DATA-DRIVEN CYBERATTACK SYNTHESIS AGAINST NETWORK CONTROL SYSTEMS

IFAC 2023 YOKOHAMA

Thapliyal, Omanshu

Urban Air mobility Researcher,
Hitachi America Ltd.

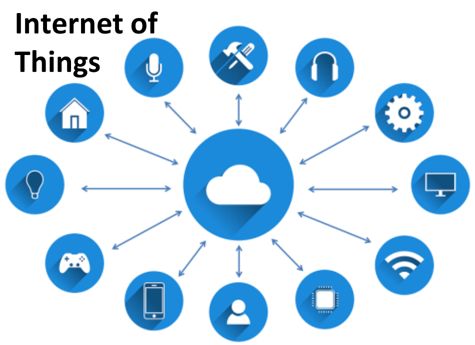
HITACHI
Inspire the Next

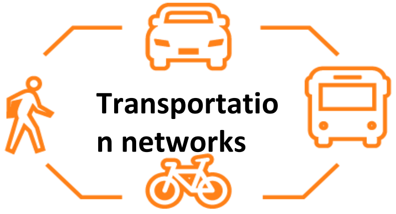
July 13th, 2023

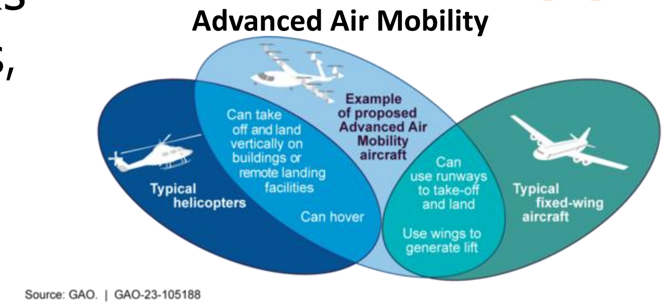
Introduction

- Network control systems allow control engineers to solve complex tasks, design sophisticated control schemes, and model cooperation of spatially separate entities, via data sharing across communication networks
  - → NCSs find applications in distributed control, power grids, multi-robot cooperation, etc.

- Increased reliance on communication → NCSs often communicate over insecure channels + susceptible to cybersecurity threats.
  - E.g., StuxNet, Capturing of RQ-170 recon a/c, cyber threats to autonomous driving







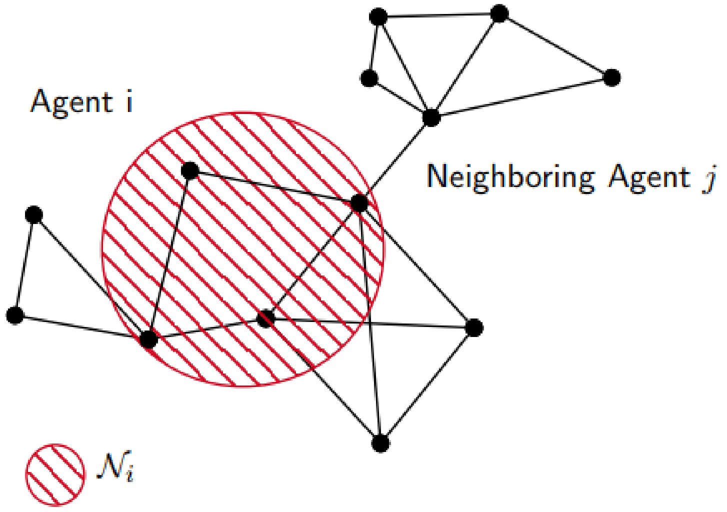
Motivation

- For dynamical systems with dedicated computational resources, a centralized reachability problem is limited only by the accuracy of the dynamical model
- Multi-Agent systems (MAS) are cheaper components in a bigger network of agents, internet-of-things network, or a system-of systems
- MASs have limited computational capabilities
- This is the most severe bottleneck in computing properties of an MAS in a distributed manner
- The sensed and communicated information from the neighborhood of an agent affects its own reachable sets in non-trivial ways

