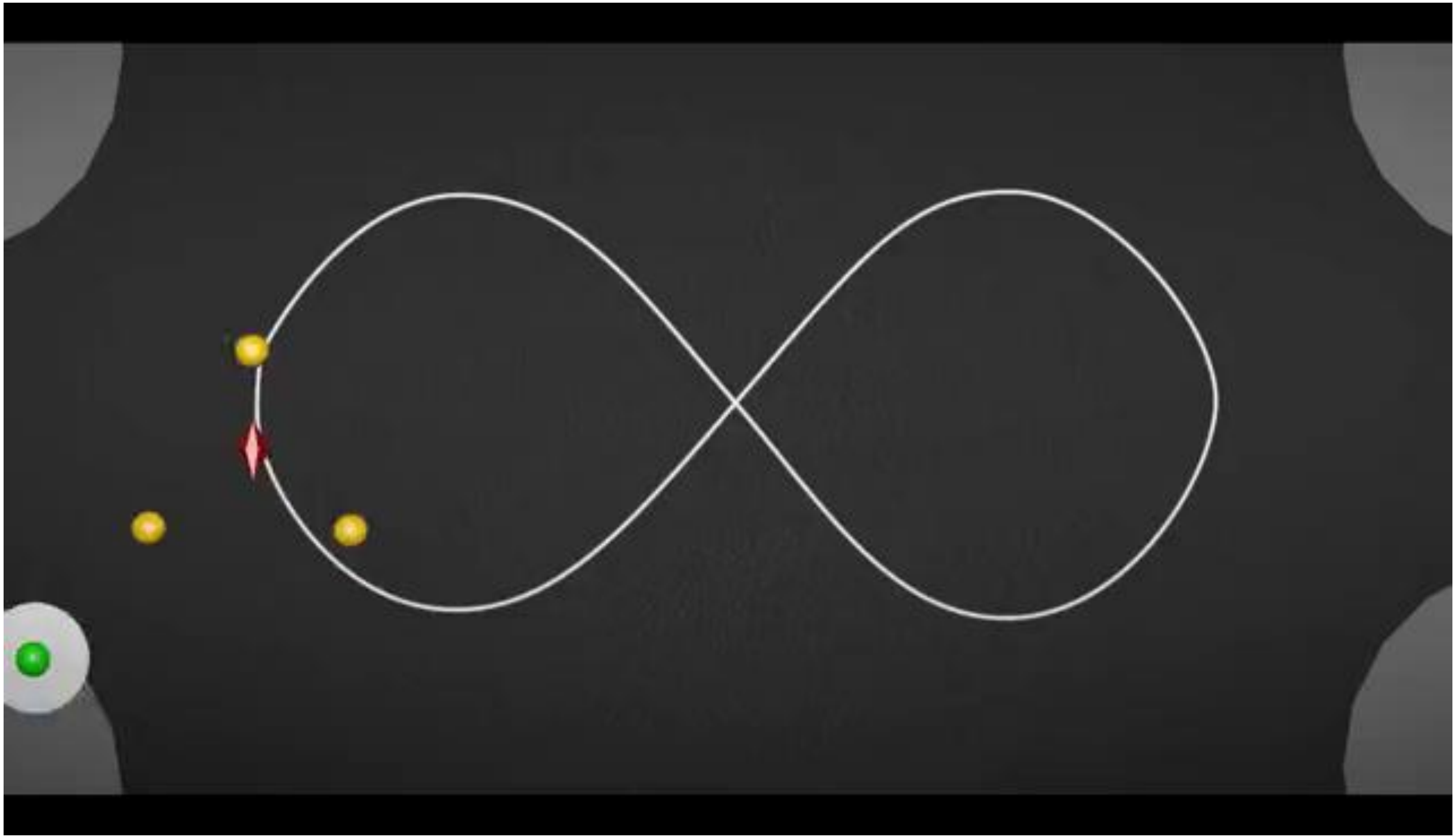
Relay-Explorer Approach for Multi-Agent Exploration of an Unknown Environment with Intermittent Communication

Submitted for publication

R. Sun, C. Harris, Z. I. Bell, and W. E. Dixon

What is Relay-Explorer control?

