Against Coordinated Cyber and Physical Attacks: Unified Theory and Technologies

Naira Hovakimyan[1], Lui Sha[2], Petros Voulgaris[3], and Xiaofeng Wang[4]

[1]Department of Mechanical Science and Engineering, [2]Department of Computer Science, [3]Department of Aerospace, University of Illinois at Urbana—Champaign
[4]College of Engineering and Computing, University of South Carolina

MOTIVATION

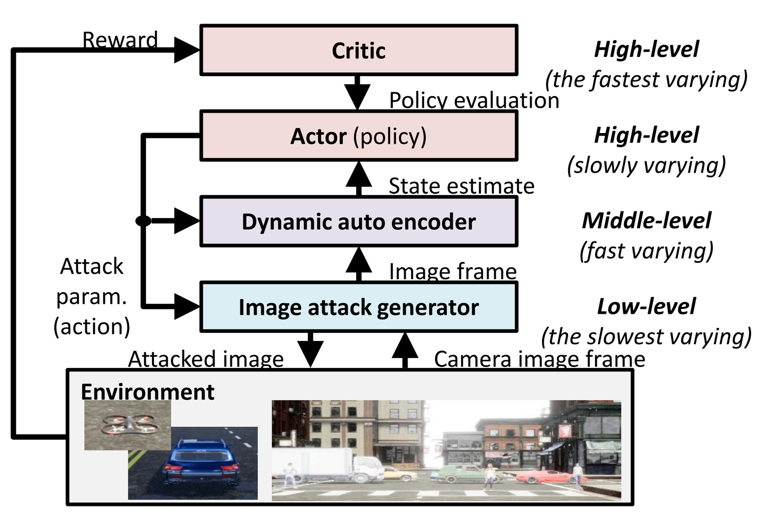
Challenge: Signal processing, robust fault-tolerant control (RFTC) theory and software assurance technologies: developed under different assumptions and models

- Software assurance technologies: model based, require no changes in the profile of the physical dynamics and observations
- RFTC techniques: compensate for the physical damage, assuming control software and sensor data are not compromised

Goal: Unified models and techniques *with coherent set of assumptions, supported by integrated technologies that can defend against Coordinated Cyber-Physical Attacks (CCPAs)*

Learning Image Attacks

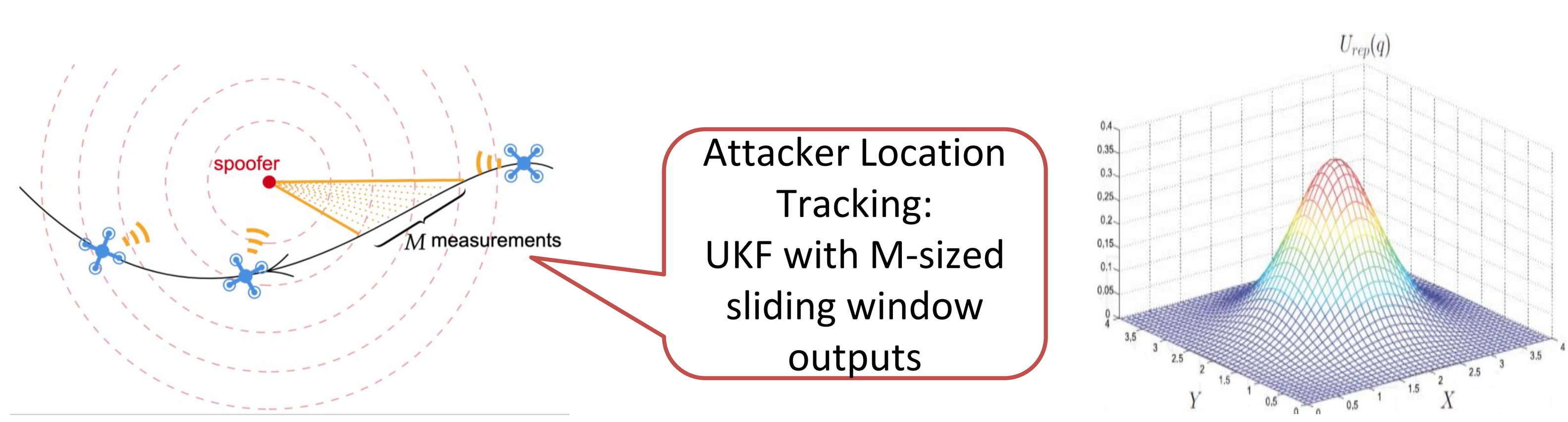
- Deep neural network perception module in autonomous vehicles are vulnerable to adversarial attack.
- Faster online recursive image attack with state estimator is needed for vision guided autonomous vehicles.