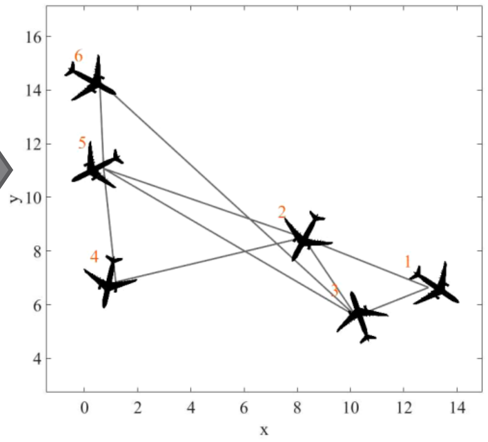
- Scope
- Smart attackers can eavesdrop to observe/measure NCS data → construct auxiliary NCS models + identify underlying communication graphs → perform realistic hybrid attacks (mixture of two different cyberattacks)

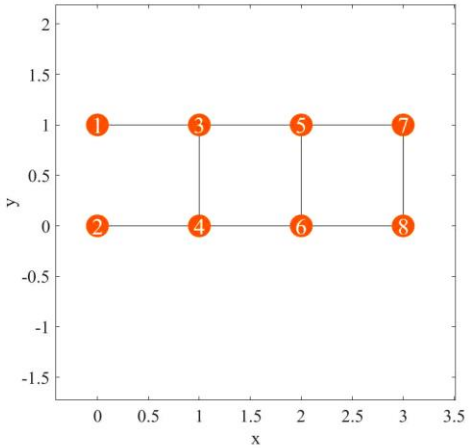
- Consider a network of agents whose states are coupled by a state feedback

$$\dot{x}_i(t) = A_i x_i(t) + B_i u_i(t),$$
$$u_i(t) = K_{ii} x_i(t) + \sum_{j \in \mathcal{N}_i(t)} K_{ij} \left(x_i(t) - x_j(t) \right)$$



- where the agents are connected according to some graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, with a graph adjacency Adj, and system matrices (A_i, B_i) for each agent i, with and control input u_i
  - ...but why such a control structure?
- Because it models many realistic NCS problems →





From the **Attacker's perspective**:

- A network of agents whose states are coupled by a state feedback control law (right):
  - where the attacker is observing states $\boldsymbol{x}(t)$ at some time instant (by eavesdropping, or state estimation)

$$\dot{\boldsymbol{x}}(t) \triangleq \mathbb{A}_{\mathcal{G}(t)}\boldsymbol{x}(t)$$
$$\boldsymbol{x}(t) \triangleq [x_1(t)^T, x_2(t)^T, \cdots, x_N(t)^T]^T$$
$$\mathbb{A}_{\mathcal{G}(t)} \triangleq \mathrm{diag}\{A_i + B_iK_{ii}\}_{i\in\mathcal{V}} + B_iK_{ij} \otimes \mathcal{L}_{\mathcal{G}(t)}$$

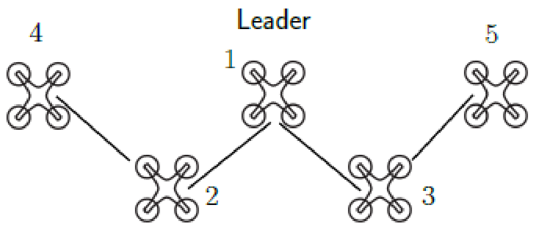
- The false data injection attack can be written as the attack synthesis problem (right)
  - where ρ is the attacker's budget, and the attacker is unaware of $\left\{A_i(t), B_i(t), \{K_{ij}\}_{(j\in\mathcal{N}_i(t))}\right\}_{i\in\mathcal{V}}$, but can collect the discrete-time trajectory data $\boxed{\{x_1(t), \cdots, x_N(t)\}_{t=t_0}^{t=t_1}}$ over time interval $[t_0, t_1]$