Stability Analysis



UF UNIVERSITY of FLORIDA

Duke UNIVERSITY

TEXAS The University of Texas at Austin

UC SANTA CRUZ

System Model

- Relay Agent:

$$\dot{x}_r(t) \triangleq f_r(x_r(t)) + v_r(x_r(t)) + d_r(t)$$

- Explorer Agents:
  - Explorer Leader:

$$\dot{x}_0(t) \triangleq f_e(x_0(t)) + v_0(x_0(t)) + d_0(t)$$

  - Explorer Followers:

$$\dot{x}_i(t) \triangleq f_e(x_i(t)) + v_i(x_i(t)) + d_i(t)$$

drift dynamics: f_r, f_e

agent states: x_r, x_0, x_i

control input: v_r, v_0, v_i

disturbances: d_r, d_0, d_i

Control Development

- Relay Agent:

$$\begin{aligned} e_r(t) &\triangleq x_r(t) - x_{rd}(t), \\ \hat{e}_r(t) &\triangleq \hat{x}_r(t) - x_{rd}(t), \\ \tilde{e}_r(t) &\triangleq x_r(t) - \hat{x}_r(t), \end{aligned}$$

- Explorer Leader:

$$\begin{aligned} e_0(t) &\triangleq x_0(t) - x_{0d}(t), \\ \hat{e}_0(t) &\triangleq \hat{x}_0(t) - x_{0d}(t), \\ \tilde{e}_0(t) &\triangleq x_0(t) - \hat{x}_0(t), \end{aligned}$$

- Explorer Followers:

$$\hat{e}_i(t) \triangleq \hat{x}_i(t) - \hat{x}_0(t) - p_i$$

Control Development

- Observer design for the relay agent:

$$\dot{\hat{x}}_r(t) \triangleq f_r(\hat{x}_r(t)) + v_r(\hat{x}_r(t))$$

- Explorer Leader:

$$\dot{\hat{x}}_0(t) \triangleq f_e(\hat{x}_0(t)) + v_0(\hat{x}_0(t))$$

- Explorer Followers:

$$\dot{\hat{x}}_i(t) \triangleq f_e(\hat{x}_i(t)) + v_i(\hat{x}_i(t))$$

Control Development

- Control design for the relay agent:

$$v_r\left(x_r\left(t\right)\right) \triangleq -k_r e_r\left(t\right) - f_r\left(x_r\left(t\right)\right) - \bar{d}_r \mathrm{sgn}\left(e_r\left(t\right)\right) + \dot{x}_{rd}\left(t\right),$$
$$v_r\left(\hat{x}_r\left(t\right)\right) \triangleq -k_{\hat{r}} \hat{e}_r\left(t\right) - f_r\left(\hat{x}_r\left(t\right)\right) + \dot{x}_{rd}\left(t\right)$$

- Control design for the explorer leader:

$$v_0\left(\hat{x}_0\left(t\right)\right) \triangleq -k_{\hat{e},0}\hat{e}_0\left(t\right) - f_e\left(\hat{x}_0\left(t\right)\right) + \dot{x}_{0d}\left(t\right)$$

- Distributed control design for explorer follower i :

$$v_i\left(\hat{x}_i\left(t\right)\right) \triangleq k_{\hat{e},f}\sum_{j\in\mathcal{N}_i, j\neq 0}\left(\hat{x}_j\left(t\right) - \hat{x}_i\left(t\right) - p_j + p_i\right)$$
$$+ k_{\hat{e},f}\left(p_i + \hat{x}_0\left(t\right) - \hat{x}_i\left(t\right)\right)$$

Stability Analysis

- Six theorems are developed to show RE w/formation control.
  - Thm 1 shows the trajectory tracking error of the relay agent is bounded when $\phi_r = a_r$.
  - Thm 2 and Thm 3 show the trajectory tracking error of the relay agent is bounded when $\phi_r = u_r$, provided the maximum dwell-time condition is satisfied for the relay agent.
  - Thm 4 shows the estimated tracking error of the explorer leader is bounded for $t \in \left[t_m^a, t_{m+1}^a\right)$.
  - Thm 5 shows the trajectory tracking error of the explorer leader is bounded for $t \in \left[t_m^a, t_{m+1}^a\right)$, provided the maximum dwell-time condition is satisfied for the explorer leader.
  - Thm 6 shows the explorer agents achieved formation control and leader tracking with the distributed controller.

Detection and Mitigation of False Data Injection Attacks in NCS

IEEE Trans Industrial Informatics 2020

A. Sargolzaei, K. Yazdani, A. Abbaspour, C. D. Crane, and W. E. Dixon

Overview

- A common type of cyber effect in network control system is a false data injection (FDI) attack.
- An Observer/Controller is developed for linear systems subject to FDI attacks.
- Attacks are detected (and distinguished from nominal uncertainty) through a Neural Network whose weights are updated by an Extended Kalman Filter

Uncertain Model

$$\begin{cases} X_{k+1} = A_d X_k + B_d U_k + D\xi_k + F(\Delta P_l)_k \\ Z_k = C_d X_k + M_k + \theta_k \end{cases}$$

Observer

$$\begin{cases} \dot{\hat{X}}(t) = A\hat{X}(t) + BU(t) + L(Z(t) - \hat{Z}(t)) \\ \hat{Z}(t) = C\hat{X}(t) + \hat{M}(t) \end{cases}$$

