itee Ph.D

iNFORMATION tECHNOLOGY eLECTRICAL eNGINEERING

Alberto Petrillo

Tutor: Stefania Santini

XXXI Cycle - III year presentation

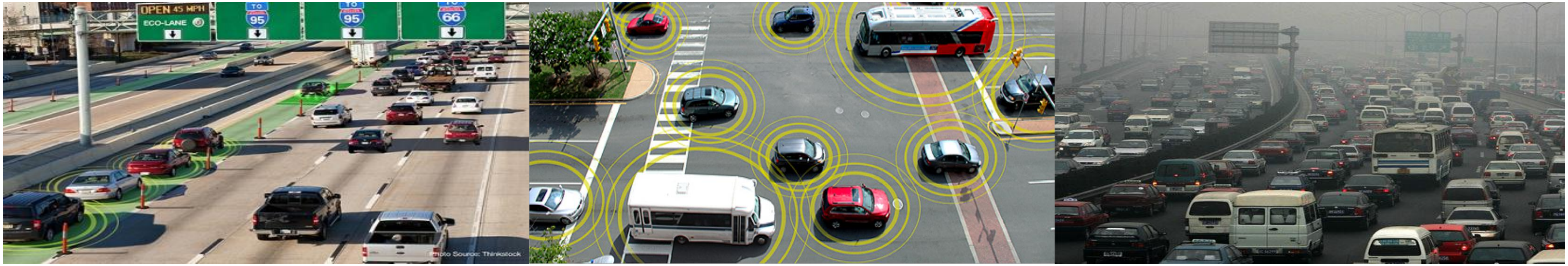
Cooperative Control of Autonomous Connected Vehicles from a Networked Control Perspective

Theory and Experimental Validation

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

Cooperative Driving of Autonomous Connected Vehicles (1/2)

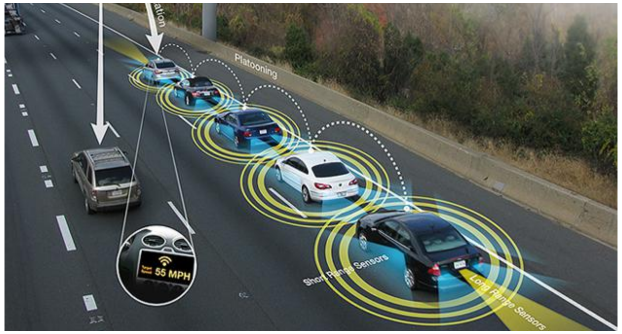
- Connected autonomous vehicles have recently attracted extensive research interest due to their potential to significantly improve the road traffic, e.g. by enhancing road safety, traffic capacity and its smoothness, and by reducing at the same time fuel consumption.

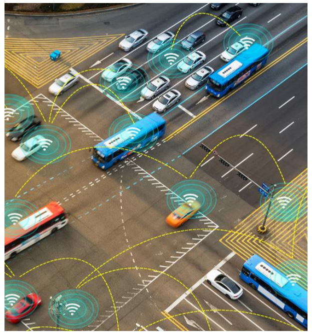


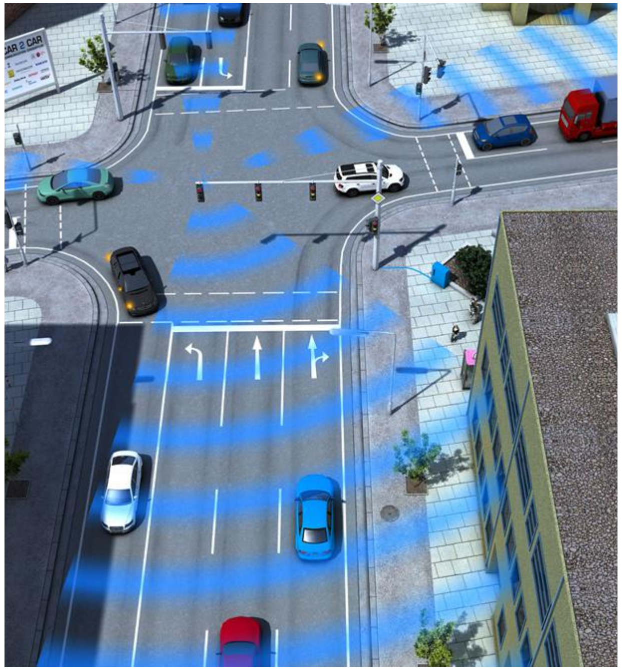
- One of the fundamental aims in ITS is to cooperatively drive along the road by operating platoons of vehicles capable to reach and maintain an optimal inter-vehicular spacing policy, tracking at the same time desired speed and acceleration profiles.

Cooperative Driving of Autonomous Connected Vehicles (2/2)

- Leveraging V2X, connected vehicles can share information with neighbours and/or receive a reference signal coming from a leading vehicle or a road infrastructure (virtual leader).







Communication networks:

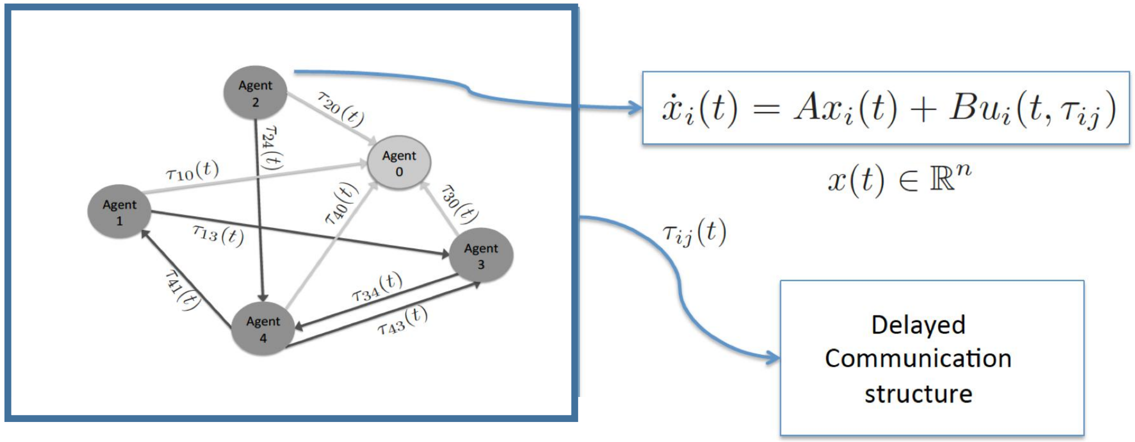
1. Wi-Fi networks (IEEE 802.11p);
2. Mobile networks 4G/5G.

The onboard control protocol for autonomous driving is responsible of:

- the safe tracking of the desired velocity and acceleration profiles;
- the maintenance a desired inter-vehicles spacing policy.

Cooperative Driving of Autonomous Connected Vehicles as a Networked Control System

The problem of controlling fleets of autonomous connected vehicles can be solved in the more general context of networked control systems.

