CPS Synergy: Collaborative Research: Formal Design of Semi-autonomous Cyber Physical Transportation Systems

Massachusetts Institute of Technology

UMTRI UNIVERSITY OF MICHIGAN TRANSPORTATION RESEARCH INSTITUTE

PI: Domitilla Del Vecchio (MIT)

co-PIs: Paul Green (UMTRI), Emilio Frazzoli (MIT)

NSF Award Number: 1239182

Abstract

The goal of this project is to develop fundamental theory, computationally efficient algorithms, and real-world experiments for the analysis and design of **safety-critical cyber-physical systems with human operators**. To this end, we propose a modeling, theoretical, and experimental collaborative effort combining human factors, control theory, and computer science.

As crashes at traffic intersections account for about 40% of overall vehicle crashes, we will focus on intersection crashes in this project. **Specifically, our grand-challenge application is to design provably safe driver-assist systems that understand driver's intentions and provide warnings/overrides to prevent collisions at traffic intersections.** With this focus, we propose to construct, from four human factors experiments hybrid automata models for the driver-vehicles-intersection system, which incorporate driver behavior and performance as an integral part. Due to the probabilistic nature of driver behavior, we propose to construct a partial order of these hybrid automata models, ordered according to confidence levels on the model parameters. These hybrid models will have imperfect state information because of uncontrollable and unobservable driver's decisions, sensor noise, and communication limitations. We propose to formulate the driver-assist design problem as a set of *partially ordered hybrid differential games* with imperfect information, in which games are ordered to parameters confidence levels. This novel approach to address safety specifications allows to formally establish a tradeoff between conservatism of the design and safety confidence. This is especially crucial for driver assist systems, in which the frequency of warnings and overrides should be carefully tuned based on driver's expectations, government regulations, and industrial and international safety standards. We propose to validate our designs experimentally in the UMTRI driving simulator and in large-scale computer simulations leveraging the software developed by the SimMobility project at MIT.

Project Overview

Challenge Application: Transportation Systems

New theory, analysis and design of safe CPS with imperfect information
Research Target Area 2:
Technology of Cyber-Physical Systems
Del Vecchio/Frazzoli (at MIT)

Disciplines: Dynamics and Control, Computer Science, Human Factors

Models of CPS with humans-in-the-loop
Research Target Area 1:
Science of Cyber-Physical Systems
Del Vecchio/Green (at MIT/UMTRI)

Human factor analysis
Experimental demonstrations
Green/Del Vecchio (at UMTRI)

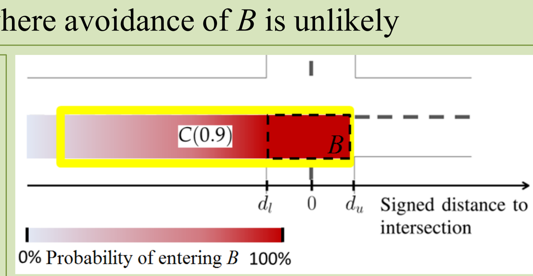
Safety supervisor for stochastic multi-modal systems

(Daniel Hoehener, Paul Green, and Domitilla Del Vecchio)

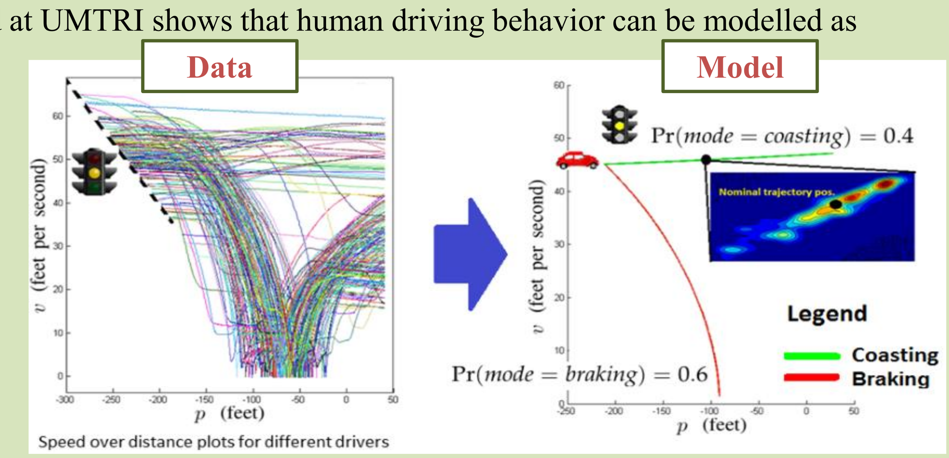
Problem: Design a **semi-autonomous** driver-assist system that
- keeps state away from an unsafe region B with given probability P
- overrides driver only when necessary