- Multi-level Framework -

Safety Constrained Control Framework

- To avoid intolerable sensor drifts for UAVs in GPS denied environment, the UAVs are desinged to adapt at the planning level.



$$\min_{u} \sum_{i=k}^{k+N} \hat{\tilde{x}}_{i+1}^{\top} Q_i \hat{\tilde{x}}_{i+1} + u_i^{\top} R_i u_i + \sum_{i=k^a+k^{esc}}^{k+N} U_{rep}(D_i)$$
$$\text{s.t. } \hat{x}_{i+1} = A\hat{x}_i + Bu_i$$
$$h(\hat{x}_i, u_i) \leq 0$$
$$\text{for } i = k, k+1, \cdots, k+N,$$

Time-delayed repulsive potential function

- Extension to the time-critical multi-agent systems:

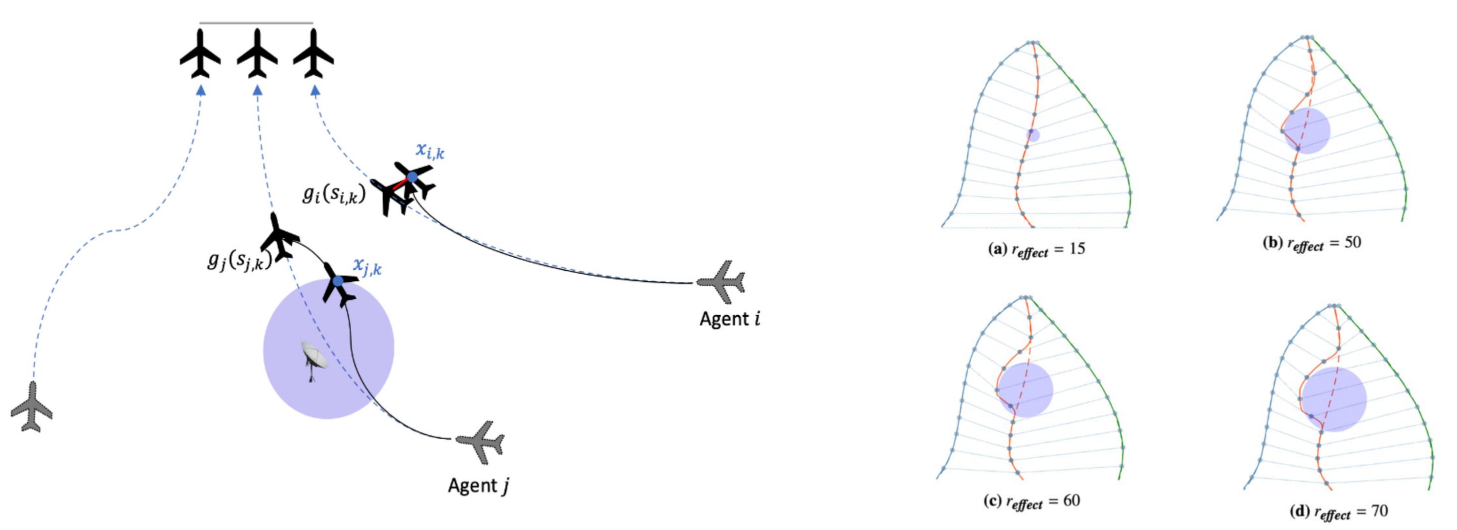
➢ Trajectory following: $g_i(s_{i,k}) - x_{i,k} \overset{k\to\infty}{\longrightarrow} 0; \quad s_{i,k+1} - s_{i,k} \overset{k\to\infty}{\longrightarrow} \rho$

