# Security of Distributed Cyber-Physical Systems with Connected Vehicle Applications


**Dr. Pierluigi Pisu[1], Dr. Richard Brooks[2], and Dr. Jim Martin[3]**

[1] pisup@clemson.edu, Department of Automotive Engineering

[2] rrb@clemson.edu, Holcombe Department of Electrical and Computer Engineering

[3] jmarty@clemson.edu, School of Computing


## Project objective

This project focuses on connected vehicle applications where vehicles share information via dedicated short-range communication (DSRC), with the goal of improving fuel efficiency of the system and avoiding collision.

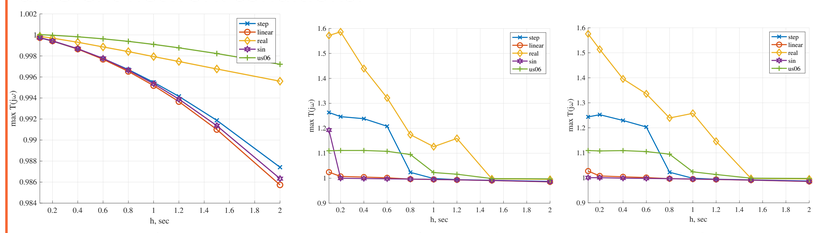
## Motivation

- Increasing the security of vehicles;
- Increasing the traffic throughput;
- Reducing fuel consumption and emission;
- Reducing the human failure and accident.

## CACC Performance Metrics

### *String Stability*

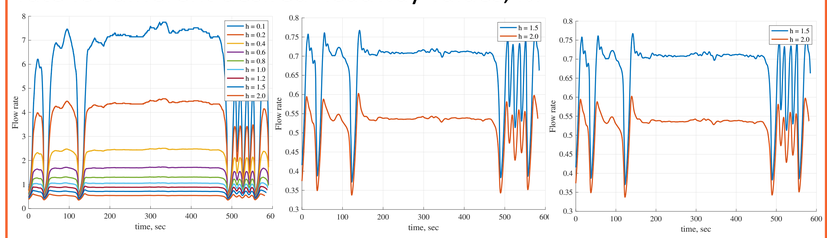
String stability defines how disturbance in the front of the platoon propagates to the rear of the platoon for a given headway value $h$. A system is string stable if $\max T(j\omega) \leq 1$. The graphs below shows string stability for different acceleration profiles under different network conditions.




No Packet Loss | Network Congestion | Denial of Service

### *Traffic Flow*

Traffic flow rate is calculated as the number of vehicles passing over a point on the road per unit second. The following graphs shows the effect of network congestion and DoS attacks on flow rate for different desired headway values, $h$.




No Packet Loss | Network Congestion | Denial of Service

Results show the traffic flow rates are greatly impacted by network impairment.

## Mitigation Strategies

The headway time value $h$ impacts the safe and efficient operation of a CACC platoon. We define an adaptive $h$ value that adapts to network reliability.

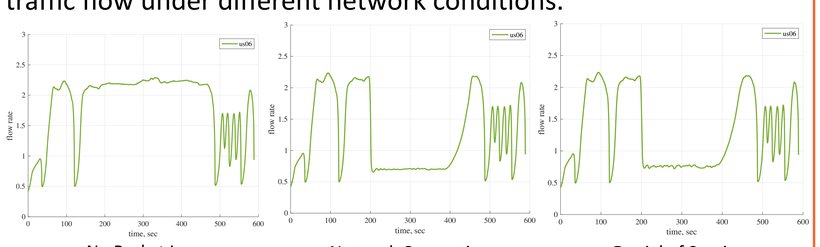
### *Network Reliability Metric*

Reliability metric of the communication network is defined as the ratio of packets that were successfully received to the total number of packets that were expected.

$$Reliability = 1 - \frac{N_{failed}}{N_{total}}$$

### *Dynamic headway assignment*

Adapting headway values to network reliability yields improved traffic flow under different network conditions.



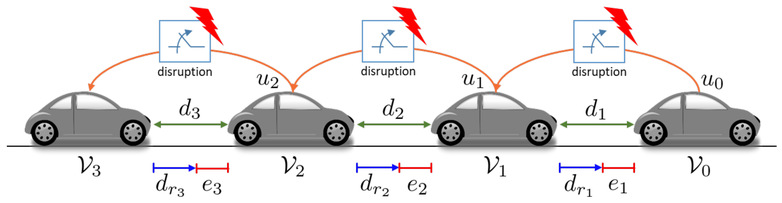

No Packet Loss | Network Congestion | Denial of Service

Adapting headway value $h$ improves traffic flow rate over using fixed $h$ value under unexpected network conditions.