Observer Design

- The observer gain is selected as

$$L(t) = \Sigma(t) C^T \Theta^{-1}.$$

$$\dot{\Sigma}(t) = A\Sigma(t) + \Sigma(t) A^T - \Sigma(t) C^T \Theta^{-1} C \Sigma(t) + D \Xi D^T.$$

- NN-based FDI estimator (weight update laws are tuned from a EKF structure)

$$\hat{M}^i(t) = W^i(t) \sigma \left(V^i(t) \delta^i(t) \right)$$

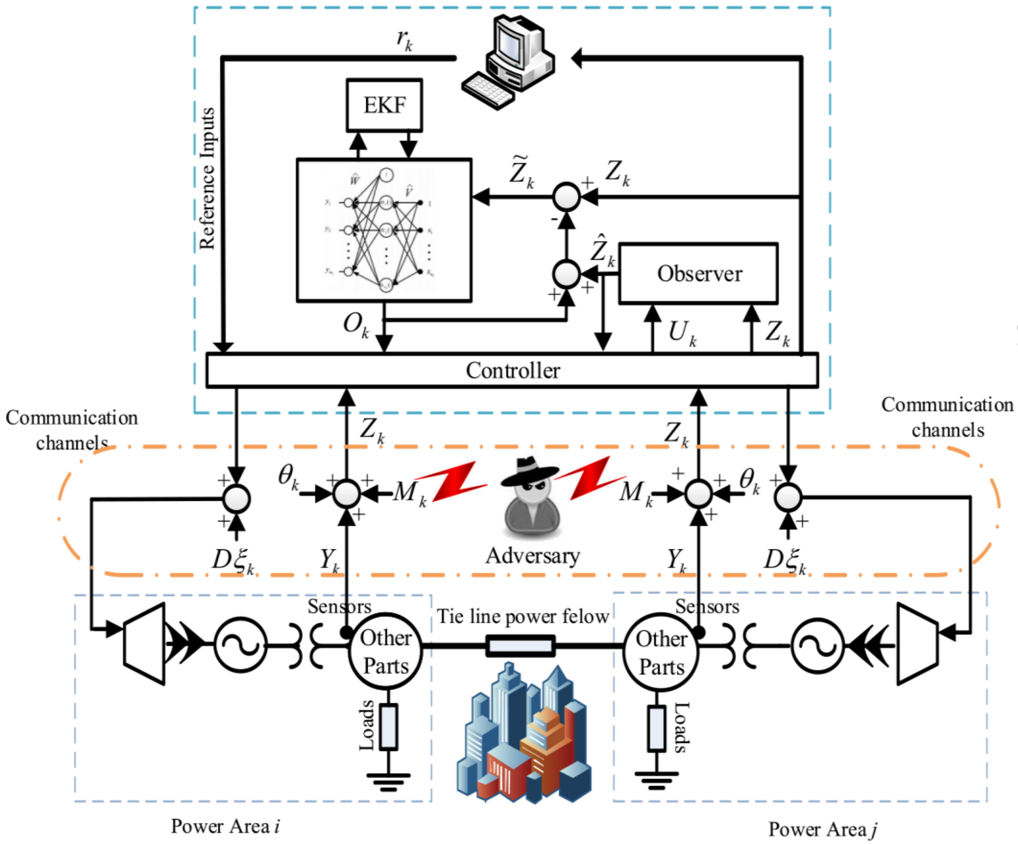
$$\zeta_k^i = \left[W_k^i, V_k^{i,1}, \ldots, V_k^{i,a+b} \right]^T. \qquad \zeta_k^i = \zeta_{k-1}^i + \eta^i \lambda_k^i [z_k^i - \hat{z}_k^i]$$

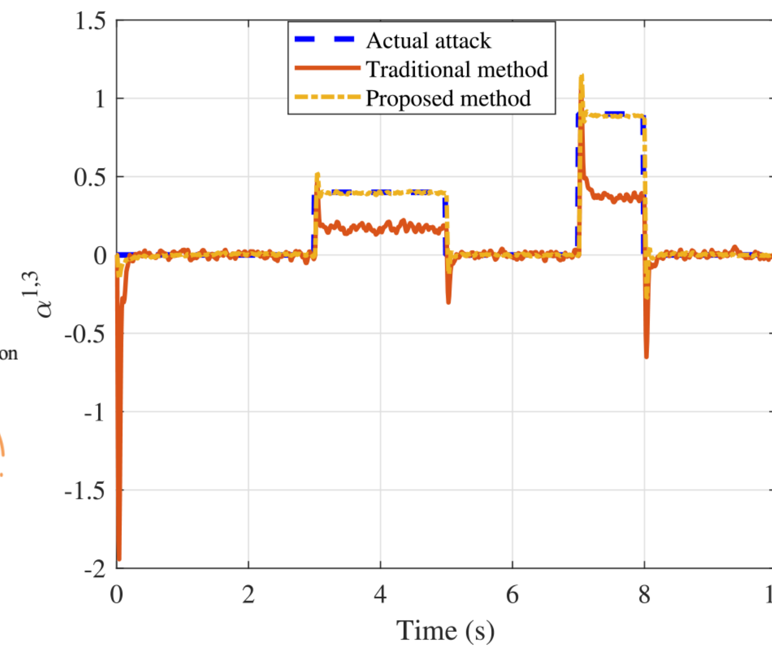
$$\lambda_k^i = \rho_k^i H_k^i [(H_k^i)^T \rho_k^i H_k^i + \Upsilon_k^i]^{-1}$$