Approach: We use the **stochastic capture set** *C(P)*, i.e. the set of states where avoidance of B is unlikely

Objectives:
1. Use probability theory to **quantify the conservatism** of the driver-assist system
2. Design an algorithm that handles the interaction between human and controller such that
   - the overall system is **provably safe** (avoids the unsafe region)
   - design is independent of the particular control strategy (**modularity**)
3. Ultimately reduce number of intersection crashes



Background and model:
- Analysis of the driving simulator data gathered at UMTRI shows that human driving behavior can be modelled as **stochastic hybrid systems**
- Key properties of the hybrid system driver model:
  - System state is composed into:
    i. Mode (driver intention) $\mathbf{q} \in Q$, where Q is a finite set
    ii. State (physical state of vehicle) $\mathbf{x}(t) \in \mathbb{R}^n \quad \forall t \in \mathbb{R}_+$
  - State is observed, **mode is unobserved**
  - The mode is a random variable with known distribution and the state satisfies the **mode-dependent** SDE: $d\mathbf{x}(t) = (A(\mathbf{q})\mathbf{x}(t) + b(\mathbf{q})\mathbf{u}(t))dt + \sigma(\mathbf{q})dW(t)$



Formal definition of capture set:

Difficulty: System dynamics depend crucially on unobserved mode

Solution: Reformulate the problem in the **information state**
- **Available information** at time t is $\mathcal{F}_t^x := \sigma\{\mathbf{x}(s) | 0 \le s \le t\}$
- Best estimate of mode q_i is given by $\pi_i(t) := \mathbb{E}(\mathbf{1}_{q_i}(\mathbf{q})|\mathcal{F}_t^x)$
- Write $\pi(t)=(\pi_1(t),\dots,\pi_r(t))$, where $r=|Q|$
- Consider as new state in information space $(\pi, \mathbf{x})$

Control dependent capture set:

$$C_{\mathbf{u}}(P) := \{(\pi_0, x_0) | Pr(\exists t, \mathbf{x}_t^{\pi_0, x_0, \mathbf{u}}) \in B) > 1 - P\}$$

where $\mathbf{u}$ is an $\mathcal{F}_t^x$–measurable input and $\mathbf{x}_t^{\pi_0,x_0,\mathbf{u}}$ is the **unique** solution of

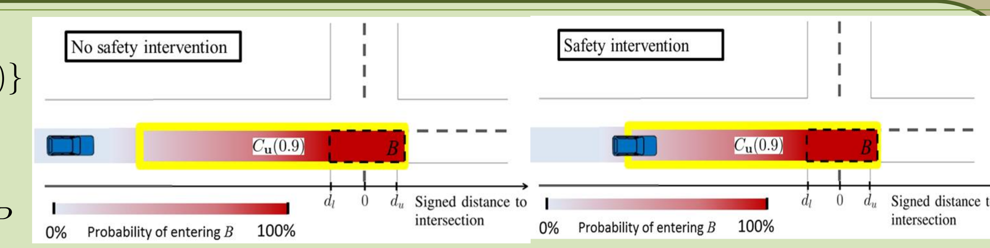
$$\begin{cases} d\mathbf{x}(t) = A(\tilde{\mathbf{q}})\mathbf{x}(t)dt + B(\tilde{\mathbf{q}})\mathbf{u}(t)dt + \sigma(\tilde{\mathbf{q}})dW_t \\ \mathbf{x}(0) = x_0, \quad \tilde{\mathbf{q}} \ \pi_0 \end{cases}$$