$$\begin{aligned} &\boxed{\text{find } \mathbb{B}^a, \boldsymbol{u}^a(t)} \\ &\text{such that } \dot{\boldsymbol{x}}(t) = \mathbb{A}_{\mathcal{G}(t)}\boldsymbol{x}(t) + \mathbb{B}^a\boldsymbol{u}^a(t), \\ &\boxed{\exists t^* \geq t_1} \text{ where } \boxed{\|x_i(t^*) - x_j(t^*)\|_2 \leq d^*}, \\ &\|\boldsymbol{u}^a(t)\|_2 \leq \rho \text{ for all } t \geq t_1 \end{aligned}$$

That is, … observe/eavesdrop for finite trajectory length, to perform FDI attack of budget ρ, to cause some 2 agents' states to 'collide', within some time t_1

False Data Injection Synthesis against a network of UAVs [formation flight]

- Consider a simple double integrator model of a network of 5 UAVs with state $[x, \dot{x}, y, \dot{y}]$ denoting the position and velocities in the 2D plane



- The UAVs intend to follow the leader, while adhering to a prescribed W-shaped formation for the NCS, with the leader determining the flock trajectory (right)

$$\dot{x}_i(t) = A_i x_i(t) + B_i u_i(t),$$

$$u_i(t) = K_{ii} x_i(t) + \sum_{j \in \mathcal{N}_i(t)} K_{ij} \left(x_i(t) - x_j(t) \right)$$

$$\dot{\boldsymbol{x}}(t) \triangleq \mathbb{A}_{\mathcal{G}(t)} \boldsymbol{x}(t)$$

$$A_i = \begin{bmatrix} 1 & \Delta t & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \Delta t \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad B_i = \begin{bmatrix} \Delta t^2/2 & 0 \\ \Delta t & 0 \\ 0 & \Delta t^2/2 \\ 0 & \Delta t \end{bmatrix}$$