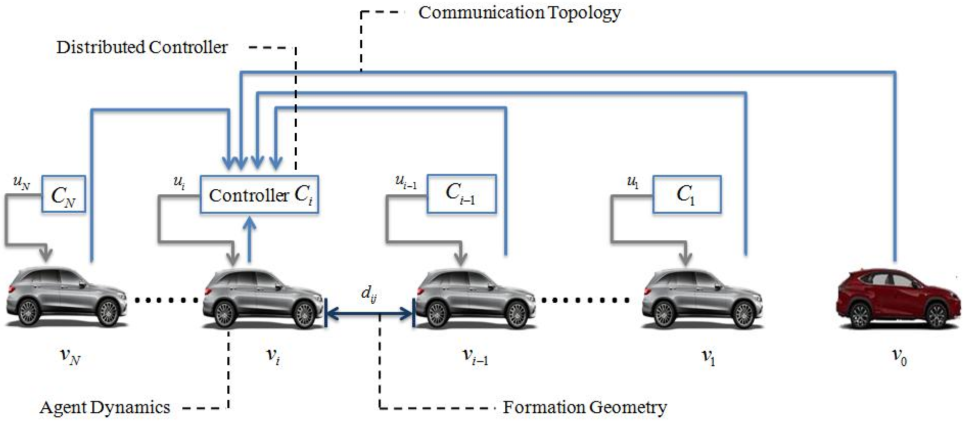


$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t, \tau_{ij})$$

$$x(t) \in \mathbb{R}^n$$

$\tau_{ij}(t)$

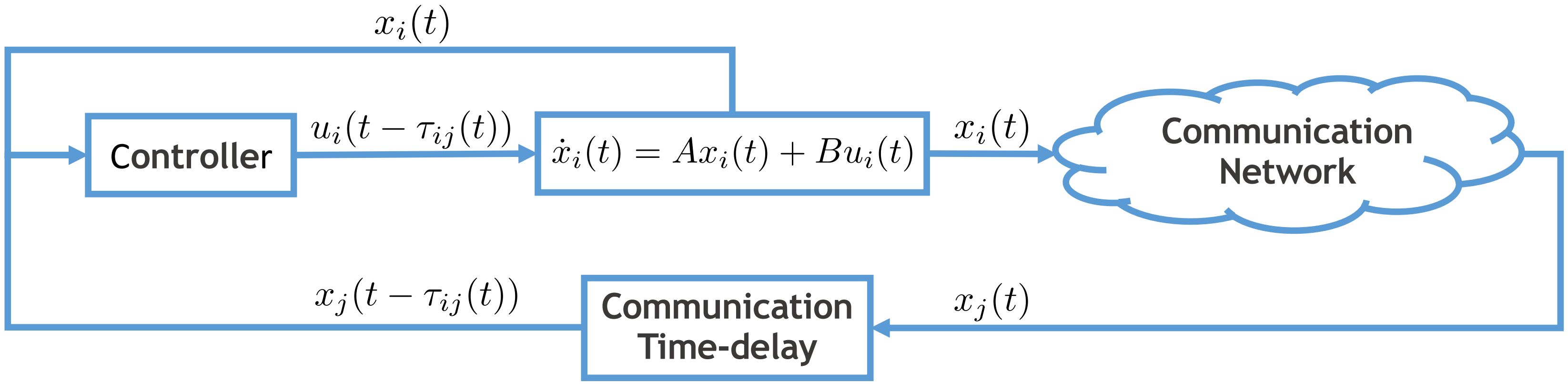
Delayed Communication structure



By leveraging this paradigm, a platoon composed by multiple connected autonomous vehicles is represented as one-dimensional network of dynamical agents, in which each agent only uses its neighbouring information to locally control its motion, while it aims to achieve certain global coordination with all other agents.

Designing of Cooperative Control Strategy

Cooperative control strategies are traditionally designed under the implicit restrictive assumption of perfect communication environments and unlimited bandwidth.



During normal operating conditions, wireless communication networks introduce unavoidable communication impairments due to the current status of each of the communications links (e.g., bounded communication delays and packet losses).

It follows that networked-induced phenomena must be taken into account from the very beginning of the design phase of cooperative control strategies.

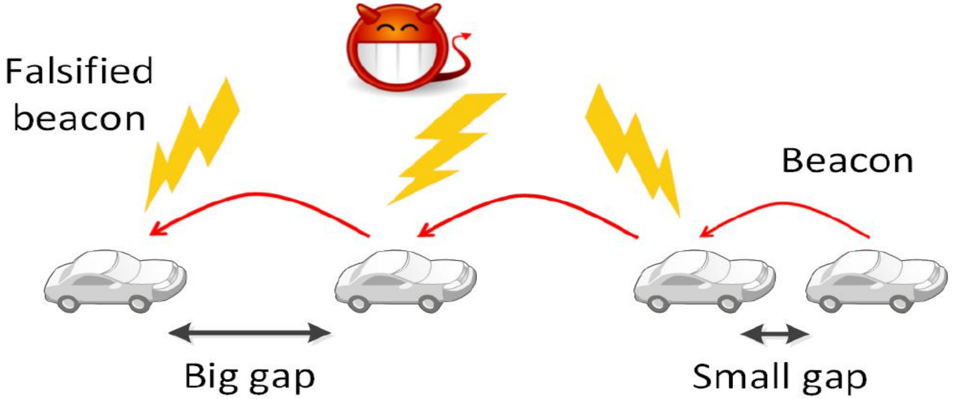
Communication Issues in Networked Control Systems and Cooperative Driving Application

- Communication issues have been tackled in the current literature on control design under the restrictive assumption that the communication delay is homogeneous and often constant.
- However, in practice, each communication link, connecting a pair of cars within a vehicular network, is affected by a different variable time-delay that depends on actual conditions, or current impairments, of the communication channel.

One open challenge in the control field for connected vehicles is hence to design cooperative control algorithms resilient and robust with respect to heterogeneous time-varying delays (e.g., due to packet losses).

Security Issues in Networked Control Systems and Cooperative Driving Application (1/2)

- Besides communication issues arising in normal operating conditions, wireless communication networks may suffer different security threats.
- In collaborative driving applications, the sudden appearance of a malicious attack on the communication network is crucial since it mainly compromises:
  a. the correctness of data traffic flow;
  b. the application safety.



Traditional security methods in the technical literature on communication networks (wireless or not) include encryption/decryption methods, authentication tools, and digital signatures.

Security Issues in Networked Control Systems and Cooperative Driving Application (2/2)

The resilience of the control system has been also very recently indicated as a further key ingredient, to be added to the more traditional ones, for enhancing the protection level or better for ensuring that control algorithm can cope with cyber-attacks on a physical process, or limit their negative effects.

- From a control viewpoint, the recent literature on the security of networked cyber-physical systems is usually devoted to the design of state estimators for the better understanding of a system dynamical behaviour under specific malicious threats or for the attacks detection.
- However, the cooperation features, implicit within the networked control systems paradigm, could be also exploited at control design level as a promising solution for counteracting security vulnerabilities.

The idea is to design cooperative distributed control protocols able to drive a networked system in the presence of the communication impairments arising during normal operating conditions, while also mitigating at the same time the effects of different kinds of possible cyber-attacks in malicious scenarios.

Work Aims

From literature overview the following main open challenges arise:

1. to design distributed cooperative control algorithms able to cope with multiple time-varying communication delays and packet losses;
2. to design resilient secure distributed control algorithms able to counteract both security vulnerabilities and time-delays.

The aim of my research activity is to tackle and solve both the challenges by designing proper control strategies.

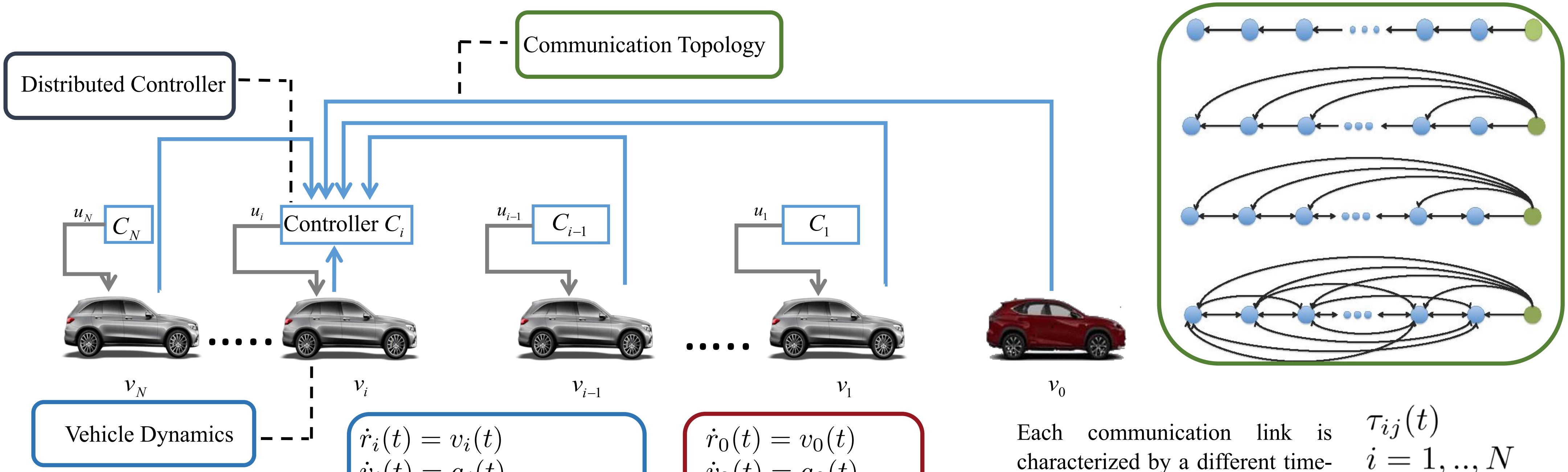
The idea is to tailor the theoretical results for solving practical problems that are crucial for innovative ITS applications with a high automation level:

i. autonomous Vehicles Platoon;

ii. cooperative driving of autonomous vehicles at traffic intersection.