Main result:

Let $\tau_{\mathbf{u}} := \inf\{t \in \mathbb{R}_+ | (\pi(t), \mathbf{x}(t)) \in C_{\mathbf{u}}(P)\}$

and define $\tilde{\mathbf{u}}(t) := \begin{cases} U & \text{if } t < \tau_{\mathbf{u}} \\ \mathbf{u}(t) & \text{if } t \ge \tau_{\mathbf{u}} \end{cases}$

then $\Pr(\exists t \in \mathbb{R}_+, \mathbf{x}_t^{\pi(0),\mathbf{x}(0),\tilde{\mathbf{u}}} \in B) < 1 - P$



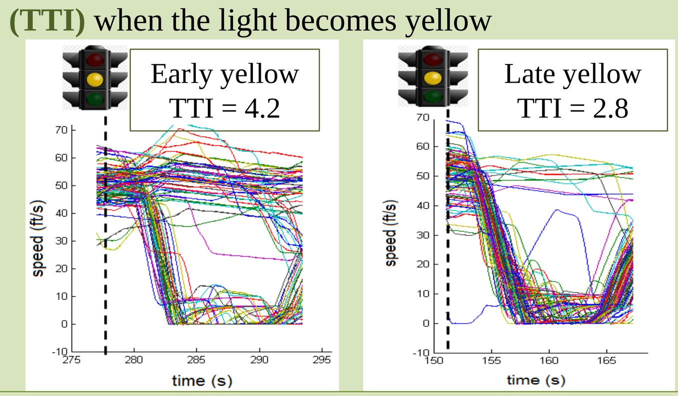
Analysis of driver reactions to warnings near signaled intersections

(Jasmine Chan, Elaine Kwan, Daniel Hoehener, Paul Green, and Domitilla Del Vecchio)

Driving simulator experiments:
- **Two experiments** conducted at UMTRI:
  - 24 subjects (12 male, 12 female) per experiment
  - 140 intersections equipped with traffic lights per subject
  - **3 types of yellow light intersections** (early, middle, late) based on time to intersection
  - **Visual and audible warnings**
- Experiment 1: Baseline experiment without warnings
- Experiment 2: Warnings given when collisions are imminent

Analysis of driving behavior:

1. Percentage of drivers stopping with yellow is positively correlated with the time to intersection (TTI) when the light becomes yellow

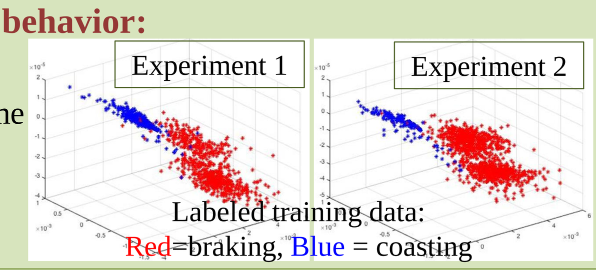


2. Warnings increase the percentage of drivers braking at the yellow light

Percentage of drivers braking		
	Baseline Experiment	Experiment with warnings
Early Yellow	89%	97%
Middle Yellow	75%	90%
Late Yellow	49%	70%

3. Warnings decrease the average reaction time (to the yellow light) of drivers: The same subject starts braking on average 0.32s faster if there is a warning

Classification of driving behavior:
- Supervised approach
- Parametrization of the time series data with a regularized least-squares method



Labeled training data:
Red=braking, Blue = coasting

- 5-Nearest neighbor classification of the parameterized data leads to accurate results:

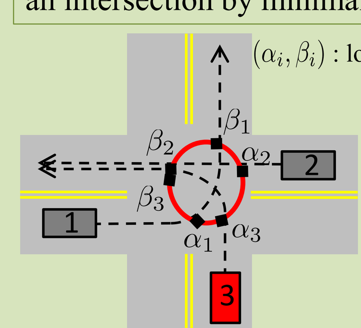
Confusion Matrix		
	Classified Coasting	Classified Braking
Coasting	94%	6%
Braking	1%	99%

A multi-vehicle supervisor for intersection collision avoidance

(Heejin Ahn and Domitilla Del Vecchio)

Problem: How can a supervisor prevent collisions at an intersection by minimally overriding vehicles?

