{T}$$

with $\bar{T}$ being a user-defined time.
Theorem [9]

If there exist \( a_{i1}, a_{i2}, \lambda, \lambda_i > 0, b_{i1} > 1, 0 < b_{i2} < 1 \) and control input \( u \) such that

\[
\bar{T} \geq \max_{i \in \Sigma} \left\{ \frac{1}{a_{i1}(b_{i1} - 1)} + \frac{1}{a_{i2}(1 - b_{i1})} \right\} \quad (C_0)
\]

\[
\inf_{u \in U} \{ L_f h + L_g hu + \lambda h \} \leq 0 \quad (C_1)
\]

\[
\inf_{u \in U} \{ L_f h_i + L_g h_i u + \lambda_i h_i \} \leq 0 \quad (C_2)
\]

\[
\inf_{u \in U} \{ L_f h_{i+1} + L_g h_{i+1} u \} \leq -a_{i1} \max\{0, h_{i+1}\}^{b_{i1}} - a_{i2} \max\{0, h_{i+1}\}^{b_{i2}} \quad (C_3)
\]

hold for \( t \in [t_i, t_{i+1}) \), then, the control input \( u(t) \) solves Problem 1.

- \( C_0 \) ensures exact convergence before \( t = t_{i+1} \) (FxTS for settling time \( \bar{T} \))
- \( C_1 \) results into \( h(x) = 0 \Rightarrow \dot{h}(x) \leq 0 \Rightarrow \) forward invariance of set \( S_s \)
- \( C_2 \) results into \( h_i(x) = 0 \Rightarrow \dot{h}_i(x) \leq 0 \Rightarrow \) forward invariance of set \( S_i \)
- \( C_3 \) results into \( \dot{h}_{i+1} \leq -a_{i1} h_{i+1}^{b_{i1}} - a_{i2} h_{i+1}^{b_{i2}} \Rightarrow \) FxTS to set \( S_{i+1} \)
- \( C_3 \) also results into forward invariance of \( S_{i+1} \) once \( x(t) \in S_{i+1} \)
A Quadratic Program (QP) to solve Problem 1

**Theorem [9]**

Let the solution to the following QP defined for \( t \in [t_i, t_{i+1}) \):

\[
\begin{align*}
\min_{v, a_{i1}, a_{i2}, \lambda_i, \delta} & \quad \frac{1}{2} v^2 \\
\text{s.t.} & \quad L_f h_i + L_g h_i v + \lambda_i h_i \leq 0, \\
& \quad L_f h_{i+1} + L_g h_{i+1} v \leq \delta h_{i+1} - a_{i1} \max\{0, h_{i+1}\}^{b_{i1}} - a_{i2} \max\{0, h_{i+1}\}^{b_{i2}}, \\
& \quad A_u v \leq b_u, \\
& \quad \frac{2}{T} \leq a_{i1} (b_{i1} - 1) \leq a_{i2} (1 - b_{i2}),
\end{align*}
\]

be denoted as \([\bar{v}_i(t), a_{i1}, a_{i2}, \lambda_i, \lambda_i] \). Then, \( u(t) = \bar{v}_i(t) \) for \( t \in [t_i, t_{i+1}) \) solves Problem 1.
Theorem (Robust FxTS Theorem)

Let $V : \mathbb{R}^n \rightarrow \mathbb{R}$ be a $C^1$, positive definite function, satisfying

$$\dot{V} \leq -c_1 V^{a_1} - c_2 V^{a_2} + c_3 V,$$

with $c_1, c_2 > 0$, $a_1 = 1 + \frac{1}{\mu}$, $a_2 = 1 - \frac{1}{\mu}$ for some $\mu > 1$, along the system trajectories. Then, there exists $D \subset \mathbb{R}^n$ such that for all $x(0) \in D$, the system trajectories reach the origin in a fixed time $T$. Furthermore, if $c_3 < 2\sqrt{c_1 c_2}$, and $V$ is radially unbounded, then $D = \mathbb{R}^n$.

- Relaxation of condition $\dot{V} \leq -c_1 V^{a_1} - c_2 V^{a_2}$
- Robustness w.r.t. additive vanishing disturbance if origin of nominal system is FxTS
- Helps guarantee feasibility of QP
Consider the following optimization problem:

$$\min_{u, \delta_1, \delta_2} \frac{1}{2} ||u||^2 + p_1 \delta_1^2 + p_2 \delta_2^2$$

s.t. $$A_u u \leq b_u,$$

$$L_f h_g(x) + L_g h_g(x) u \leq \delta_1 h_g(x) - \alpha_1 h_g(x)^{\gamma_1} - \alpha_2 h_g(x)^{\gamma_2},$$

$$L_f h_s(x) + L_g h_s(x) u \leq -\delta_2 h_s(x),$$

where $$p_1, p_2 > 0, \gamma_1 = 1 + \frac{1}{\mu}$$ and $$\gamma_2 = 1 - \frac{1}{\mu}$$ with $$\mu > 1, \alpha_1 = \alpha_2 = \frac{\mu \pi}{2T}.$$ 

- Slack terms $$\delta_1, \delta_2 \rightarrow$$ feasibility for all $$x$$
- $$\delta_1$$ dictates region of convergence
- Convergence time $$\leq \bar{T}$$

**Theorem 5.** Let Assumption 3 hold. If the solution of (10), given as \((v^*(\cdot), \delta_1^*(\cdot), \delta_2^*(\cdot))\), satisfies
\[
\delta_1^*(x) < 2\sqrt{\alpha_1\alpha_2}, \quad \forall x \in S_S,
\]
then, for all \(x(0) \in S_S\), the closed-loop trajectories \(x(t)\) under \(u(\cdot) = v^*(\cdot)\) reach the set \(S_G\) in a fixed time, while satisfying safety requirement, i.e., \(x(t) \in S_S\) for all \(t \geq 0\). If (11) does not hold, then there exists \(D \subset S_S\) such that for all \(x(0) \in D\), the closed-loop trajectories satisfy \(x(t) \in S_S\) for all \(t \geq 0\) and reach the goal set \(S_G\) within a fixed time.