$$H_k^i = \frac{\partial e_k^i}{\partial \lambda_k^i} \Big|_{\zeta_i = \lambda_{k-1}^i} = \begin{cases} \sigma(z_k^i) & \zeta^i = W^i \\ W_k^i \hat{M}_{k-j}^i \acute{\sigma}(z_k^i) & \zeta^i = V^{i,j} \\ W_k^i e_{k-j}^i \acute{\sigma}(z_k^i) & \zeta^i = V^{i,a+j} \end{cases}$$

LFC Example

- Simulation results for load frequency control on smart grid





- Examined four different attack signals, and outperformed previous published results

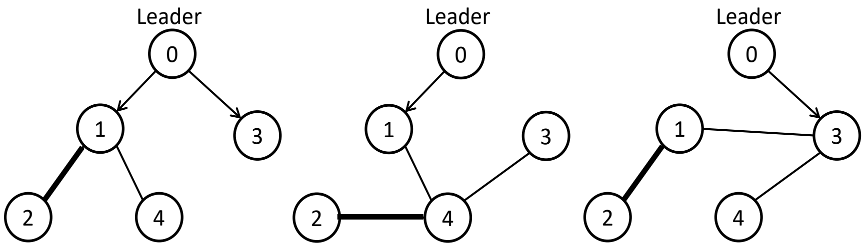
Event/Self-Triggered Approximate Leader-Follower Consensus with Resilience to Byzantine Adversaries

CDC 2019

F. Zegers, P. Deptula, J. Shea, and W. E. Dixon

Intermittent Measurements

- Intermittency can result in time varying topologies



$\bar{\mathcal{G}}_1$ $\bar{\mathcal{G}}_2$ $\bar{\mathcal{G}}_3$

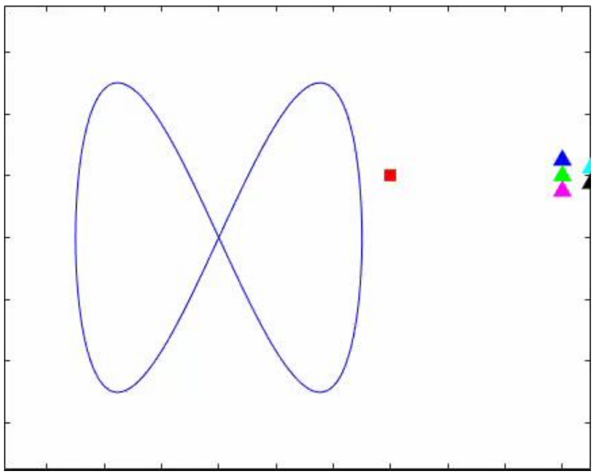
$$\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, \mathcal{A})$$
$$H_p = L_p + D_p, \; p = 1, \, 2, \, 3$$

- Switched systems theory provides a framework for analyzing the stability and performance of the resulting switched/hybrid dynamic system

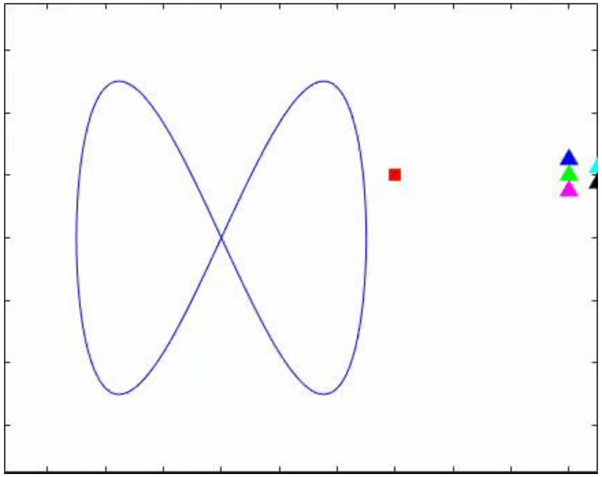
- Dynamics matter for these problems because of the need to develop predictors
  - Frameworks from Nonsmooth Analysis provide toolsets to allow switching with uncertainty
  - Network specific challenges: connectivity, fixed or time-varying topology, directed/undirected, signed/unsigned, resiliency