Objectives: The supervisor must guarantee
Safety: all vehicles crossing the intersection without conflict
Least restrictiveness: not fully autonomous



(α_i, β_i) : location of an intersection for vehicle i

■ : communicating vehicles
■ : not communicating vehicles

- Vehicles follow predetermined paths
- There is one vehicle per road

1. An intersection is modeled as one conflict area → single machine scheduling

Dynamic model: $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \mathbf{u}) \quad \mathbf{y} = \mathbf{h}(\mathbf{x})$
where $\mathbf{x}$ state, $\mathbf{u}$ input, $\mathbf{y}$ position

Collision occurs if $\mathbf{y} \in B$ where
$B := \{\mathbf{y} : y_j \in (\alpha_j, \beta_j) \text{ and } y_{j'} \in (\alpha_{j'}, \beta_{j'})\}$

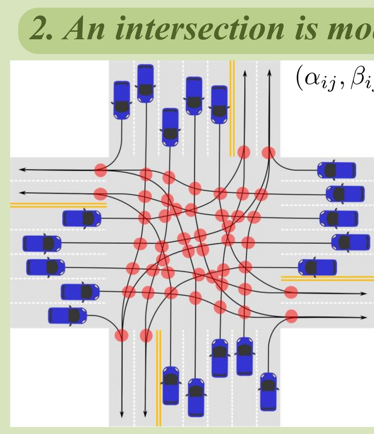
Schematic of the supervisor: Given $\mathbf{x}(0)$, the supervisor override the vehicles only when if there is no $\mathbf{u}$ such that $\mathbf{y}(t, \mathbf{u}, \mathbf{x}(0)) \notin B$.

Experimental testing:
3 RC cars:

2 communicating cars and 1 not communicating car driven by a random user, Blue boxes: the time when the supervisor overrides the communicating cars

2. An intersection is modeled as multiple conflict area → multi-machine scheduling

Dynamic model: $\dot{\mathbf{y}} = \mathbf{u}$
$\mathbf{y}$ position, $\mathbf{u}$ input (speed)



$(\alpha_{ij}, \beta_{ij})$: location of conflict area i on the longitudinal path of vehicle j

Collision occurs if $\mathbf{y} \in B$ where
$B := \{\mathbf{y} : y_j \in (\alpha_{ij}, \beta_{ij}) \text{ and } y_{j'} \in (\alpha_{ij'}, \beta_{ij'})\}$

Theorem:
The following three are equivalent.

1. Given $\mathbf{y}(0)$, determine if there exists $\mathbf{u}$ such that $\mathbf{y}(t,\mathbf{u},\mathbf{y}(0)) \in B$.
2. Given $\mathbf{y}(0)$, determine if there exists $\mathbf{T} := \{T_{ij} \in \mathbb{R} : y_j(T_{ij}, u_j, y_j(0)) = \alpha_{ij} \text{ for some } u_j\}$ such that

$\boxed{R_{ij}} \le T_{ij} \le \boxed{D_{ij}}$ $\qquad T_{ij} \le T_{ij'} \Rightarrow \boxed{P_{ij}} \le T_{ij'}$

Release time soonest time for vehicle j to enter conflict area i
Deadline latest time for vehicle j to enter conflict area i
Process time soonest time for vehicle j to exit conflict area i

* If vehicle j crosses conflict area i' and then conflict area i, R_{ij} and D_{ij} are functions of $T_{i'j}$
* If vehicle j crosses conflict area i and then conflict area i', P_{ij} is a function of T_{ij} and $T_{i'j}$