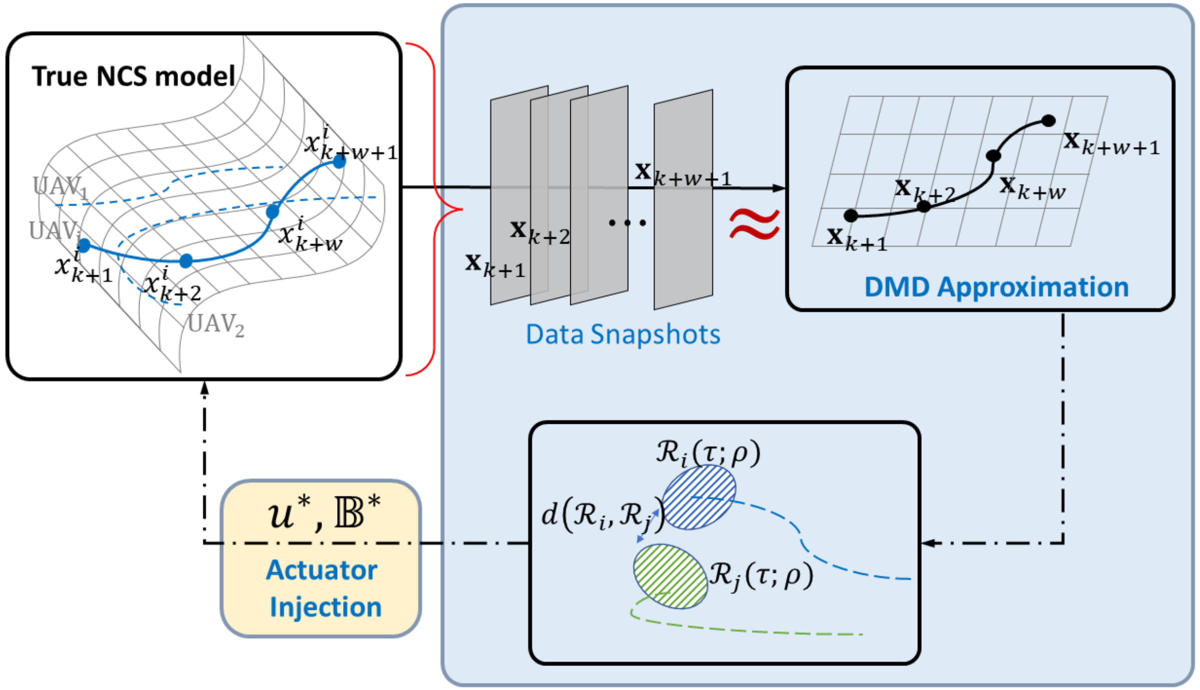
Reference trajectory

$$u_{1,k} = K_1 (x_{1,k} - x_k^\star) + \sum_{j \in \mathcal{N}_1} K_{1j} (x_{1,k} - x_{j,k} - x_{1j}^\star)$$

$$u_{i,k} = \sum_{j \in \mathcal{N}_i} K_{ij} (x_{i,k} - x_{j,k} - x_{ij}^\star), \; i = \{2 \cdots, 5\}$$

- If the trajectory data could be used to construct approximate models using DMD, the injection vehicles can be chosen according to pairs $i-j$ for which the **reach sets** $\mathcal{R}(t_1; t_0)$ are the closest:

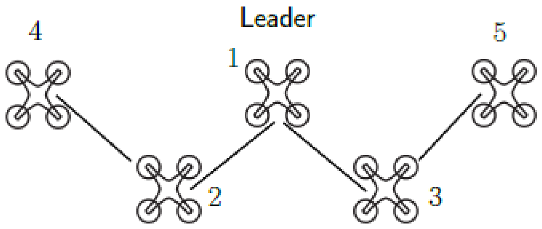
Solution Outline

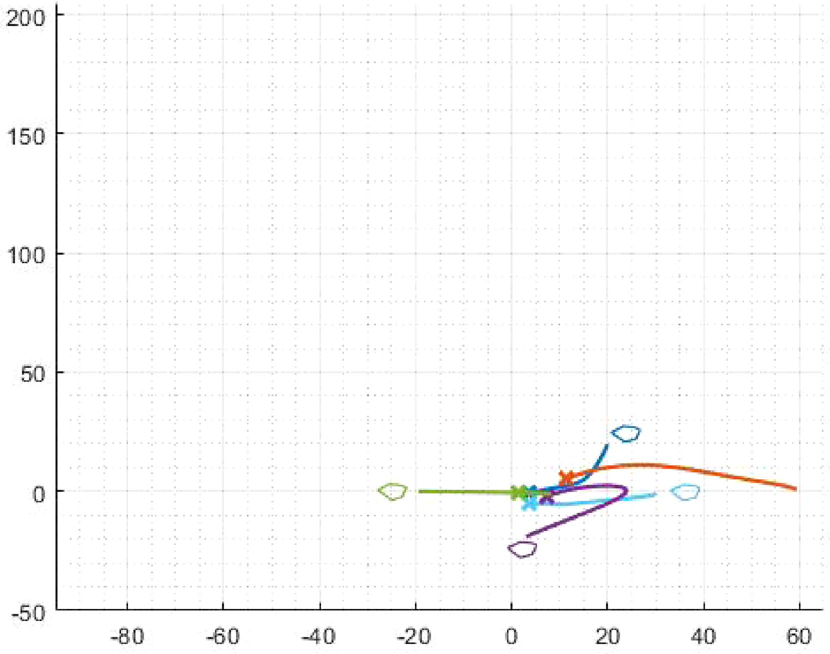


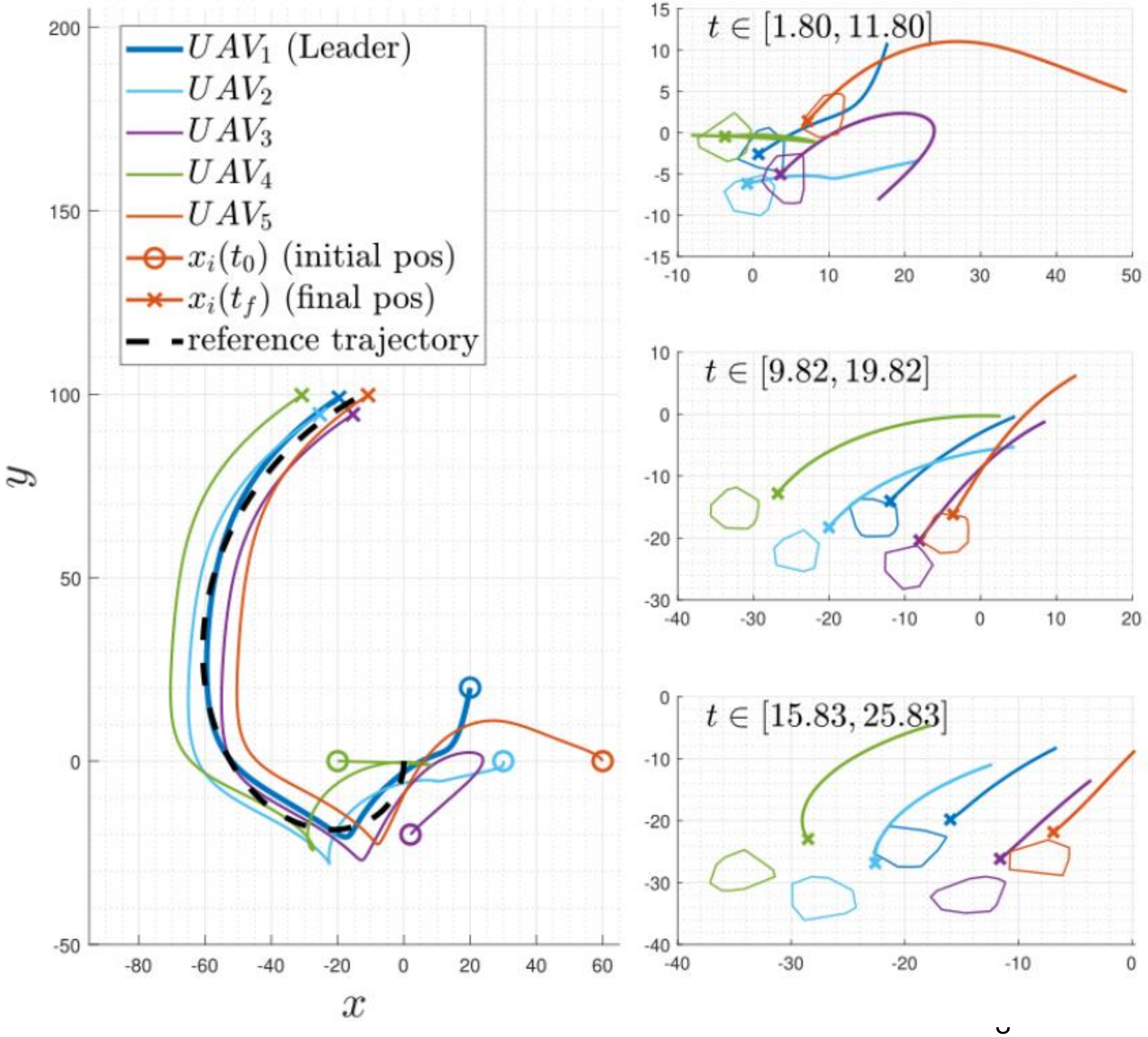
- That is, $(i^*, j^*) = \underset{i,j}{\arg\max}\, d\left(\mathcal{R}_i(\tau;\rho), \mathcal{R}_j(\tau;\rho)\right)$

$$\boldsymbol{u}^a = \arg\max d\left(\mathcal{R}_i(\tau+\Delta t;\rho), \mathcal{R}_j(\tau+\Delta t;\rho)\right)$$