Motivation

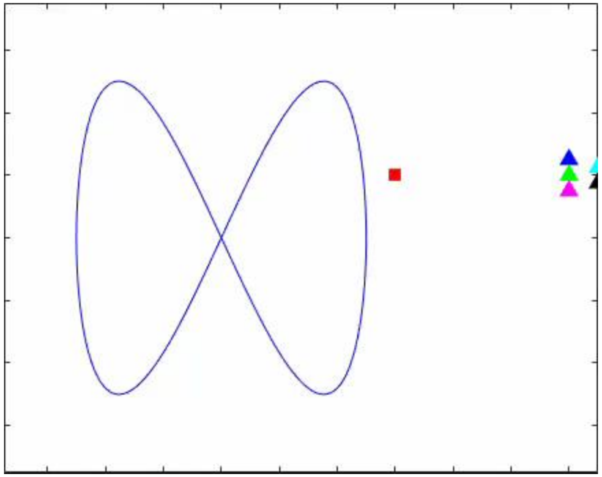
Neutral Environment



Contested Environment



Type I Byzantine Adversary: Communicates False Data



Type II Byzantine Adversary: Abandons MAS

UF UNIVERSITY of FLORIDA · Duke UNIVERSITY · TEXAS The University of Texas at Austin · UC SANTA CRUZ

Byzantine Model

Common threats for a mobile network

- Denial-of-Service (DoS)
- Time-Delay Switch (TDS)
- False Data Injection (FDI)

Byzantine attack: a more general threat where communication can be delayed, corrupted, and/or interrupted arbitrarily

Current Assumptions:
- Only followers can become Byzantine
- No teamwork between Byzantine agents

- **Type I** - Physically remains within network; FDI

- **Type II** - Abandons network

Agent Categorization

- A Type I Byzantine agent is defined as a follower that executes the intended controller but communicates false state information about itself to its neighbors.

- A Type II Byzantine agent is defined as a follower that executes a controller that is different from the intended controller or executes the intended controller under the influence of faulty hardware, while communicating true or no state information about itself to its neighbors.

- A cooperative agent is defined as a follower that successfully executes the intended controller and provides true state information about itself to all its neighbors.

$$\mathcal{D}_i = \lim_{t \to \left(t_k^i\right)^-} \Xi_i(t) \leq 0,$$

$$\mathcal{X}_i = \left(x_i(t) = \vartheta_1(t)\, x_i(t) + \vartheta_2(t)\right),$$

$$\mathcal{T}_i = t_k^i \leq t_{k-1}^i + \Delta_i.$$

With respect to follower *j*, follower $i \in \mathcal{N}_j(t)$ is

$$\begin{cases} \text{cooperative}, & \mathcal{D}_i \wedge \mathcal{X}_i \wedge \mathcal{T}_i \\ \text{Type I}, & \neg\left(\mathcal{D}_i \vee \mathcal{X}_i\right) \wedge \mathcal{T}_i \\ \text{Type II}, & \neg\left(\mathcal{D}_i \wedge \mathcal{T}_i\right) \wedge \mathcal{X}_i. \end{cases}$$

Objective

Design a distributed controller for the followers that

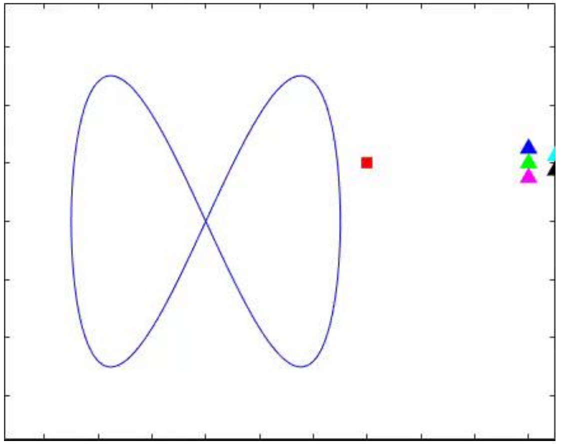
- performs approximate leader-follower consensus, i.e.,

$$\varepsilon \in \mathbb{R}_{>0}$$

$$\limsup_{t\to\infty} \|e_{1,i}(t)\| \leq \varepsilon \quad \forall i \in \mathcal{V} \setminus \left(\bigcup_{i\in\mathcal{V}} \bigcup_{k\in\mathbb{Z}_{\geq 0}} \mathcal{B}\left(t_k^i\right) \right)$$

$$e_{1,i}(t) \triangleq x_i(t) - x_0(t)$$

- Event-Triggered
- Resilient to Byzantine adversaries



Assumptions

- Each agent can measure its position for all time
- The pair (A, B) is stabilizable
- The control and position of the leader are bounded
- The leader is a cooperative agent for all time
- The graph of the CMAS is connected for all time
- At least one cooperative follower is connected to the leader for all time