3. Given $\mathbf{y}(0)$, there exists **T, p, k** such that $\mathbf{T} := \{T_{ij} \in \mathbb{R} : y_j(T_{ij}, u_j, y_j(0)) = \alpha_{ij} \text{ for some } u_j\}$
$\mathbf{p} := \{p_{ij} \in \mathbb{R} : y_j(p_{ij}, u_j, \alpha_{ij}) = \beta_{ij} \text{ for some } u_j\}$

$$k_{ijj'} = \begin{cases} 1 & \text{if vehicle } j \text{ precedes } j' \\ 0 & \text{otherwise} \end{cases}$$

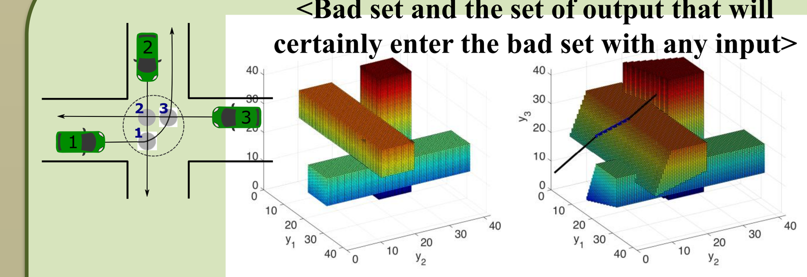
$$\frac{\alpha_{ij} - y_j(0)}{u_{j,max}} \le T_{ij} \le \frac{\alpha_{ij} - y_j(0)}{u_{j,min}} \qquad \frac{\beta_{ij} - \alpha_{ij}}{u_{j,max}} \le p_{ij} \le \frac{\beta_{ij} - \alpha_{ij}}{u_{j,min}}$$

$$T_{i'j} + p_{i'j} + \frac{\alpha_{ij} - \beta_{i'j}}{u_{j,max}} \le T_{ij} \le T_{i'j} + p_{i'j} + \frac{\alpha_{ij} - \beta_{i'j}}{u_{j,min}}$$

$$T_{ij} + p_{ij} \le T_{i'j} + M(1 - k_{ijj'})$$
$$T_{i'j} + p_{i'j} \le T_{ij} + M(1 - k_{ij'j})$$
$$k_{ijj'} + k_{ij'j} = 1 \qquad M \text{ sufficiently large}$$

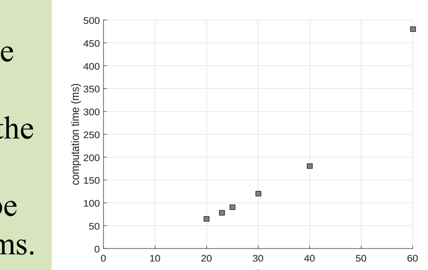
Mixed-Integer Linear Programming (MILP)

Simulation Results:



<Computation time with respect to the number of vehicles>

- Computation time is the time required for one iteration of the supervisor algorithm in the worst case.
- More than 20 vehicles can be handled in the allotted 100 ms.

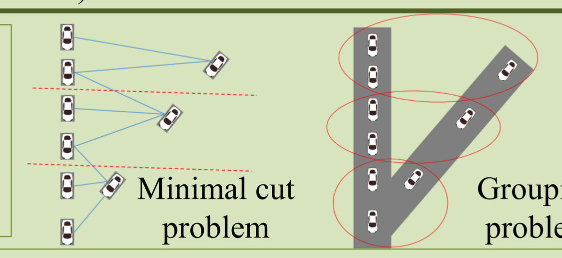


A distributed and scalable least restrictive supervisor

(Bomin Jiang and Domitilla Del Vecchio)

Problem: how to design a least restrictive safety supervisor that can do the computation in a distributed manner? How to make the supervisor design practical for huge number (probably infinite number) of vehicles?