➢ Time coordination: $s_{i,k} - s_{j,k} \overset{k\to\infty}{\longrightarrow} 0$

➢ Consensus model: $s_{i,k+1} = s_{i,k} + z_{i,k}$

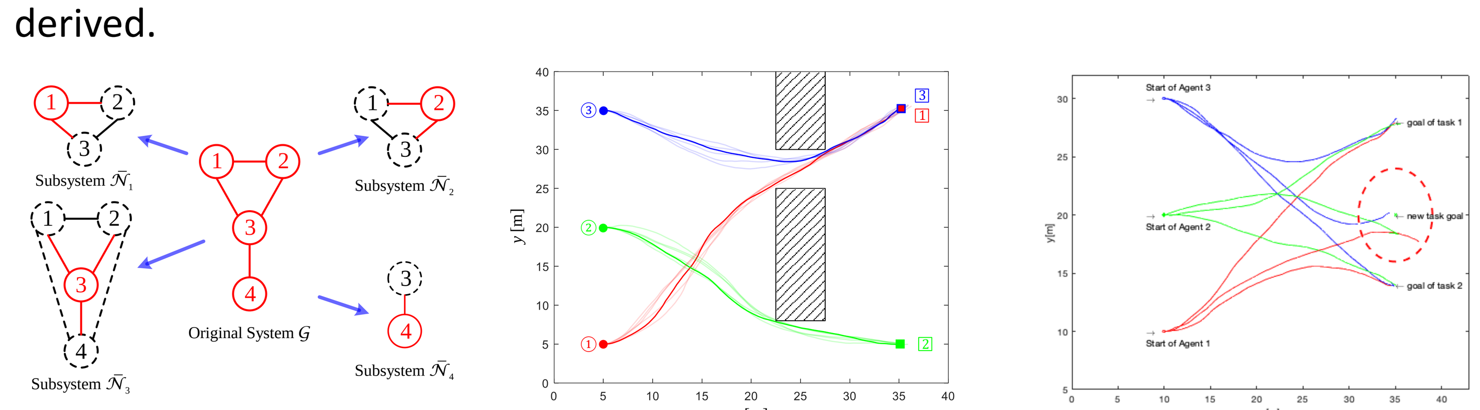
$$z_{i,k} = \max\left\{ -k_e\|g_i(s_{i,k}) - x_{i,k}\| - k_s \sum_{j\in\mathcal{N}(i)} (s_{i,k} - s_{j,k}) + \rho + \mathbf{1}_{\text{attacked}}\hat{z}_{i,k}, \quad 0\right\}$$

- Attack detection / State estimation with confidence / Escape away from the spoofer



Cooperative Control and Generalization

- Decentralized framework and learning algorithms are proposed for stochastic multi-agent systems with moderate requirements on computation and communication.
- Generalization algorithms that immediately generate cooperative control law for unlearned tasks from previously learned control tasks using compositionality is derived.