Limitations of Detector

- Exact model knowledge
- Bound on neighbor's control
- No re-integration

....A Reputation-Based Approach

Reputation-Based Event-Triggered Formation Control and Leader Tracking with Resilience to Byzantine Adversaries

2020 ACC

F. Zegers, M. Hale, J. Shea, and W. E. Dixon

Problem Formulation

Problem Formulation

- Consider a heterogeneous multi-agent system of *N* follower agents and a single leader

- Influence between followers: Weight Undirected Network Topology

$$\mathcal{G}(t) = (\mathcal{V}, \mathcal{E}(t), \mathcal{A}(t))$$

$$\mathcal{V} \triangleq \{1, 2, \ldots, N\}$$

$$\mathcal{E}(t) \subseteq \mathcal{V} \times \mathcal{V}$$

$$\mathcal{A} \triangleq [a_{ij}] \in \mathbb{R}_{\geq 0}^{N \times N}$$

$$\mathcal{G}_C(t) = (\mathcal{C}(t), \mathcal{E}_C(t), \mathcal{A}_C(t)) \subseteq \mathcal{G}(t)$$

Subgraph of cooperative agents

$$H(t) = L(t) + B(t)$$

Connectivity matrix encoding flow of information between the followers and the leader

- Dynamics of agent *i* (control affine)

$$\dot{x}_i(t) \triangleq f_i(x_i(t)) + g_i(x_i(t))\, u_i(t) + d_i(t)$$

Problem Formulation

Objective: Design a controller for the followers that

- achieves formation control and leader tracking (FCLT)
- is distributed & event-triggered
- is resilient to Byzantine adversaries

Assumptions

- The uncertain drift dynamics are continuously differentiable and bounded given a bounded argument
- The control effectiveness matrix is continuously differentiable, full-row rank, and bounded given a bounded argument
- The disturbance is bounded
- All followers are initially cooperative
- The leader is cooperative for all time
- All agents can measure their state
- The control and state of the leader are bounded
- If agent *i* broadcasts its state to its neighbors, then all neighbors receive *r-1* reliable copies of the state of agent *i*
- The graph $\mathcal{G}_C(t)$ is connected for all time

UF UNIVERSITY of FLORIDA Duke UNIVERSITY TEXAS The University of Texas at Austin UC SANTA CRUZ

Trust Model

Idea: Make edge weights a function of trust, use multi-point authentication

Given r state measurements from neighbor $j \in \mathcal{N}_i\left(t_k^j\right)$

$$\Psi_{ij}\left(t_k^j\right) = \sum_{p=1}^{r-1} \sum_{q>p}^{r} \left\| x_{j,p}\left(t_k^j\right) - x_{j,q}\left(t_k^j\right) \right\|$$

Measures discrepancy in state information of agent *j* wrt agent *i*

$x_{j,1}\left(t_k^j\right)$ = communicated state

$x_{j,2}\left(t_k^j\right)$ = sensed state

Example of two-point authentication scenario (r=2)

Let $S_j = \left\{ t_k^j \in \mathbb{R}_{\geq 0} : t - t_{\text{reset}} \leq t_k^j < t \right\}$

$$\tau_{ij}(t) = \begin{cases} 1, & |S_j| = 0 \\ \frac{1}{|S_j|} \sum_{t_k^j \in S_j} e^{-s_1 \Psi_{ij}\left(t_k^j\right)}, & |S_j| \neq 0 \end{cases}$$

Controls rate of change of trust

Reputation Model

Cannot isolate Byzantine agent from MAS

$$\dot{\zeta}_{ij}(t) = \operatorname{proj}\left(\underbrace{\eta_{\tau}\left(\tau_{ij}(t) - \zeta_{ij}(t)\right)}_{\text{Accounts for what } i \text{ thinks of } j} + \sum_{n \in \mathcal{N}_{ij}(t)} \underbrace{\eta_{\zeta}\zeta_{in}(t)\left(\zeta_{nj}\left(t_k^n\right) - \zeta_{ij}(t)\right)}_{\text{Accounts for what } k \text{ thinks of } j \text{ weighted by what } i \text{ thinks } k} \right)$$

$$\operatorname{proj}\left(\dot{x}(t)\right) \triangleq \begin{cases} \dot{x}(t), & x_{\min} < x(t) \wedge x(t) < x_{\max} \\ \dot{x}(t), & x_{\min} = x(t) \wedge \dot{x}(t) > 0 \\ \dot{x}(t), & x_{\max} = x(t) \wedge \dot{x}(t) < 0 \\ 0, & \text{otherwise} \end{cases}$$

$$\zeta_{ij}(t) \in [0, 1] \; \forall t \geq 0$$

Edge Weight

Edge weight policy

$$a_{ij}(t) = \begin{cases} \zeta_{ij}(t), & \zeta_{ij}(t) \geq \zeta_{\min} \text{ and } j \in \mathcal{N}_i(t) \\ 0, & \zeta_{ij}(t) < \zeta_{\min} \text{ or } j \notin \mathcal{N}_i(t), \end{cases}$$

$$\zeta_{\min} \in [0, 1]$$

Cooperative & Byzantine neighbor set of agent *i*

$$\mathcal{C}_i(t) = \{j \in \mathcal{N}_i(t) : a_{ij}(t) \neq 0\}$$

$$\mathcal{B}_i(t) \triangleq \mathcal{N}_i(t) \setminus \mathcal{C}_i(t)$$

Benefits

- No exact model knowledge needed for detection
- No bounds on neighbor quantities needed
- Enables re-integration of rehabilitated agents