Objectives:
- Safety
- Least restrictive
- Distributed
- Scalable



Approach: the intersection verification problem is NP hard. In order to be distributed and scalable, one can put them into groups. The **grouping problem** is equivalent with a graph **minimal cut problem**.
- Grouping → Solve each local problem → Synthesis to obtain the solution to the original problem
- Trade off between computing time and conservatism: A bound of conservatism is obtainable.

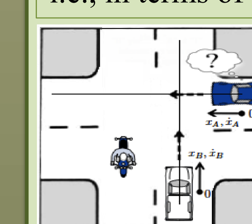
Intention Inference and Input-state Estimation of Semi-autonomous Vehicles

(Sze Zheng Yong, Minghui Zhu, and Emilio Frazzoli)

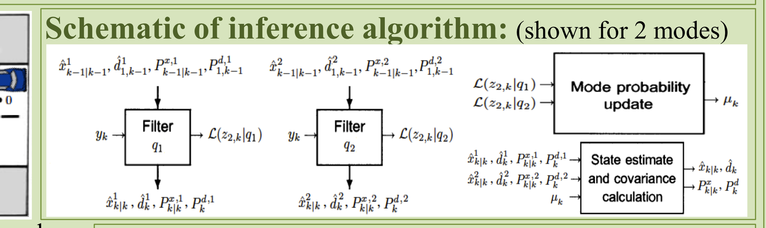
Problem: Asymptotic analysis of mode, state and unknown input estimation algorithm

Approach: 1. Static multiple-model approach with one optimal input and state filter for each mode 2. Exploit whiteness of generalized innovation to form likelihood function 3.Use likelihood function to determine the most probable mode, and thus input and state estimates

Results: 1. Generalized innovation is a Gaussian white noise 2. Asymptotic properties of the estimation algorithm (mean consistency and convergence) depend on closeness in an information-theoretic sense, i.e., in terms of the minimum Kullback-Leibler (KL) divergence.



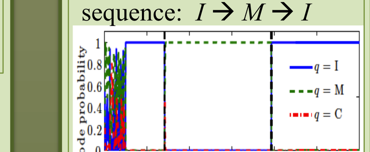
Schematic of inference algorithm: (shown for 2 modes)



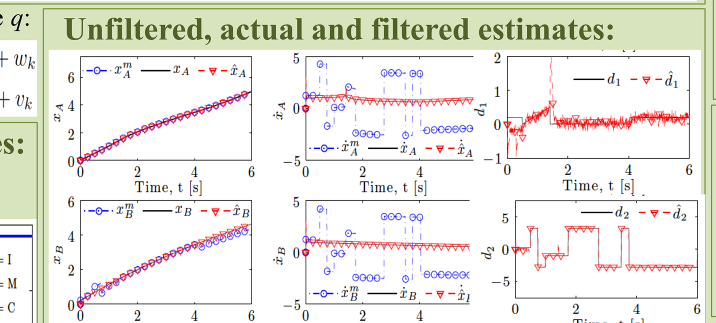
Dynamics for each mode q:

$$x_{k+1} = A_k x_k + B_k u_k + G_k d_k + w_k$$
$$y_k = C_k x_k + D_k u_k + H_k d_k + v_k$$

Mode probabilities:
True mode (intention) sequence: $I \to M \to I$



Unfiltered, actual and filtered estimates:



d_1: Input of vehicle A $\quad d_2$: Measurement bias

Problem: Optimal state and unknown input estimation for broader classes of systems

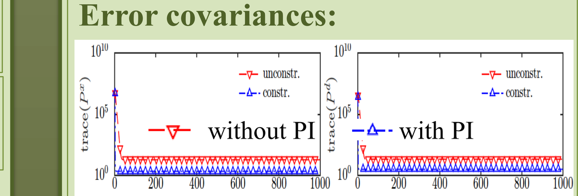
Extension #1: Input and state filtering with partial input information: Aggregate information about inputs as given linear equality or inequality constraints, e.g., conservation laws and lower and upper bounds
Results: Using a projection approach, input information reduces trace of estimation error covariance