Autonomous Vehicles Platoon

Let consider an autonomous platoon of N+1 vehicles travelling on a single lane and sharing information through wireless communication network.



$$\begin{aligned}\dot{r}_i(t) &= v_i(t)\\ \dot{v}_i(t) &= a_i(t)\\ \dot{a}_i(t) &= \tfrac{1}{T}(u_i(t) - a_i(t))\end{aligned}$$

$$\begin{aligned}\dot{r}_0(t) &= v_0(t)\\ \dot{v}_0(t) &= a_0(t)\\ \dot{a}_0(t) &= -\tfrac{1}{T}a_0(t)\end{aligned}$$

Each communication link is characterized by a different time-varying delay

$$\tau_{ij}(t)$$
$$i = 1, .., N$$
$$j = 0, 1, .., N$$

Control Objectives

The platoon control goal is to guarantee that each vehicle:

1. **safely tracks the desired velocity and acceleration profiles as imposed by the leader;**
2. **reaches and maintains a desired inter-vehicles spacing policy;**

$$\begin{array}{ll} \lim_{t\to\infty} \|r_i(t) - r_0(t) - d_{i0}\| = 0 & \\ \lim_{t\to\infty} \|v_i(t) - v_0(t)\| = 0 & \qquad \forall i = 1, ..., N, \\ \lim_{t\to\infty} \|a_i(t) - a_0(t)\| = 0 & \end{array}$$

despite the presence of communication impairments and/or eventual cyber-attacks.

Safe leader-Tracking: Adaptive Synchronization-based Control Protocol

The proposed strategy is:

$$\boxed{u_i = -\sum_{j=0}^{N} \alpha_{ij} k_{ij}^{\top}(t) \begin{bmatrix} r_i(t-\tau_{ij}(t)) - r_j(t-\tau_{ij}(t)) - d_{ij} \\ v_i(t-\tau_{ij}(t)) - v_j(t-\tau_{ij}(t)) \\ a_i(t-\tau_{ij}(t)) - a_j(t-\tau_{ij}(t)) \end{bmatrix}}$$

- **Communication time-varying delay** $\tau_{ij}(t)$
- **Network topology** α_{ij}
- **Desired spacing between each pair of vehicles** d_{ij}
- **Adaptive control gains** $k_{ij}(t) = \begin{bmatrix} \rho_{ij}(t) \\ \beta_{ij}(t) \\ \gamma_{ij}(t) \end{bmatrix}$ $\left\{ \begin{array}{ll} \dot{\rho}_{ij}(t) & = \zeta_{ij,1}\left(r_i(t-\tau_{ij}(t)) - r_j(t-\tau_{ij}(t)) - d_{ij}\right)^2 \\ \dot{\beta}_{ij}(t) & = \zeta_{ij,2}\left(v_i(t-\tau_{ij}(t)) - v_j(t-\tau_{ij}(t))\right)^2 \\ \dot{\gamma}_{ij}(t) & = \zeta_{ij,3}\left(a_i(t-\tau_{ij}(t)) - a_j(t-\tau_{ij}(t))\right)^2 \end{array} \right.$
- **Positive constants** $\zeta_{ij,k} \in \mathbb{R}^+ \ (\forall k = 1, 2, 3)$

Closed-loop Dynamics

To prove the cooperative synchronization of vehicles dynamics to the leader motion, define the state error dynamics of the whole vehicles platoon

$$e_i(t) = \begin{bmatrix} r_i(t) - r_0(t) - d_{i0} \\ v_i(t) - v_0(t) \\ a_i(t) - a_0(t) \end{bmatrix} \quad e_j(t) = \begin{bmatrix} r_j(t) - r_0(t) - d_{j0} \\ v_j(t) - v_0(t) \\ a_j(t) - a_0(t) \end{bmatrix} \quad \Longrightarrow \quad \begin{aligned} \dot{e}_i(t) = \quad & A e_i(t) + \mathcal{C}_{i0}(t) e_i(t - \tau_{i0}(t)) + \\ & \sum_{j=1}^{N} \widehat{\mathcal{C}}_{ij}(t) \left[e_i(t - \tau_{ij}(t)) - e_j(t - \tau_{ij}(t)) \right]. \end{aligned}$$

where

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{T} \end{bmatrix}, B = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{T} \end{bmatrix};$$

$$-B\alpha_{i0} k_{i0}^{\top}(t) = \mathcal{C}_{i0}(t) \in \mathbb{R}^{3\times3},$$

$$-B\alpha_{ij} k_{ij}^{\top}(t) = \widehat{\mathcal{C}}_{ij}(t) \in \mathbb{R}^{3\times3},$$

By defining

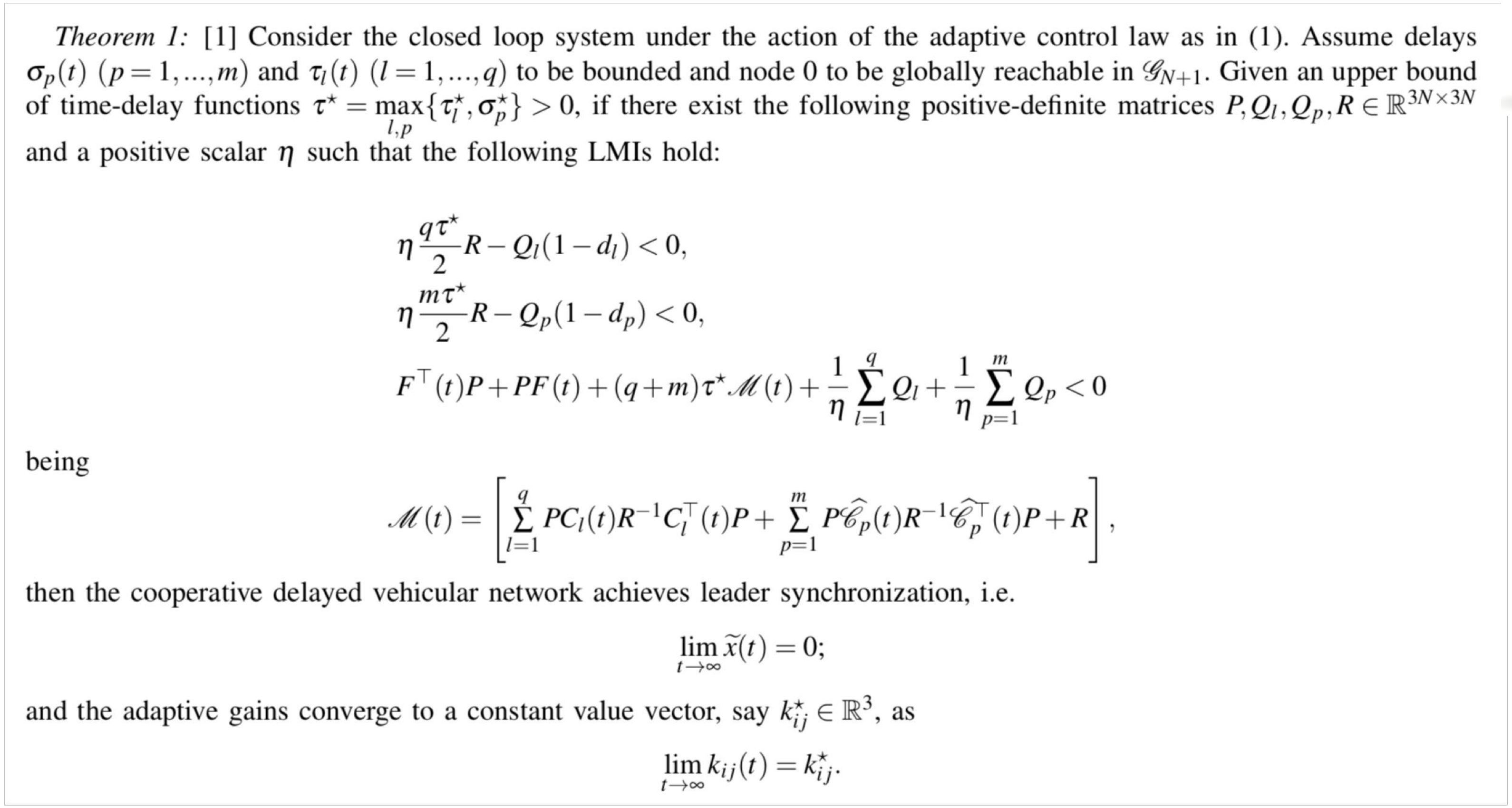
$$\sigma_p(t) \in \{\tau_{ij}(t) : i, j = 1, 2, ..., N, i \neq j)\}$$