Closed-Loop Dynamics

Controller, Observer, and Event Trigger of Follower *i*:

$$u_i(t) = g_i^{+}(x_i(t))\left(k_1 z_i(t) + k_2 e_{2,i}(t)\right)$$

$$z_i(t) = \sum_{j \in \mathcal{N}_i(t)} a_{ij}(t)\left(\hat{x}_j(t) - \hat{x}_i(t) \underbrace{- v_j + v_i}_{\text{Follower } i \text{ knows the formation}}\right) + b_i(t)\left(v_i + x_0(t) - \hat{x}_i(t)\right)$$

Follower *i* knows the formation

Positive only if connected to leader

$$\hat{x}_j(t) = x_{j,1}\left(t_k^j\right), \quad t \in \left[t_k^j, t_{k+1}^j\right)$$

State estimate of follower *j*, which is synchronized among all $i \in \mathcal{N}_j(t) \cup \{j\}$

$$t_{k+1}^i = \inf\left\{t > t_k^i : \phi_2 \left\|e_{2,i}(t)\right\|^2 \geq \phi_3 \left\|z_i(t)\right\|^2 + \frac{\varepsilon}{N}\right\}$$

Positive parameters

Positive parameter used to exclude Zeno behavior in trigger, selected small

Result

The trust model, reputation model, edge weight policy, state observer, and controller ensure E_1 is globally uniformly ultimately bounded in the sense that

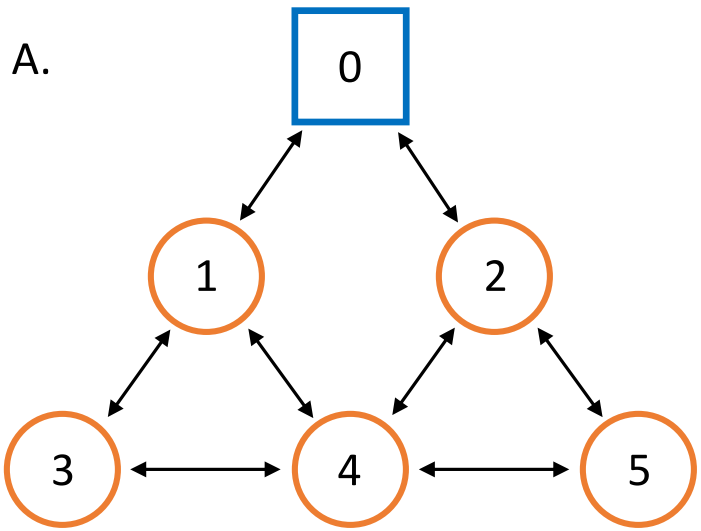
$$\|E_1\| \leq \sqrt{\beta_1 e^{-\beta_3 t} + \beta_2 \left(1 - e^{-\beta_3 t}\right)}$$

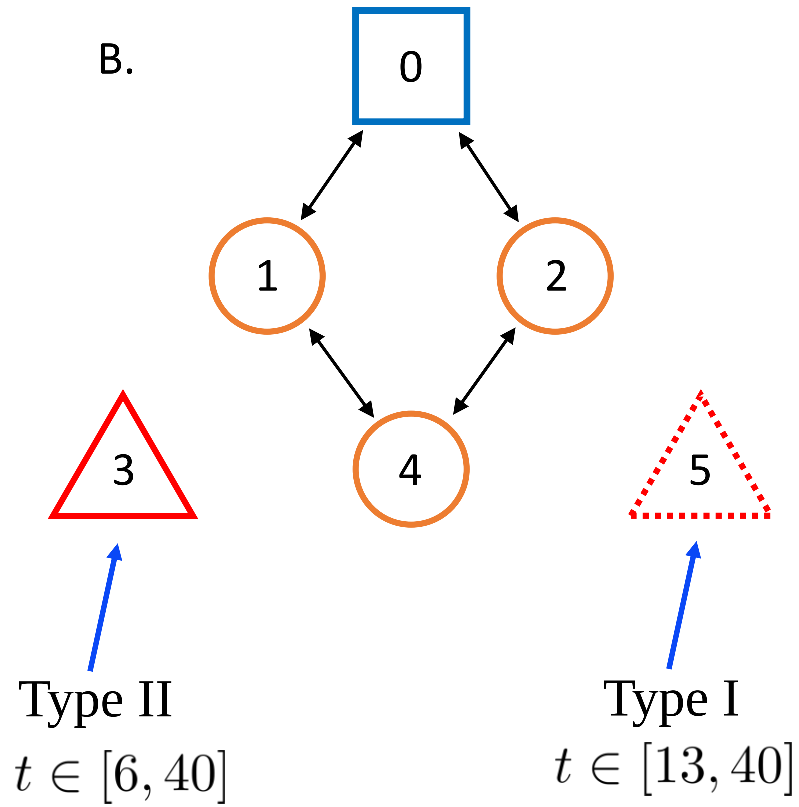
where $\beta_1, \ \beta_2, \ \beta_3 \in \mathbb{R}_{\geq 0}$ are known constants provided state feedback is available as dictated by the event-trigger, all assumptions are satisfied, and sufficient gain conditions are satisfied.