## DoS-Resilient Hybrid Controller for String-Stable Connected Vehicles

Radio jamming with unknown strategy

Energy and geography constrained



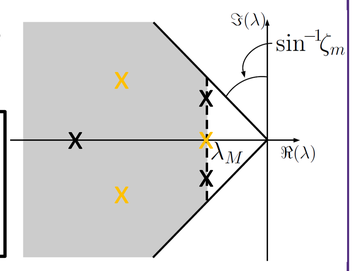

The attacker generates DoS with the purpose of disrupting the network for the longest time possible.

Design a controller to be resilient to the longest possible sequence of packet drop out, under certain performance constraints and satisfying string stability.

### *Performance Requirements*

The "networked-free" error dynamics must satisfy given performance

$$\mathbb{P}(\lambda_M, \zeta_m) := \{A \in \mathbb{R}^{n\times n} | \Lambda_{\max}(A) = \lambda_M, \; \zeta_{\min}(A) \geq \zeta_m\}$$




Case C1

$k_d = f_{C1}(k_p)$

$k_p \in [\underline{k}_{p_{C1}}, \bar{k}_{p_{C1}}]$

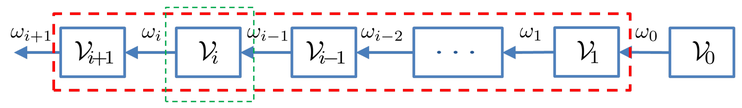
Case C2

$k_d = f_{C2}(k_p)$

$k_p \in (\underline{k}_{p_{C2}}, \bar{k}_{p_{C2}}]$

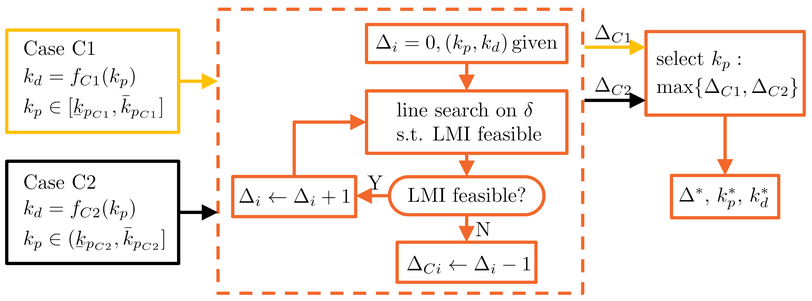
### *String Stability*

String stability of the whole vehicle platoon can be studied as input-output stability of the single vehicle.




$\frac{\|\omega_0\|_{\mathcal{L}_2}}{\|\omega_{i-1}\|_{\mathcal{L}_2}} \leq 1$ ⇨ $\mathcal{L}_2$ stability ⇨ LMI-based analysis

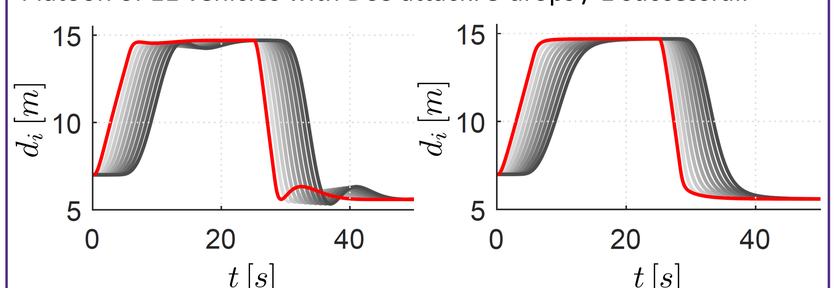
### *Design Algorithm*




### *Numerical Results*

Comparison between tuning in [Ploeg ea CITS '11] [1] and tuning with proposed approach.

Platoon of 11 vehicles with DoS attack: 5 drops / 1 successful.




Tuning as in [Ploeg ea CITS '11] [1] | Tuning as the proposed approach

[1] J. Ploeg et al., "Design and experimental evaluation of cooperative adaptive cruise control," in 14th IEEE Intelligent Transportation Systems Conference, 2011.

