FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Resilient Supervisory Control of Autonomous Intersections in the Presence of Sensor Attacks

Amin Ghafouri and Xenofon Koutsoukos

Institute for Software Integrated Systems, Vanderbilt University

Berkeley UNIVERSITY OF CALIFORNIA
Massachusetts Institute of Technology
NSF
MICHIGAN
VANDERBILT UNIVERSITY

Motivation

* Cyber-physical systems (CPS), such as autonomous vehicles crossing an intersection, are vulnerable to sensor attacks.
* In autonomous intersections, the aim is to provide a **safe**, **scalable**, and **efficient** framework for coordinating autonomous vehicles.
* Supervisory control of discrete event systems (DES) allows incorporating the continuous dynamics and formally analyzing system safety.

Resilient Supervisory Control

* Resilient supervisory control design steps:
  1. Show supervisory control is vulnerable to sensor attacks
  2. Introduce a **detector** in the control architecture with the purpose of detecting sensor attacks
  3. Characterize **stealthy attacks** that cannot be detected but are capable of compromising safety
  4. Present a **resilient supervisory controller** that is secure against stealthy attacks
  5. Demonstrate functionality using examples and simulations

Amin Ghafouri and Xenofon Koutsoukos. "Resilient supervisory control of autonomous intersections in the presence of sensor attacks," Submitted to *the 19th ACM International Conference on Hybrid Systems: Computation and Control (HSCC 2016)*. Vienna, Austria, April 12-14, 2016.

System Model

* Vehicles are modeled as single integrators. For a set of vehicles, their dynamics are described by

$$\dot{x} = v + d$$

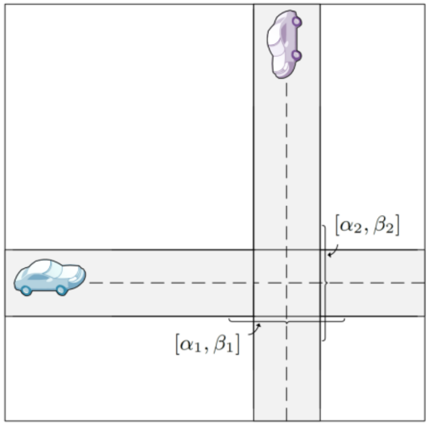
* Assuming the input is kept constant over each time interval, the time discretization is

$$x_{k+1} = x_k + u_k + \delta_k$$

* Sensor attacks on measurements are described as

$$\tilde{x}_k = x_k + e_k, \; k \in [k_s, k_e]$$

* They can lead to collision or deadlock among cars.



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Supervisory Control System

* Supervisory control has three operational goals:
  1. **Safety**: collisions must be avoided.
  2. **Non-blockingness**: vehicles must eventually cross the intersection.
  3. **Maximal-permissiveness**: vehicles must not be restricted unless necessary.
* In order to achieve these requirements, a supervisory controller disables inputs that lead to unsafety and deadlock based on the estimates.

Detector

* Detects attacks before they can cause significant damage.
* Nonparametric **Cumulative sum (CUSUM)** statistic as detection method.
* Incorporates knowledge of the physical system with the previously received data.
* Expected value is less than zero in the case of normal behavior.

$$z(k) := \inf_{\hat{x}(k) \in \mathbf{Post}_u \tilde{x}_{k-1}} ||\tilde{x}(k) - \hat{x}(k)|| - b$$

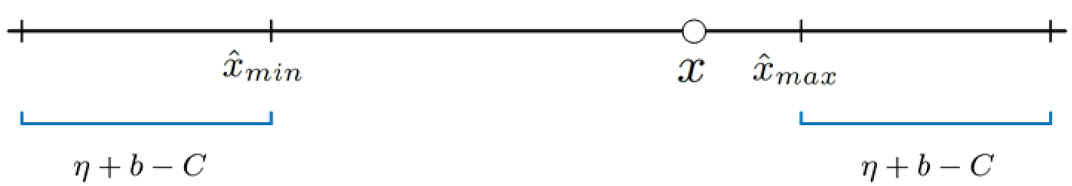
* Upon detection, vehicles are controlled by a fail-safe controller.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Stealthy Attacks

- Cannot be detected but are capable of compromising safety.
- They exist because of the following factors:
  1. Detector's threshold
  2. Disturbances and uncontrolled vehicles
- We characterize the **set of stealthy attacks** that contains all the corrupted measurements that cannot be detected.

$$I_k^s(\tilde{x}_{k-1}, u_{k-1}, C_{k-1}) = [\hat{x}_{min} - \eta - b + C, \hat{x}_{max} + \eta + b - C]$$