$$\tau_l(t) \in \{\tau_{i0}(t) : i = 1, 2, ..., N\}$$

$$\widetilde{x}\,(t) = \left[\begin{array}{cccc} e_1^{\top}\,(t) & e_2^{\top}\,(t) & \cdots & e_N^{\top}\,(t) \end{array} \right]^{\top} \in \mathbb{R}^{3N}$$

$$\Longrightarrow \quad \boxed{\dot{\widetilde{x}}\,(t) = A_0 \widetilde{x}\,(t) + \sum_{l=1}^{q} C_l(t) \widetilde{x}\,(t - \tau_l\,(t)) + \sum_{p=1}^{m} \widehat{\mathcal{C}}_p(t) \widetilde{x}\,(t - \sigma_p\,(t)) \qquad \text{(1)}}$$

Stability Analysis



Theorem 1: [1] Consider the closed loop system under the action of the adaptive control law as in (1). Assume delays $\sigma_p(t)$ $(p=1,\dots,m)$ and $\tau_l(t)$ $(l=1,\dots,q)$ to be bounded and node 0 to be globally reachable in $\mathscr{G}_{N+1}$. Given an upper bound of time-delay functions $\tau^\star = \max_{l,p}\{\tau_l^\star, \sigma_p^\star\} > 0$, if there exist the following positive-definite matrices $P, Q_l, Q_p, R \in \mathbb{R}^{3N\times 3N}$ and a positive scalar η such that the following LMIs hold:

$$\eta\frac{q\tau^\star}{2}R - Q_l(1-d_l) < 0,$$
$$\eta\frac{m\tau^\star}{2}R - Q_p(1-d_p) < 0,$$
$$F^\top(t)P + PF(t) + (q+m)\tau^\star\mathscr{M}(t) + \frac{1}{\eta}\sum_{l=1}^{q} Q_l + \frac{1}{\eta}\sum_{p=1}^{m} Q_p < 0$$

being

$$\mathscr{M}(t) = \left[\sum_{l=1}^{q} PC_l(t)R^{-1}C_l^\top(t)P + \sum_{p=1}^{m} P\widehat{\mathscr{C}}_p(t)R^{-1}\widehat{\mathscr{C}}_p^\top(t)P + R\right],$$

then the cooperative delayed vehicular network achieves leader synchronization, i.e.

$$\lim_{t\to\infty}\tilde{x}(t) = 0;$$

and the adaptive gains converge to a constant value vector, say $k_{ij}^\star \in \mathbb{R}^3$, as

$$\lim_{t\to\infty}k_{ij}(t) = k_{ij}^\star.$$

[1] Petrillo, A., Salvi, A., Santini, S., & Valente, A. S. (2018). Adaptive multi-agents synchronization for collaborative driving of autonomous vehicles with multiple communication delays. *Transportation research part C: emerging technologies*, *86*, 372-392.

Numerical Analysis

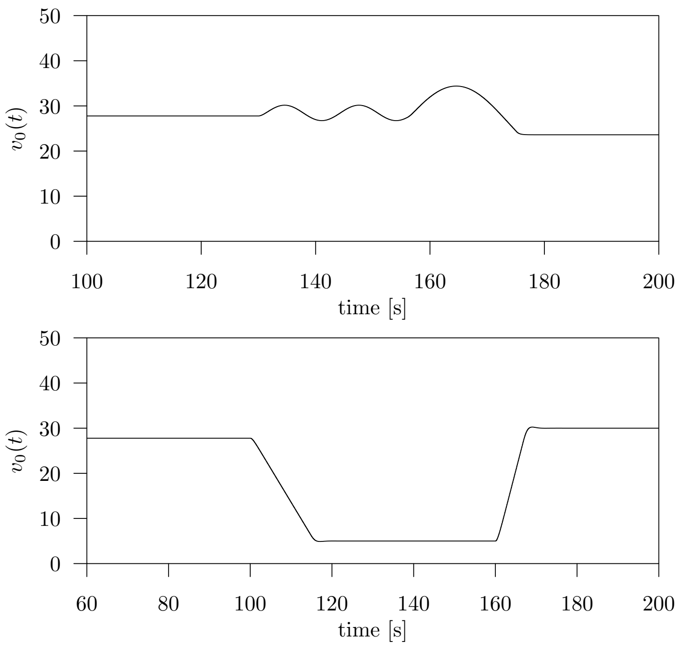
To validate the theoretical results we exploit the PLEXE simulator that leverages:

- •OMNeT++/MiXiM for simulating V2V communications based on the IEEE 802.11p standard;
- • SUMO for simulating the vehicle dynamics under the action of the collaborative driving strategy.

We consider an autonomous platoon of 7 vehicles plus leader that travels along a single lane. The tracking performances have been evaluated considering two representative leader maneuvers:

i. Trapezoidal Speed Profile;

ii. Realistic Driving Profile.

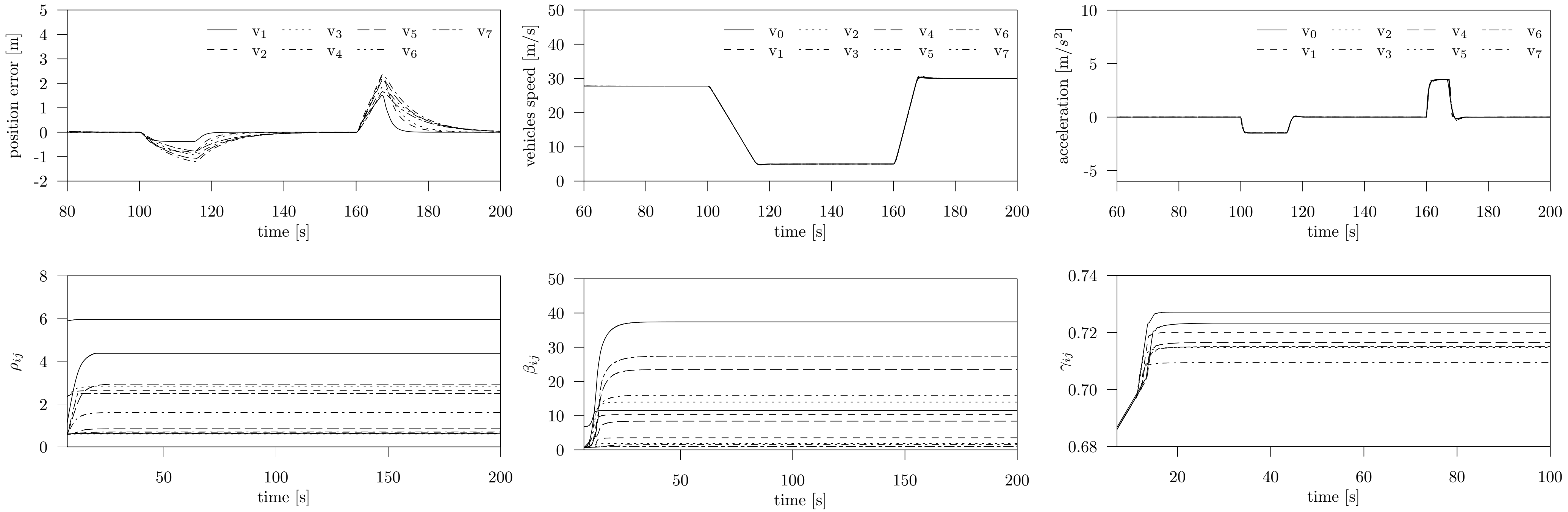


The investigation is conducted for different exemplar communication topologies:

1. Leader-Predecessor-Follower (L-P-F);
2. Predecessor-Follower (P-F);
3. Bidirectional-Leader-Follower (B-L-F);
4. Broadcast (BR)

Tracking Performances: Trapezoidal Speed Profile

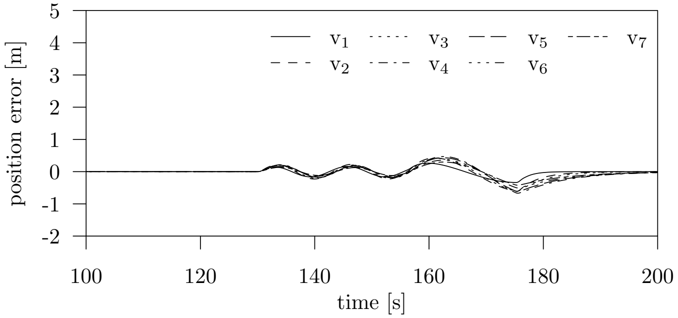
Consider vehicles sharing information via Leader-Predecessor-Follower (L-P-F) Topology.

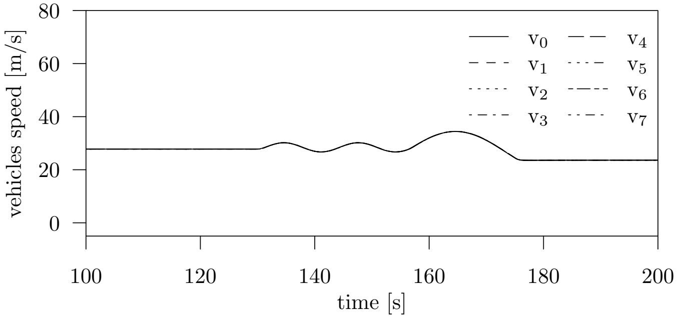


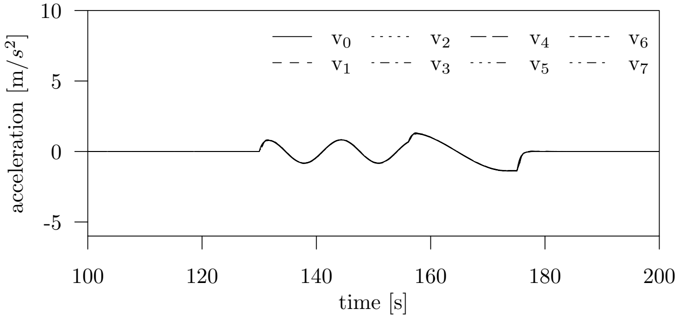
Alberto Petrillo

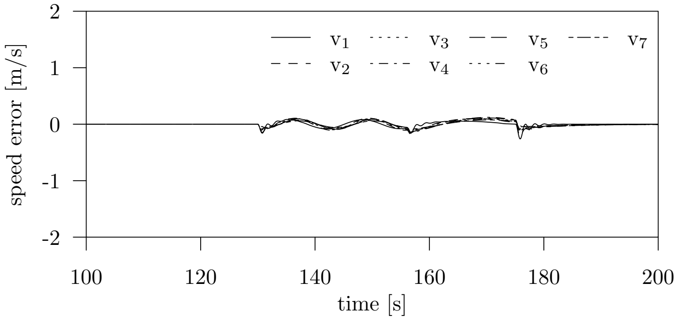
Tracking Performances: Realistic Speed Profile

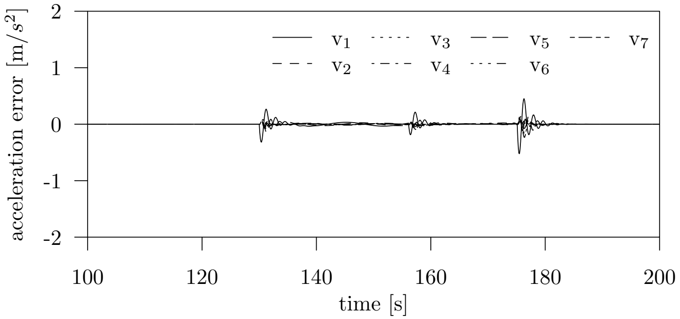
Consider vehicles sharing information via Leader-Predecessor-Follower (L-P-F) Topology.





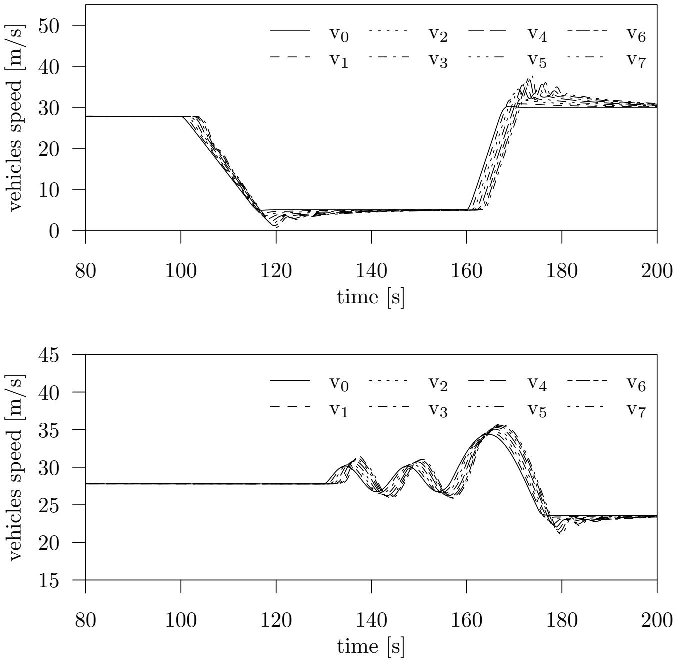




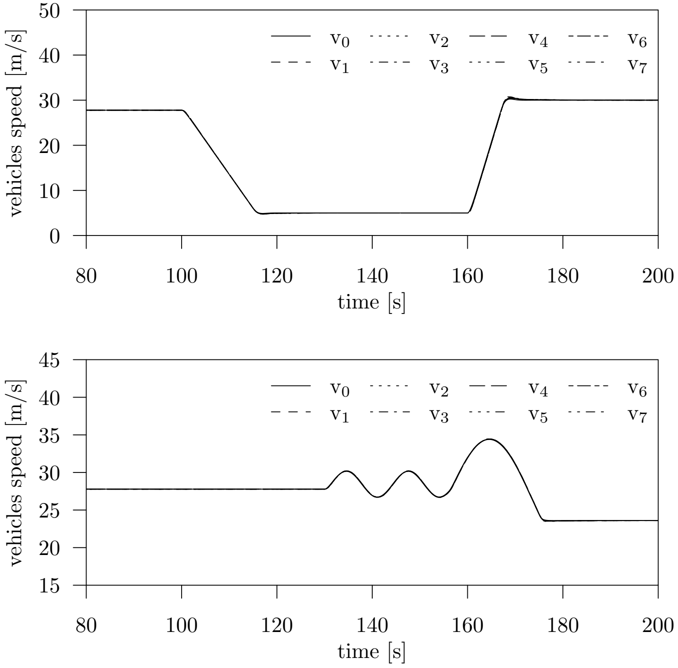


Tracking Performances: Alternative Topologies

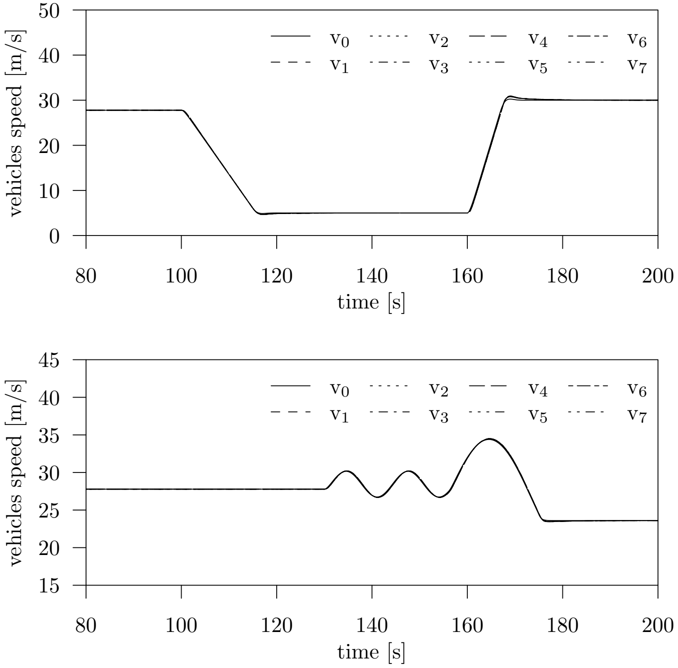
Consider vehicles sharing information via: 1)P-F; 2) B-L-F; 3)BR