## Robust Control For Distributed Automotive System

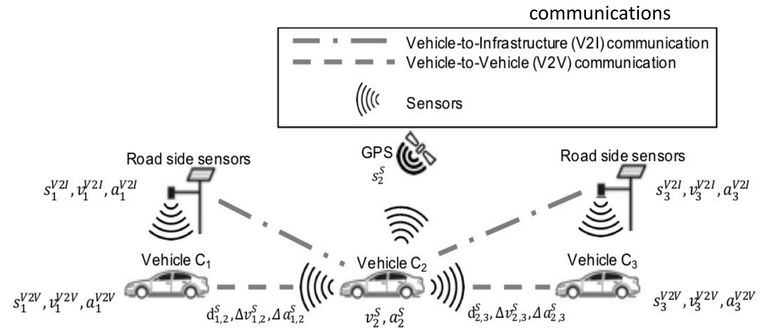
### *Sensor Measurements of a Distributed Automotive System*

| Description | Sensor Type | Symbol |
|---|---|---|
| $C_2$'s local measurement of its position | Raw GPS data | $s_2^S$ |
| $C_2$'s local measurement of its velocity | Wheel rotation speed | $v_2^S$ |
| $C_2$'s local measurement of its acceleration | Accelerometer data | $a_2^S$ |
| Distance between $C_1$ and $C_2$ | Laser distance sensor | $d_{1,2}^S$ |
| Speed difference between $C_1$ and $C_2$ | Doppler radar | $\Delta v_{1,2}^S$ |
| Acceleration difference between $C_1$ and $C_2$ | Lidar | $\Delta a_{1,2}^S$ |
| Distance between $C_2$ and $C_3$ | Laser distance sensor | $d_{2,3}^S$ |
| Speed difference between $C_2$ and $C_3$ | Doppler radar | $\Delta v_{2,3}^S$ |
| Acceleration difference between $C_2$ and $C_3$ | Lidar | $\Delta a_{2,3}^S$ |

Local sensor measurements of C2

| Description | Sensor Type | Symbol |
|---|---|---|
| $C_1$'s position sent by RSU at $t$ | V2I | $s_1^{V2I}$ |
| $C_1$'s velocity sent by RSU at $t$ | V2I | $v_1^{V2I}$ |
| $C_1$'s acceleration sent by RSU at $t$ | V2I | $a_1^{V2I}$ |
| $C_1$'s position sent by $C_1$ at $t-1$ | V2V | $s_1^{V2V}$ |
| $C_1$'s velocity sent by $C_1$ at $t-1$ | V2V | $v_1^{V2V}$ |
| $C_1$'s acceleration sent by $C_1$ at $t-1$ | V2V | $a_1^{V2V}$ |
| $C_3$'s position sent by RSU at $t$ | V2I | $s_3^{V2I}$ |
| $C_3$'s velocity sent by RSU at $t$ | V2I | $v_3^{V2I}$ |
| $C_3$'s acceleration sent by RSU at $t$ | V2I | $a_3^{V2I}$ |
| $C_3$'s position sent by $C_3$ at $t-1$ | V2V | $s_3^{V2V}$ |
| $C_3$'s velocity sent by $C_3$ at $t-1$ | V2V | $v_3^{V2V}$ |
| $C_3$'s acceleration sent by $C_3$ at $t-1$ | V2V | $a_3^{V2V}$ |

Data inputs to C2 via V2X communications




### *Faults*

**Physical**
- Sensor malfunctions.
- Actuator malfunctions

**Cyber**
- Denial of service
- Packet dropping
- Code/data insertion, etc.

### *Fault-tolerant Control Schemes*

- **Naive Averaging:** Simply uses the arithmetic average of all the different ways to estimate a parameter as its estimate.
- **Averaging Without Maximum and Minimum:** Input is very similar to the naive averaging, except that the maximum value and the minimum value are excluded in the calculating the average values of each parameter.
- **Kalman filter:** Takes inputs from multiple sources to correct the estimate from the previous time step, and then make a prediction for the next step.

### *Design Approach*

1. Automotive system (Platoon) integrated with fault conditions and countermeasures is simulated.
2. Simulation information is collected (fuel performance & no crashes).
3. Game between fault conditions and fault-tolerant control schemes is established. Payoff matrix is prepared.
4. Z-test is conducted. Dominance strategies are identified.
5. Solution of the game is identified from dominance strategies.
6. Solution is used to improve controller robustness.

## Benefits

### Scientific Impacts

- Potential improvement in traffic conditions, vehicle and personal safety, and energy consumption.
- Collision avoidance.
- More security is valuable for car makers and auto insurances.

### Broader Impacts

- General approach for distributed networked CPSs.
- This method makes CPSs more resilient and secure to cyber attacks.
- Research data is useful for public and private agencies responsible for providing infrastructure side of the connected vehicle system.


This material is based upon work supported by the National Science Foundation (NSF) under grant No. CNS-1544910. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.