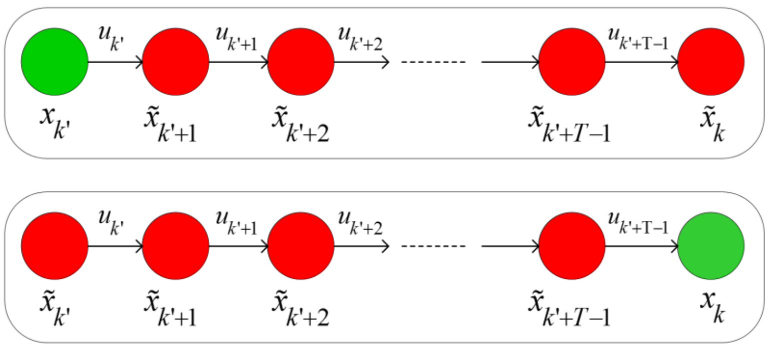
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Resilient Supervisor Design

* Maintains safety even in the presence of stealthy attacks.
* Resilient supervisor design:
  1. Constructing an **estimator system** that computes the smallest state estimate containing the actual state taking into consideration possibly corrupted measurements.
  2. Creating a **finite DES abstraction** of the estimator system.
  3. Translating the control problem to the DES domain, solving it, and translating the results back to the continuous domain.

Estimator

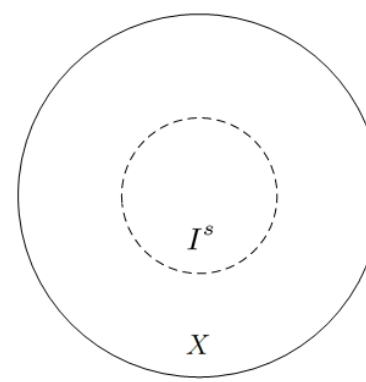
- Assuming $k' = k - T_{max}$, either $\tilde{x}_k$ or $\tilde{x}_{k'}$ is not attacked.



$$\hat{I}_k(\tilde{x}_{k'}, \tilde{x}_k) = \{\mathbf{Post}_{u_{k'} \ldots u_{k-1}} \tilde{x}_{k'}\} \cup \tilde{x}_k$$

- The set $\hat{I}$ contains the true state despite the attack.
- The estimator **predicts** a set of states and then **corrects** it:

$$I_k(I_{k-1}, I_k^s, \tilde{x}_k) = \begin{cases} \{\mathbf{Post}_u I\} \cap \hat{I}_k & \tilde{x}_k \in I_k^s \\ \text{detection} & \text{else} \end{cases}$$

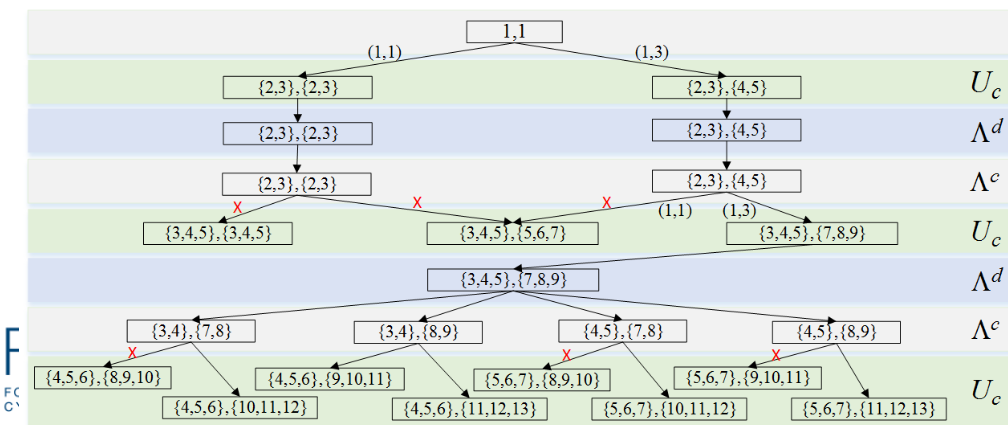


Discrete Event System (DES)

- Consider the **DES** $G := (Q, E, \psi, q_0, Q_m)$ with discrete states Q defined using the map $\ell(x) := \min_{q \in Q} \{q : \|x - q\| \leq \tau\mu/2\}$.

- The five-layer event set is shown in the table.
- An **Observer** of G is constructed using the notion of information states.
- Example of an observer:

Event	Controllable	Observable
Controlled input	✓	✓
Uncontrolled input	×	×
Disturbance	×	×
Prediction-Correction	×	✓
Detection	×	✓



Supervisor Construction

* Theorem: The relation between the observer and the estimator system is **simulation/alternating simulation.**
* Supervisory controller solution:
  1. Translating safety and non-blockingness specifications to the DES domain
  2. Solving the problem using the Basic Supervisory Control Problem in the Non-Blocking (BSCP-NB) algorithm and obtaining a supervisor S such that:

$$\mathcal{L}_m(S/G) = (\mathcal{L}_m(H))^{\uparrow C} \text{ and } \mathcal{L}(S/G) = \overline{(\mathcal{L}_m(H))^{\uparrow C}}$$