P-F



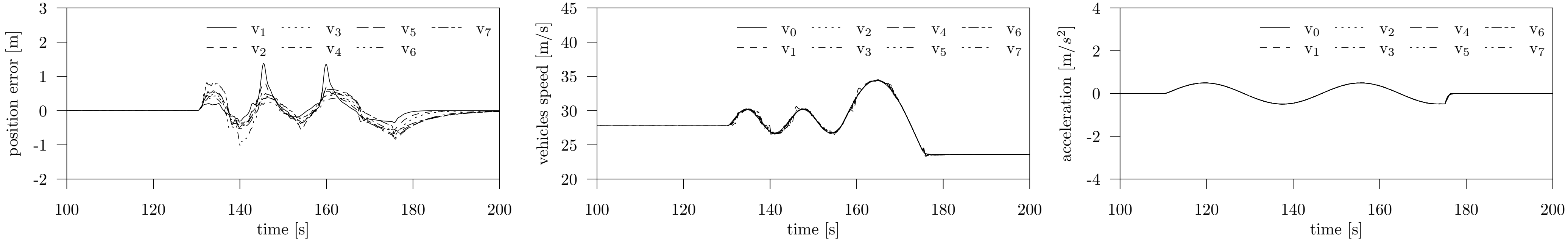
B-L-F



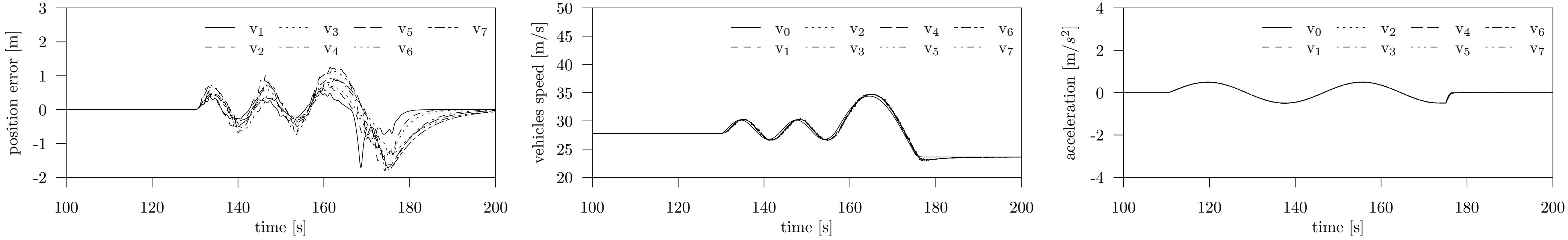
BR

Tracking Performances: Robusteness w.r.t. packet losses

Consider vehicles sharing information via Leader-Predecessor-Follower (L-P-F) Topology.



Gilbert Elliot



Bernoulli

Robusteness w.r.t. External Disturances

- Although robustness w.r.t. delays is crucial, another fundamental requirement, however less addressed in the current platoon literature, is to provide robustness also w.r.t. external disturbances arising from different environmental factors.
- External disturbances could arise from variations in wind velocity and/or road slope.
- When considering both external disturbances effects and time-varying delays, the dynamics of each vehicle within the platoon is described by the following third-order systems

$$\dot{x}_i = Ax_i + Bu_i(t;\tau_{ij}(t)) + Ew_i(t) \qquad A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{T} \end{bmatrix}, \ B = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{T} \end{bmatrix}, \ E = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix};$$

$$x_i(t) = [r_i(t)\ v_i(t)\ a_i(t)]^\top \in \mathbb{R}^3 \qquad u_i = -\sum_{j=0}^{N} \alpha_{ij} k_{ij}^\top(t) \begin{bmatrix} r_i(t-\tau_{ij}(t)) - r_j(t-\tau_{ij}(t)) - d_{ij} \\ v_i(t-\tau_{ij}(t)) - v_j(t-\tau_{ij}(t)) \\ a_i(t-\tau_{ij}(t)) - a_j(t-\tau_{ij}(t)) \end{bmatrix} \qquad w_i(t) \in \mathcal{L}_2[0;\infty)$$

Robusteness w.r.t. External Disturances: Stability Analysis

- **When considering external disturbances, the closed-loop platoon dynamics is described by the following dynamical systems**

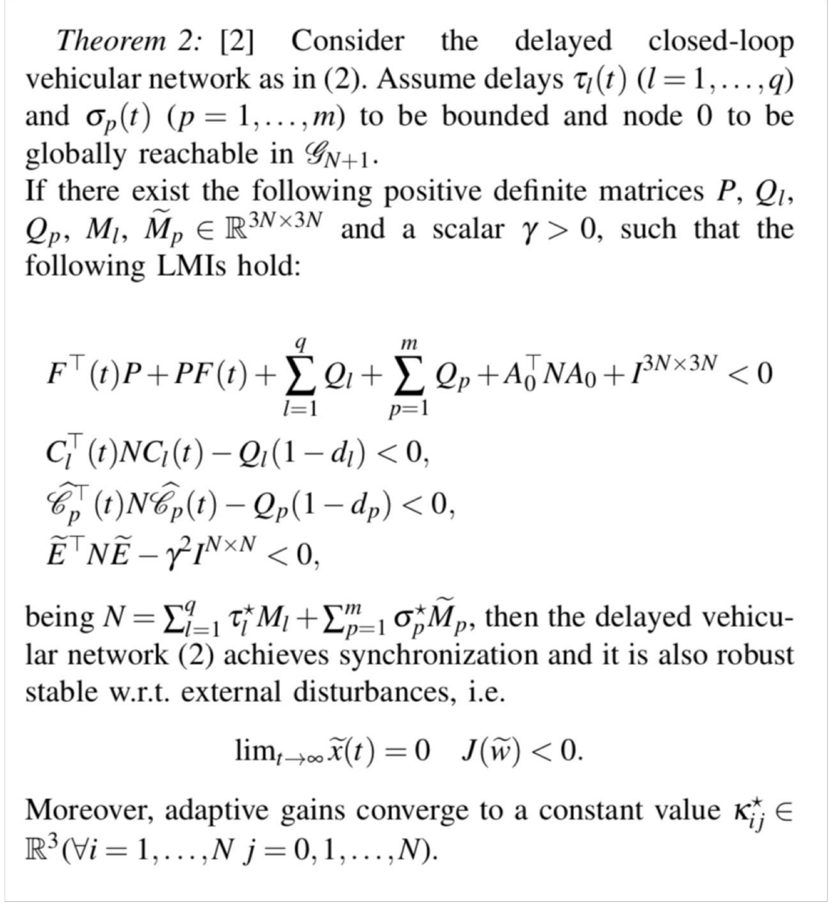
$$\boxed{\dot{\widetilde{x}}(t) = A_0\widetilde{x}(t) + \sum_{l=1}^{q} C_l(t)\widetilde{x}(t-\tau_l(t)) + \sum_{p=1}^{m} \widehat{\mathcal{C}}_p(t)\widetilde{x}(t-\sigma_p(t)) + \widetilde{E}\widetilde{w}(t)} \quad (2)$$

$$\widetilde{w}(t) = \left[\; w_1^\top(t),\; w_2^\top(t),\; \cdots,\; w_N^\top(t) \;\right]^\top \in \mathbb{R}^N$$

$$\widetilde{x}(t) = \left[\; e_1^\top(t),\; e_2^\top(t),\; \cdots,\; e_N^\top(t) \;\right]^\top \in \mathbb{R}^{3N}$$