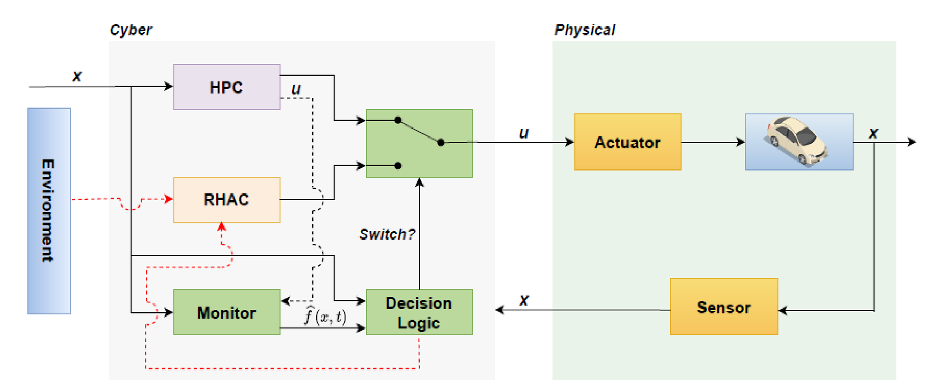


Finite-Time Model-Learning Based $\mathcal{L}1$-Simplex

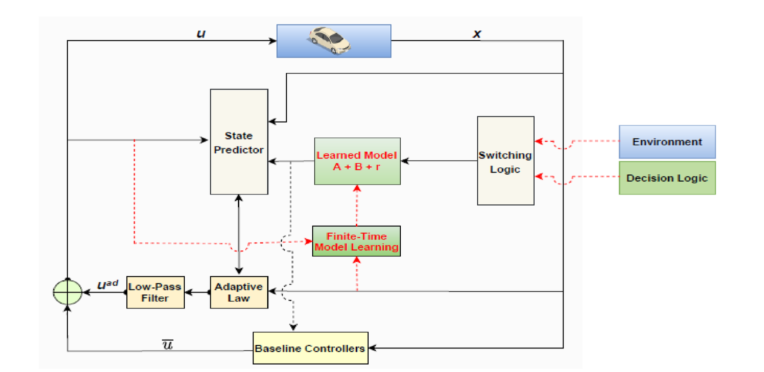
- The fundamental assumption of model-based controllers is the availability of a good model of the underlying dynamics in consideration. The large model mismatch induced operational environment therefore poses a formidable threat to the reliability of control systems, especially in the time-critical and safety-critical environments.
- Main idea:

➢ Incorporate finite-time model learning into $\mathcal{L}1$-Simplex to update the system model when any deviation from the safety envelope occurs.

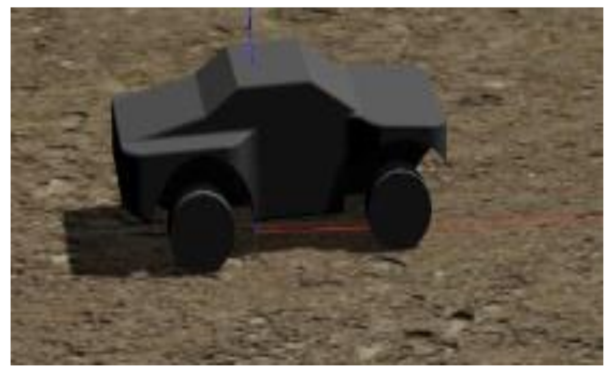
➢ Leverage sample-complexity bounds to achieve fast and reliable model learning.