- The resulting formation behaves as:







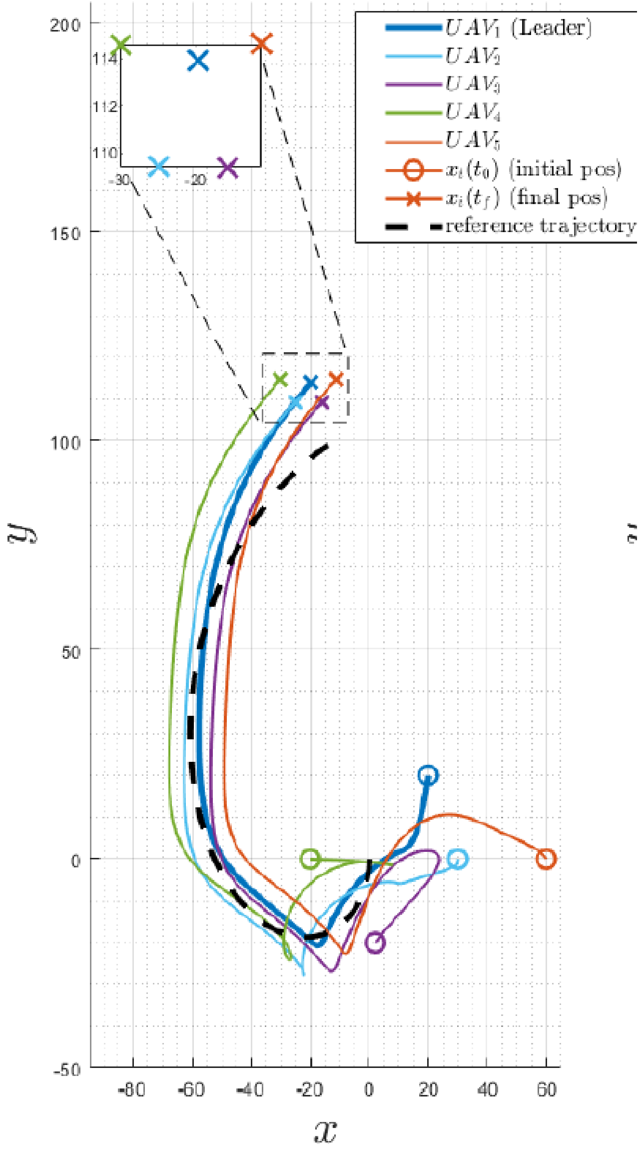
Case 1: Naïve FDI

Find vulnerable agent pair that can be deviated maximally:

$$(i^*, j^*) = \arg\max_{i,j} d\left(\mathcal{R}_i(\tau;\rho), \mathcal{R}_j(\tau;\rho)\right)$$

$$\boldsymbol{u}^a = \arg\max_{\|u\| \le 0.05} d\left(\mathcal{R}_i(\tau + \Delta t;\rho), \mathcal{R}_j(\tau + \Delta t;\rho)\right)$$

- The FDI results in:
  - UAVs no longer stick to the reference trajectory (→FDI has introduced a bias in reference tracking), but
  - 'W'-shaped formation still being preserved



Case 2: DoS + FDI

A smarter attacker can accompany the FDI of same budget with a preceding DoS attack (unsophisticated to carry out)

$$\hat{\mathcal{L}} = \arg\min_{L} \|K - (S + T \otimes L)\|_F \leftrightarrow \mathbb{A}_{\mathcal{G}(t)} \triangleq \text{diag}\{A_i + B_i K_{ii}\}_{i \in \mathcal{V}} + B_i K_{ij} \otimes \mathcal{L}_{\mathcal{G}(t)}$$