Robust Stability conditions have to ensure both asymptotic stability and disturbances attenuation, i.e.

$$\lim\nolimits_{t\to\infty} \widetilde{x}(t) = 0$$
$$J(\widetilde{w}) = \int_0^t \widetilde{x}^\top(s)\widetilde{x}(s) - \gamma^2\widetilde{w}^\top(s)\widetilde{w}(s)ds < 0.$$



Theorem 2: [2] Consider the delayed closed-loop vehicular network as in (2). Assume delays $\tau_l(t)$ $(l = 1,\dots,q)$ and $\sigma_p(t)$ $(p = 1,\dots,m)$ to be bounded and node 0 to be globally reachable in $\mathcal{G}_{N+1}$.
If there exist the following positive definite matrices P, Q_l, Q_p, M_l, $\widetilde{M}_p \in \mathbb{R}^{3N\times 3N}$ and a scalar $\gamma > 0$, such that the following LMIs hold:

$$F^\top(t)P + PF(t) + \sum_{l=1}^{q} Q_l + \sum_{p=1}^{m} Q_p + A_0^\top N A_0 + I^{3N\times 3N} < 0$$
$$C_l^\top(t)NC_l(t) - Q_l(1-d_l) < 0,$$
$$\widehat{\mathcal{C}}_p^\top(t)N\widehat{\mathcal{C}}_p(t) - Q_p(1-d_p) < 0,$$
$$\widetilde{E}^\top N\widetilde{E} - \gamma^2 I^{N\times N} < 0,$$

being $N = \sum_{l=1}^{q} \tau_l^\star M_l + \sum_{p=1}^{m} \sigma_p^\star \widetilde{M}_p$, then the delayed vehicular network (2) achieves synchronization and it is also robust stable w.r.t. external disturbances, i.e.

$$\lim\nolimits_{t\to\infty} \widetilde{x}(t) = 0 \quad J(\widetilde{w}) < 0.$$

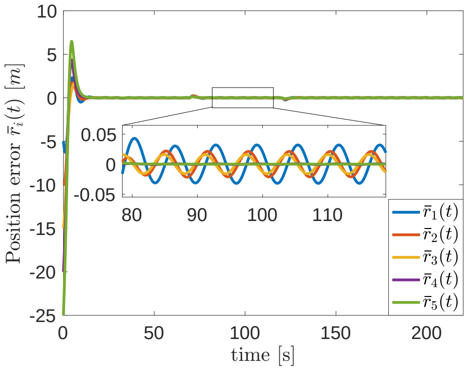
Moreover, adaptive gains converge to a constant value $\kappa_{ij}^\star \in \mathbb{R}^3 (\forall i = 1,\dots,N\ j = 0,1,\dots,N)$.

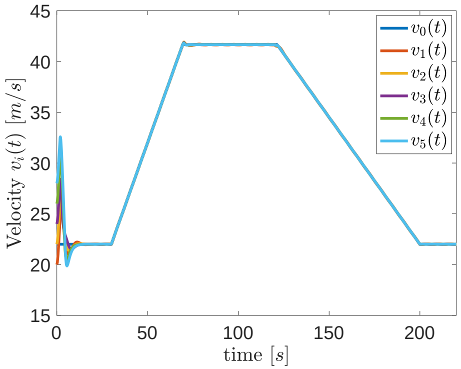
[1] Marco Di Vaio, Alberto Petrillo and Stefania Santini. "On the Robustness of a Distributed Adaptive Synchronization Protocol for Connected Autonomous Vehicles with Multiple Disturbances and Communication Delays". *57th IEEE Conference on Decision and Control (CDC).* Accepted.

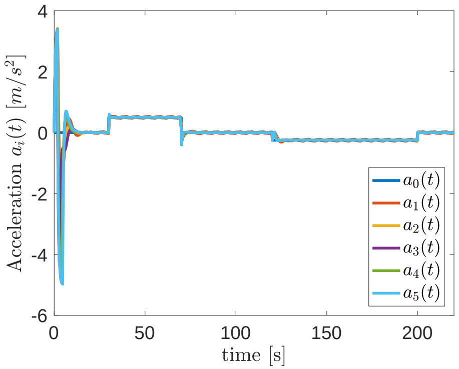
Robusteness w.r.t. External Disturances: Numerical Analysis

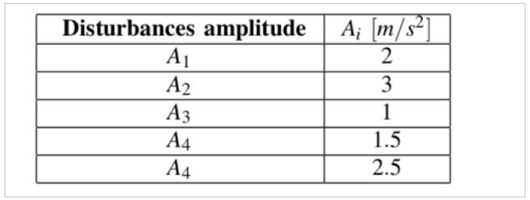
Consider an exemplar platoon of five vehicles plus a leader connected via L-P-F topology.

The leader travels following a trapezoidal speed profile and the dynamics of platoon members are affected by sinusoidal disturbances with different amplitudes, i.e. $w_i(t) = A_i \sin(t)$ for t ≥ 20 [s]