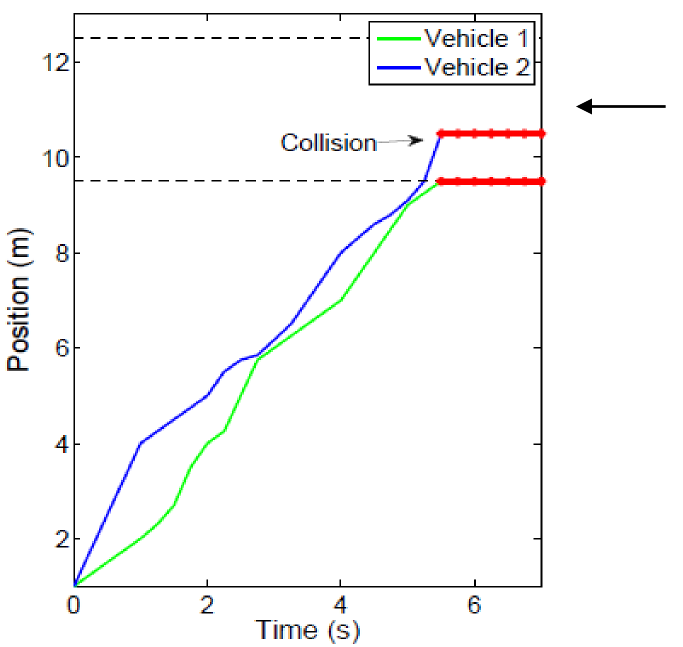
  1. Translating the obtained supervisor to the continuous domain

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

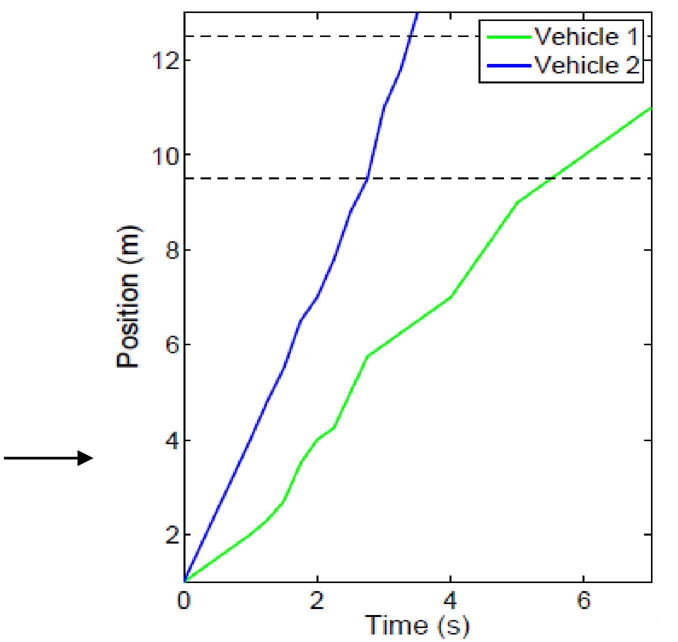
Example

* Intersection with a controllable and an uncontrollable car
* Surge attack on the controllable car: $\tilde{x}_k = \begin{cases} \hat{x}_{max,k_s} + \eta + b & k = k_s \\ \tilde{x}_{k-1} + u_{k-1} + d_{max} + b & \text{else} \end{cases}$
* **Simulation** in SUMO using TraCI4MATLAB

Non-resilient Supervisor



Resilient Supervisor



Conclusion

* Supervisory control of autonomous intersections is vulnerable to sensor attacks. To improve the system resilience:
  * Introduced a **detector** in the control architecture
  * Characterized **stealthy attacks** that bypass the detector
  * Presented a **resilient supervisory controller** that is safe, non-blocking, and maximally permissive, despite the presence of sensor attacks
  * Demonstrated functionality using **simulations** in SUMO
* Future work: actuator attacks, decentralized resilient controllers, other control protocols

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Thank you!

Questions?

Appendix

1. Safety: $\inf_{t \geq 0, b' \in B} ||x(t) - b'||_\infty > 0$
2. CUSUM: $C_i(k) = (C_i(k-1) + z_i(k))^+$
3. Detector Decision: $d(C_i(k)) = \begin{cases} H_1 & \text{if } C_i(k) > \eta_i \\ H_0 & \text{otherwise} \end{cases}$
4. Event set: $E = \Lambda^d \times \Lambda^c \times U_c \times U_{uc} \times W$
5. Transition:

$$\psi(q, \lambda^d, \lambda^c, u_c, u_{uc}, w) = \psi_3(\psi_2(\psi_1(\psi^c(\psi^d(q, \lambda^d), \lambda^c), u_c), u_{uc}), w)$$

6. Supervisor map: $\sigma(I) = \{u_c/\tau : u_c \in S(\ell(I))\}$