- DMD-based approximation of the NCS already computed by eavesdropping + snapshot data
- Underlying graph (Laplacian) $\mathcal{L}\_G$ can be approximated by finding the matrix $\mathcal{L}\hat{}$ that comes closest to the Laplacian

- Resulting matrix finding problem is:

$$\begin{aligned} &\min \gamma \\ &\text{subject to} \begin{bmatrix} \gamma I & K - (S + T \otimes L) \\ [K - (S + T \otimes L)]^T & \gamma I \end{bmatrix} \succ 0 \\ &L \succeq 0, L\mathbb{1} = 0 \end{aligned}$$

$\lambda_2(\hat{\mathcal{L}}) \rightarrow$ solves sparsest cut problem for $\mathcal{G} \rightarrow$ DoS-ing edge corresponding to λ_2 have maximal impact on graph connectivity

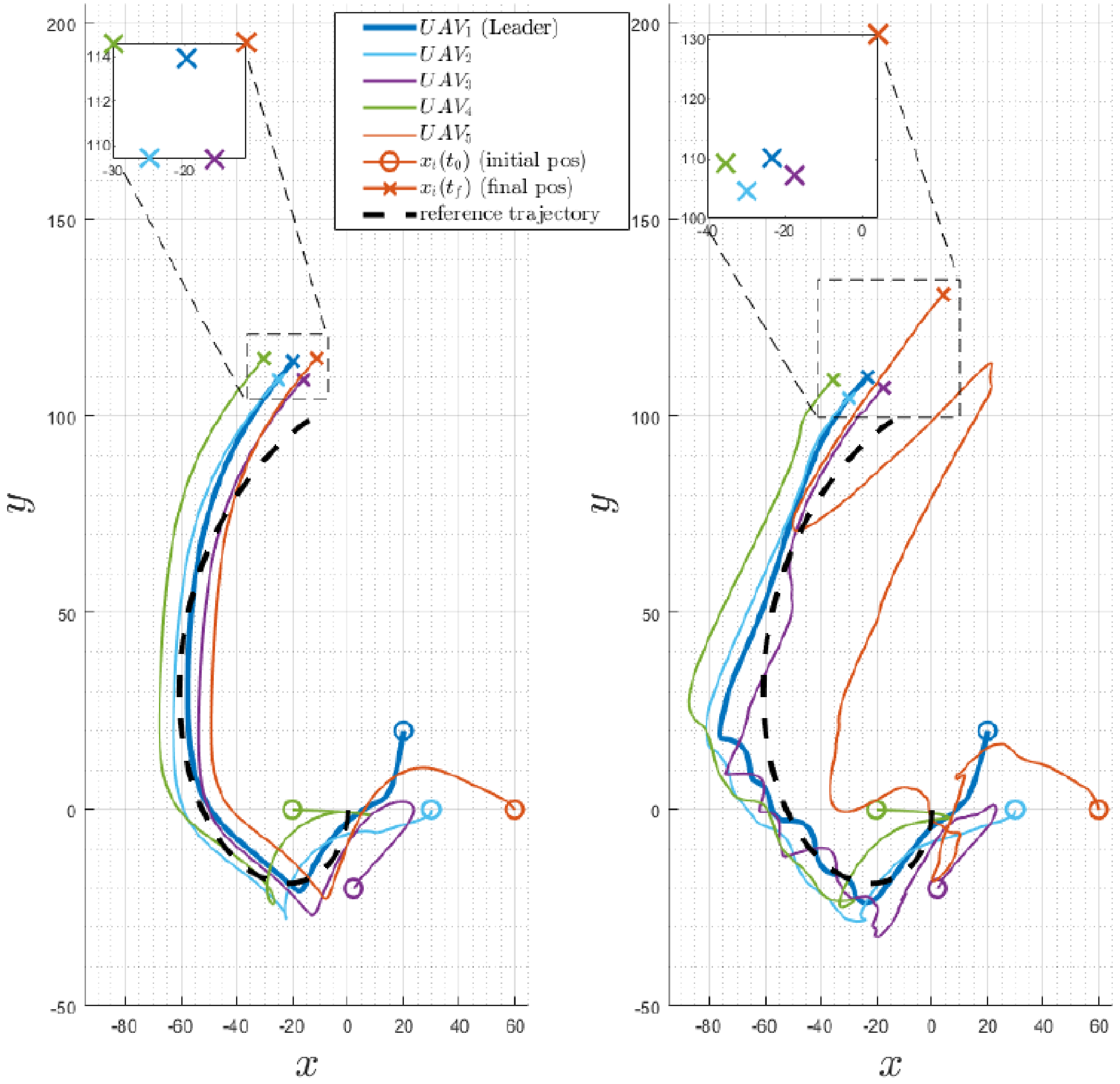
Compute $\lambda_2(\hat{\mathcal{L}}) \rightarrow$ vulnerable edge to DoS $\rightarrow$ FDI attack