**Assumption 3:** The strict complementary slackness holds.
Simulation Results

System Dynamics:
\[ \dot{x}_i = u_i \]

Objective:
\[(x_1, t) = G_{[0,T_4]} \phi_s \land F_{[0,T_1]} \phi_2 \land F_{[T_1,T_2]} \phi_3 \land F_{[T_2,T_3]} \phi_4 \land F_{[T_3,T_4]} \phi_1 \]
\[(x_2, t) = G_{[0,T_4]} \phi_s \land F_{[0,T_1]} \phi_2 \land F_{[T_1,T_2]} \phi_1 \land F_{[T_2,T_3]} \phi_4 \land F_{[T_3,T_4]} \phi_3 \]

Equivalently,

- \( x_1(t), x_2(t) \in S_s = \{x_i(t)| ||x_i||_{\infty} \leq 2, ||x_i||_2 \geq 1.5 \} \) for all \( t \geq 0 \), and maintain a minimum separation \( d_m \) at all times.
- On or before a given \( T_1 \) satisfying \( 0 < T_1 < \infty \), agent 1 and 2 should reach the square \( C_2 \) and so on.
Simulation Results

Construction of sets $\bar{S}, \bar{S}_i$

Closed-loop trajectories

Control input and inter-agent distance

Example: STL Mission Synthesis
• Resilient Multi-Agent Networks
  • Information Reconstruction
  • Formation Control

• Safety Control under Spatiotemporal Constraints
  • Finite-Time Stability (FTS) and Fixed-Time Stability (FxTS)
  • Fixed-Time Control Barrier Functions
    • QP approach
    • CLF approach (WeB18.5)

• Future Research
Problem 1. Find a control input $u_i(t) \in \mathcal{U}_i = \{v \in \mathbb{R}^m; \quad u_{i,\min_j} \leq v_j \leq u_{i,\max_j}, j = 1, 2, \ldots, m\}, \ t \geq 0,$ such that for all $x_i(0) \in S_{S_i},$

- $x_i(\bar{T}) \in S_G$, for some user-defined $\bar{T} > 0$, for all $i = 1, 2, \ldots, N$;
- $\|x_i(t) - x_j(t)\| \geq d_s$, for all $t \geq 0$, for all $i \neq j$, where $d_s > 0$ is a user-defined safety distance;
- $x_i(t) \in S_{S_i}$, for all $t \geq 0$, for all $i = 1, 2, \ldots, N$. 

\[ x_1 \quad x_2 \]
-30 -20 -10 0 10 20 30
-30 -20 -10 0 10 20 30

• CBF condition for set invariance

\[ \sum_{i=1}^{N} \left( \frac{\partial h(\vec{x})}{\partial x_i} f_i(x_i) + \frac{\partial h(\vec{x})}{\partial x_i} g_i(x_i)u_i \right) \geq -\alpha(h(\vec{x})) \]

\( \alpha \): any locally Lipschitz extended class-\( K_{\infty} \) function

• Worst-case adversarial agents:

\[ u_k^{\inf}(t) = \arg \inf_{u_k \in \mathcal{U}_k} \left[ \frac{\partial h(\vec{x})}{\partial x_k} (f_k(x_k) + g_k(x_k)u_k) \right] \]

• Intent: drive \( h(\vec{x}) \) to negative value (violate set invariance)

• Best-case control action for normal agents:

\[ u_i^{\sup}(t) = \arg \sup_{u_i \in \mathcal{U}_i} \left[ \frac{\partial h(\vec{x})}{\partial x_i} (f_i(x_i) + g_i(x_i)u_i) \right] \]

• Intent: drive \( h(\vec{x}) \) to positive value (preserve set invariance)

\[ \sum_{i \in \mathcal{V} \setminus \mathcal{A}} \sup_{u_i \in \mathcal{U}_i} \left[ \frac{\partial h(\vec{x})}{\partial x_i} (f_i(x_i) + g_i(x_i)u_i) \right] + \sum_{k \in \mathcal{A}} \inf_{u_k \in \mathcal{U}_k} \left[ \frac{\partial h(\vec{x})}{\partial x_k} (f_k(x_k) + g_k(x_k)u_k) \right] \geq -\alpha(h(\vec{x})) \]
CAREER: Autonomy of Multi-Agent Systems

10 Years: Safe and Secure Multi-Agent Systems

5 Years: Perceivability via Synergistic Control and Observation in Given Time Horizons

Network

Fooding / Estimation

Controller

Platform

\( x = \mathcal{X}[t] \)

Safe Set Estimator

Goal Set Estimator

External Communication

\( u_t[t] \)

\( \mathcal{X}[t], \dot{X}[t], X[i] \)

\( \mathcal{X}_u[t] \)

\( \mathcal{X}_v[t] \)

\( \mathcal{X}_s[t] \)

Communication influence

sensing uncertainty

unsafe sets

environmental influence

goal set

safe set
[1] J. Usevitch and D. Panagou “r-Robustness and (r,s)-Robustness of Circulant Graphs”, CDC 2017
Thank you!

Questions?