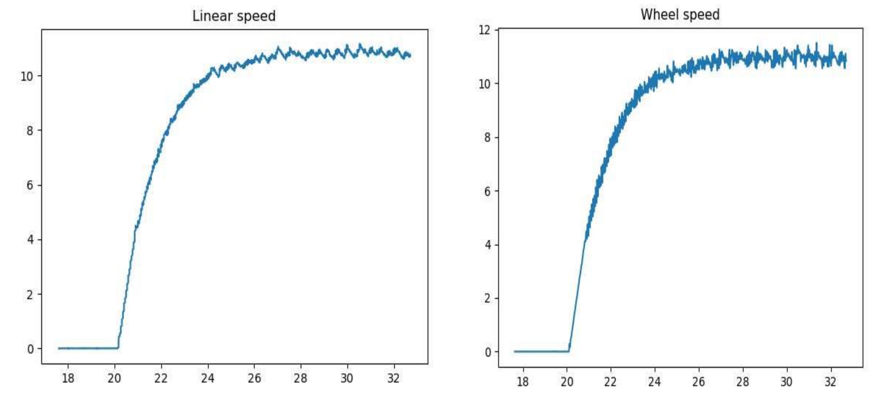
$\mathcal{L}1$-Simplex architecture



Model-learning based RHAC



AutoRally: unforeseen driving environment



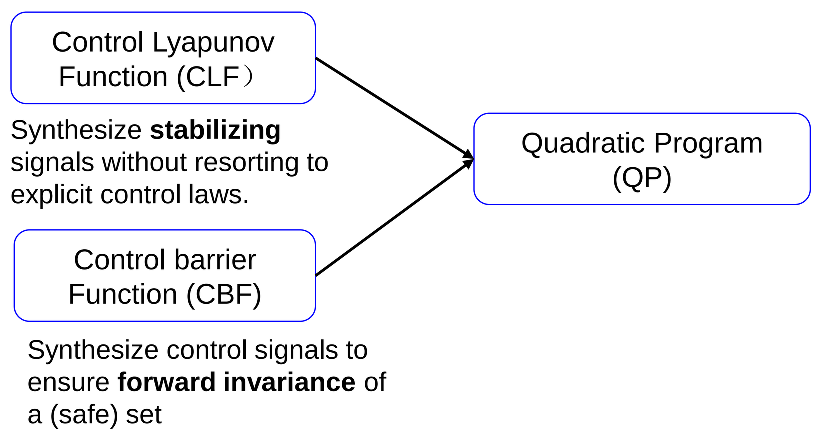
Safe velocity regulation

Adaptive Robust Quadratic Programs

- QP performance and/or safety guarantee will be compromised in the presence of model uncertainties and disturbances.
- Growth rate of the uncertainty is bounded with prior known constants, such that the uncertainty with computable error bounds can be estimated.
- Adaptive robust QP: handle both state-dependent uncertainties and disturbances, and guarantee satisfaction of safety-related CBF conditions:

➢ Estimate the pointwise value of the uncertainty with computable error bounds.

➢ Formulate a robust QP using the estimated uncertainty and the error bounds.



$$u^{\star}(t,x) = \underset{(u,\delta)\in\mathbb{R}^{m+1}}{\arg\min} \frac{1}{2}u^T H(x)u + p\delta^2 \quad \text{(aR-QP)}$$
$$\text{s.t. } L_f V(x) + L_g V(x)u + V_x(x)\hat{d}(t) + \|V_x(x)\|\,\gamma(T) + \alpha(V(x)) < \delta, \quad \text{(R-CLF)}$$
$$L_f h(x) + L_g h(x)u + h_x(x)\hat{d}(t) - \|h_x(x)\|\,\gamma(T) + \beta(h(x)) > 0, \quad \text{(R-CBF)}$$
$$u \in U.$$

REFERENCES

- H. Yoon, and P. Voulgaris. "Learning Image Attacks toward Vision Guided Autonomous Vehicles." submitted to International Conference on Machine Learning, 2021.
- A. Lakshmanan, A. Gahlawat, and N. Hovakimyan. "Safe Feedback Motion Planning: A Contraction Theory and $\mathcal{L}1$-Adaptive Control Based Approach," In 59th IEEE Conference on Decision and Control, pp. 1578-1583, Jeju Island, Republic of Korea, 2020.
- W. Wan, H. Kim, N. Hovakimyan, L. Sha, and P. Voulgaris, "A Safety Constrained Control Framework for UAVs in GPS Denied Environment," In 59th IEEE Conference on Decision and Control, pp. 214-219, Jeju Island, Republic of Korea, 2020.
- W. Wan, H. Kim, Y. Cheng, N. Hovakimyan, P. Voulgaris, and L. Sha, "Safety Constrained Multi-UAV Time Coordination: A Bi-level Control Framework in GPS Denied Environment," to appear in AIAA AVIATION, 2021.
- N. Wan, A. Gahlawat, N. Hovakimyan, E. A. Theodorou, and P. G. Voulgaris, "Cooperative Path Integral Control for Stochastic Multi-Agent Systems," in Proceedings of the American Control Conference, New Orleans, LA, 2021.
- L. Song, N. Wan, A. Gahlawat, N. Hovakimyan, and E. A. Theodorou, "Compositionality of Linearly Solvable Optimal Control in Networked Multi-Agent Systems," in Proceedings of the American Control Conference, New Orleans, LA, 2021.
- Y. Mao, Y. Gu, N. Hovakimyan, P. Voulgaris, and L. Sha, "Finite-Time Model-Learning Based L1-Simplex for Integrated TCS and ABS," in preparation for IEEE Transactions on Vehicular Technology.
- Y. Mao, N. Hovakimyan, P. Voulgaris, and L. Sha, "Finite-Time Model Inference from A Single Noisy Trajectory," submitted to IEEE Transactions on Automatic Control.
- P. Zhao, Y. Mao, C. Tao, N. Hovakimyan, and X. Wang, "Adaptive Robust Quadratic Programs using Control Lyapunov and Barrier Functions". In 59th IEEE Conference on Decision and Control, pp. 3353-3358, Jeju Island, Republic of Korea, 2020.

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting
June 2-4, 2021

Award ID#: ECCS-1739732, ECCS-1739886