Conclusion

Attacker can worsen performance very easily by preceding the FDI with a DoS attack

Not only is the reference trajectory following worsened, but UAV corresponding to $\lambda_2(\cdot)$ is unable to conform to the formation

- Eavesdropping for system trajectory can be utilized by attackers to perform auxiliary 'system models'
- FDI + DoS attacks can 'modify' the eigenvalues of stable NCS controllers on the auxiliary models
- The said technique was demonstrated in numerical simulation where unknown dynamical models of UAV formation flight were destabilized by attacker by:
    - System ID (Koopman linearization) combined with sequential semi-definite programming (DoS attack to precede more devastating FDI attack)
    - Combining relatively inexpensive attacks, the effects can be compounded and attacker has more adverse effect on unknown NCS dynamical models



Selected References

1. Fathian, Kaveh, Tyler H. Summers, and Nicholas R. Gans. "Distributed formation control and navigation of fixed-wing UAVs at constant altitude." 2018 International Conference on Unmanned Aircraft Systems (ICUAS). IEEE, 2018.

2. K. Fathian, T. H. Summers, N. R. Gans, "Robust Distributed Formation Control of Agents with Higher-Order Dynamics," IEEE Control Systems Letters, 2018

3. Uma, M. and Padmavathi, G., 2013. A Survey on Various Cyber Attacks and their Classification. *Int. J. Netw. Secur.*, *15*(5), pp.390-396.

4. Singh, S. and Silakari, S., 2009. A survey of cyber attack detection systems. *International Journal of Computer Science and Network Security*, *9*(5), pp.1-10.

5. Mauroy, A., Mezić, I. and Susuki, Y. eds., 2020. *The Koopman Operator in Systems and Control: Concepts, Methodologies, and Applications* (Vol. 484). Springer Nature.

6. Varaiya, P., 2000. Reach set computation using optimal control. In *Verification of Digital and Hybrid Systems* (pp. 323-331). Springer, Berlin, Heidelberg.

7. Hwang, I., Stipanović, D.M. and Tomlin, C.J., 2005. Polytopic approximations of reachable sets applied to linear dynamic games and a class of nonlinear systems. In *Advances in control, communication networks, and transportation systems* (pp. 3-19). Birkhäuser Boston.

8. Wang, P., Man, Z., Cao, Z., Zheng, J. and Zhao, Y., 2016, November. Dynamics modelling and linear control of quadcopter. In *2016 International Conference on Advanced Mechatronic Systems (ICAMechS)* (pp. 498-503). IEEE.

9. Kurzhanski, Alexander B., and Pravin Varaiya. "On ellipsoidal techniques for reachability analysis. Part I: external approximations." Optimization methods and software 17.2 (2002): 177-206.

Acknowledgments

The authors would like to acknowledge that this work was supported by NASA University Leadership Initiative (ULI) under Grant 80NSSC20M0161.

-Thank you

Q&A