Simulation Results

Desired formation

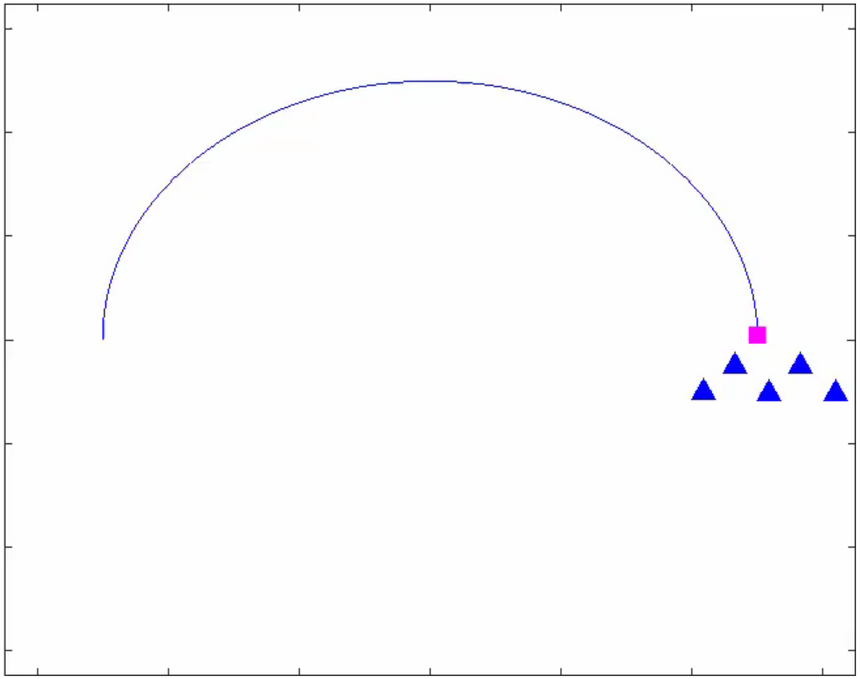
Compromised formation

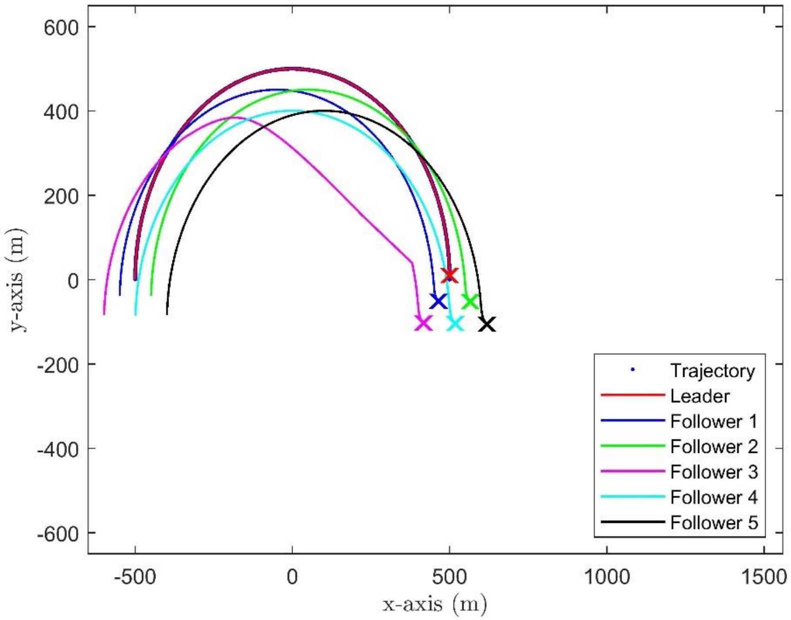




Simulation is 60 seconds long

Simulation Results





- Purple = leader
- Blue = cooperative follower
- Red = Byzantine follower