Extension #2: Input and state filtering for linear continuous-time systems with unknown inputs
Results:
- Additional "output derivative" information or assumptions on system necessary
- Developed corresponding optimal filters
- Separation of control and estimation

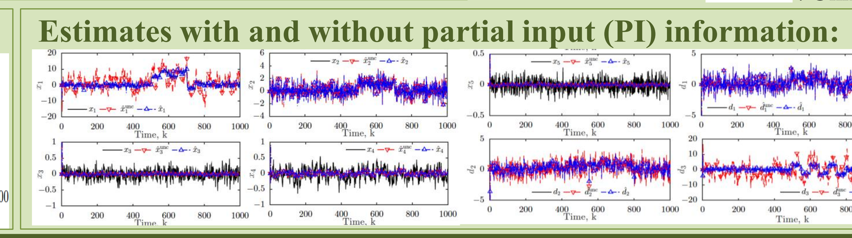
Extension #3: Input and state filtering with a fixed delay (not in "real-time")
Results: • Weaker assumptions: Strong detectability is the key system property • Developed optimal filters with delays

x_1, x_2, x_3, x_4, x_5 : States of a benchmark system
d_1, d_2, d_3 : Unknown inputs/faults

Error covariances:



Estimates with and without partial input (PI) information:



Products

- D. Hoehener, P.A. Green, and D.Del Vecchio. Stochastic Hybrid Models for Predicting the Behavior of Drivers Facing the Yellow-Light-Dilemma, *Proc. American Control Conference*, 2015.
- H. Ahn, A. Rizzi, A. Colombo, and D. Del Vecchio. Experimental Testing of a Semi-autonomous Multi-vehicle Collision Avoidance Algorithm at an Intersection Testbed, *Proc. IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2015.
- H. Ahn and D. Del Vecchio. Semi-autonomous Intersection Collision Avoidance through Job-shop Scheduling, *Summited to 19th ACM International Conference on Hybrid Systems: Computation and Control,* 2016. Available from: http://arxiv.org/abs/1510.07026.
- D. Bresch-Pietri and D. Del Vecchio. Estimation for decentralized safety control under communication delay and measurement uncertainty, *Automatica*, 2015. Accepted.
- S. Z. Yong, M. Zhu, and E. Frazzoli. Resilient state estimation against switching attacks on stochastic cyber-physical systems. *Proc IEEE Conference on Decision and Control*, 2015. To appear.
- S. Z. Yong, M. Zhu, and E. Frazzoli. On strong detectability and simultaneous input and state estimation with a delay. *Proc. IEEE Conference on Decision and Control*, 2015. To appear.
- S. Z. Yong, M. Zhu, and E. Frazzoli. Simultaneous input and state estimation of linear discrete-time stochastic systems with input aggregate information. *Proc. IEEE Conference on Decision and Control,* 2015. To appear.
- S. Z. Yong, M. Zhu, and E. Frazzoli. Simultaneous input and state estimation for linear time-invariant continuous-time stochastic systems. *Proc. American Control Conference*, 2015.
- S. Z. Yong, M. Zhu, and E. Frazzoli. Generalized innovation and inference algorithms for hidden mode switched linear stochastic systems with unknown inputs. *Proc. IEEE Conference on Decision and Control*, 2014.
- S. Z. Yong, M. Zhu, and E. Frazzoli. Simultaneous input and state smoothing for linear discrete-time stochastic systems with unknown inputs. *Proc. IEEE Conference on Decision and Control*, 2014.
- S.Z. Yong, M. Zhu, and E. Frazzoli. A unified filter for simultaneous input and state estimation of linear discrete-time stochastic systems. *Automatica*, 2015. Provisionally accepted. Available from: http://arxiv.org/abs/1309.6627.
- S. Z. Yong, M. Zhu, and E. Frazzoli. Simultaneous input and state estimation for linear time-varying continuous-time stochastic systems. *IEEE Transactions on Automatic Control*, 2015. In review.