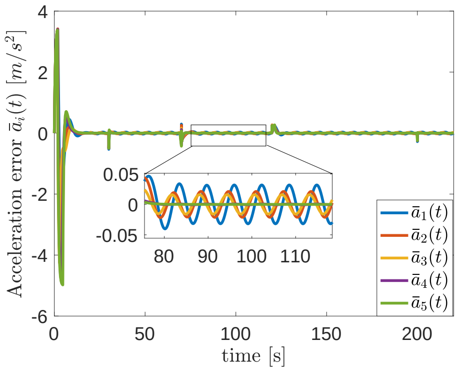


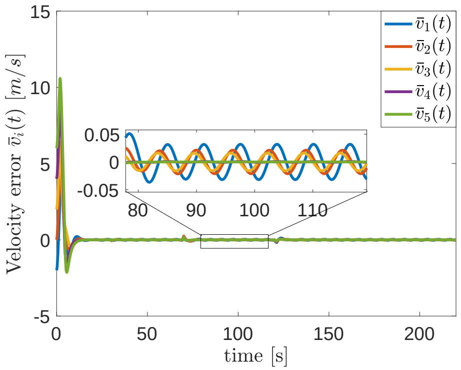


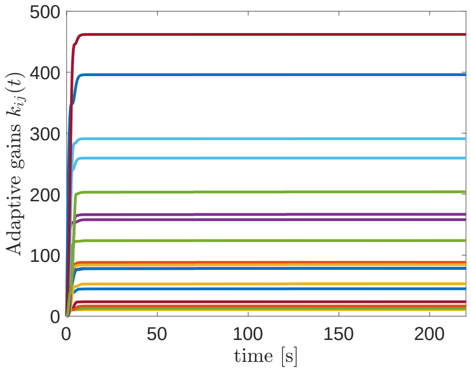




Disturbances amplitude	A_i $[m/s^2]$
A_1	2
A_2	3
A_3	1
A_4	1.5
A_4	2.5







Security in Vehicular Network

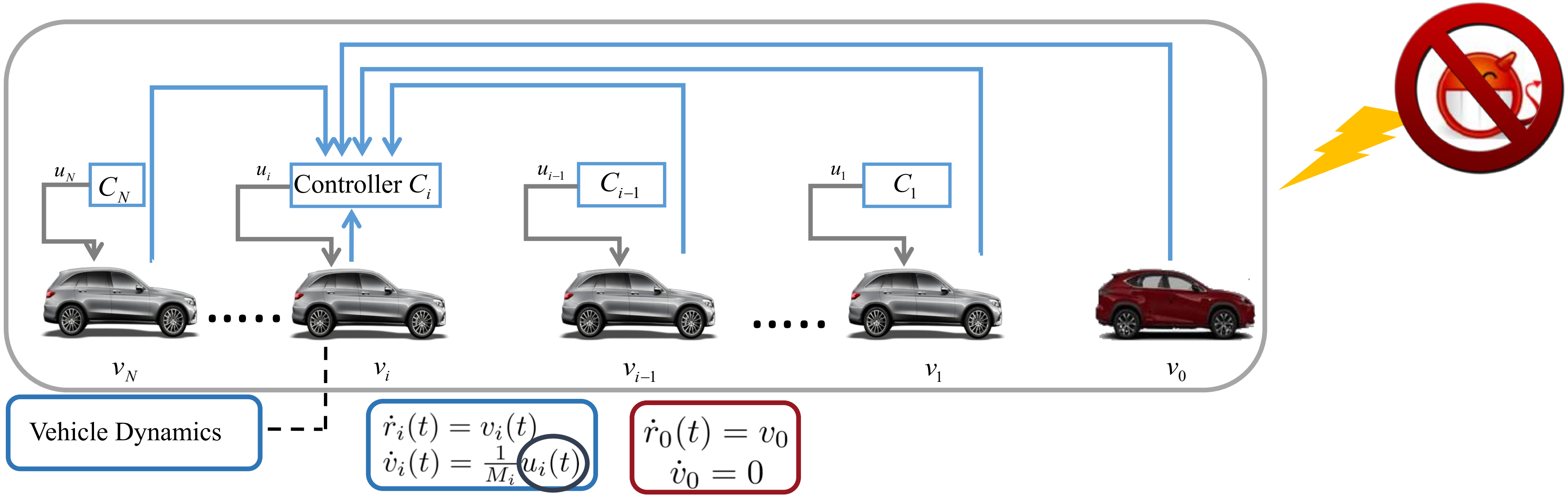
Vehicular networks can also suffer different security threats that compromise the correct functioning of platooning application and its safety.

We analyse the following security vulnerabilities:

1. Spoofing: an internal adversary takes the control of one vehicle within the fleet and imposes a constant offset to its current acceleration value from a given time instant.
2. Message Falsification: an adversary starts listening the messages wirelessly sent on networks and, after receiving each beacon, it tries to manipulate and to falsify the content of positions messages in order to rebroadcast them.
3. Denial-of-Service (DoS): an adversary overloads and overwhelms the communication capacity of one specific vehicle within the platoon in order to make them unable to exchange the necessary information for cooperative driving.
4. Burst Transmission: an internal adversary, tries to manipulate all the data traffic flow in order to disperse some beacons with a randomly loss rate.

Autonomous Vehicles Platoon Under Attacks

Let consider an autonomous platoon of N+1 vehicles travelling on a single lane and sharing information through a non reliable V2V wireless communication.



$$\dot{r}_i(t) = v_i(t)$$
$$\dot{v}_i(t) = \frac{1}{M_i} u_i(t)$$

$$\dot{r}_0(t) = v_0$$
$$\dot{v}_0 = 0$$

Our aim is to design a control strategy able to guarantee platoon formation while counteracting cyber attacks and network-induced phenomena.

Resilient Cooperative Control Strategy for Counteracting Cyber Attacks

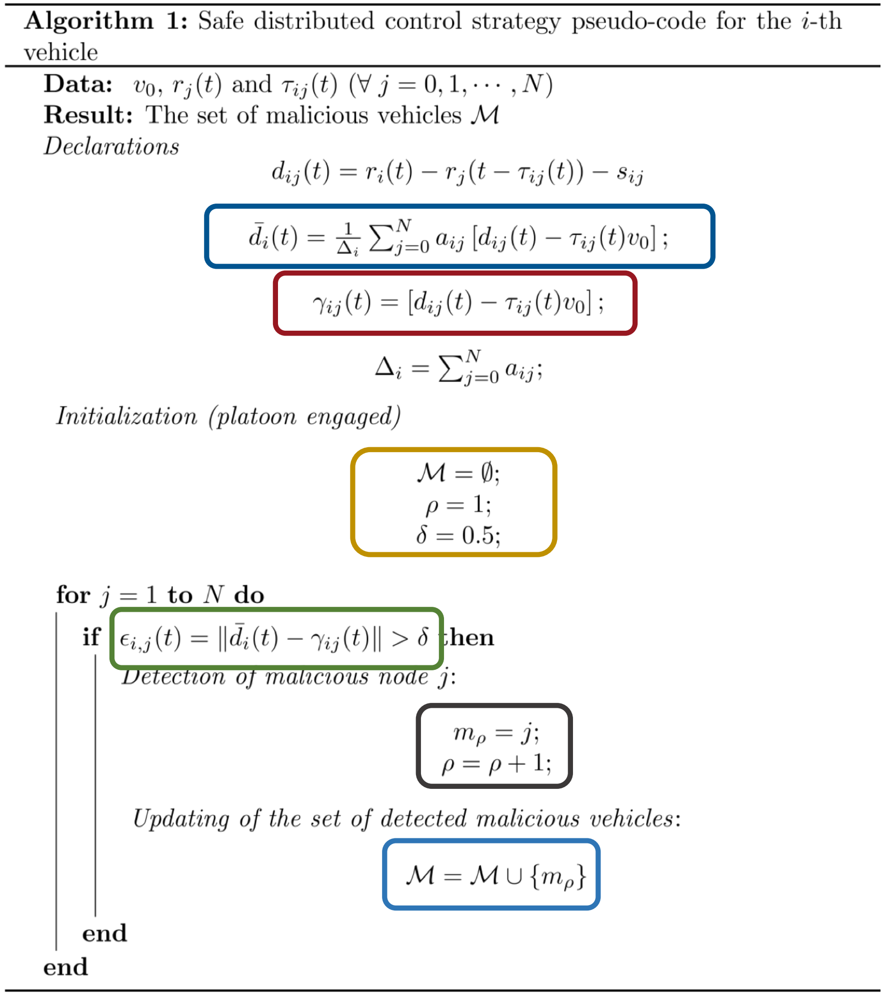
To counteract cyber attacks, here we exploit the cooperation features of one of the proposed control strategies for vehicles platoon control, as well as their ability to cope with time-delays. Namely:

1. a collaborative mechanism is embedded in the control strategies to detect and react to Spoofing and Message Falsification with the aim of discarding compromised information.
2. the intrinsic ability to react to communication time-varying delay is exploited for counteracting DoS and Burst and hence for somehow compensating the lack of information during the attacks.

$$\boxed{u_i(t) = -b\left[v_i(t) - v_0\right] - \frac{1}{\Delta_i}\sum_{\substack{j=0\\ j\notin\mathcal{M}}}^{N} k_{ij}\alpha_{ij}[d_{ij}(t) - \tau_{ij}(t)v_0]}$$

- Constant control gains $b\ , k_{ij} \forall i = 1, ..., N\ j = 0, 1, ..., N$
- Actual inter-vehicle distance $d_{ij}(t) = r_i(t) - r_j(t - \tau_{ij}(t)) - s_{ij}$
- Desired spacing policy s_{ij}

Collaborative Detection Algorithm



Algorithm 1: Safe distributed control strategy pseudo-code for the i-th vehicle

```
**Data:** $v_0$, $r_j(t)$ and $\tau_{ij}(t)$ $(\forall\, j = 0, 1, \cdots, N)$
**Result:** The set of malicious vehicles $\mathcal{M}$
*Declarations*
    $d_{ij}(t) = r_i(t) - r_j(t - \tau_{ij}(t)) - s_{ij}$
    $\boxed{\bar{d}_i(t) = \frac{1}{\Delta_i} \sum_{j=0}^{N} a_{ij}\left[d_{ij}(t) - \tau_{ij}(t) v_0\right];}$
    $\boxed{\gamma_{ij}(t) = \left[d_{ij}(t) - \tau_{ij}(t) v_0\right];}$
    $\Delta_i = \sum_{j=0}^{N} a_{ij};$
*Initialization (platoon engaged)*
    $\boxed{\mathcal{M} = \emptyset; \quad \rho = 1; \quad \delta = 0.5;}$
**for** $j = 1$ **to** $N$ **do**
    **if** $\boxed{\epsilon_{i,j}(t) = \|\bar{d}_i(t) - \gamma_{ij}(t)\| > \delta}$ **then**
        *Detection of malicious node $j$:*
            $\boxed{m_\rho = j; \quad \rho = \rho + 1;}$
        *Updating of the set of detected malicious vehicles:*
            $\boxed{\mathcal{M} = \mathcal{M} \cup \{m_\rho\}}$
    **end**
**end**
```

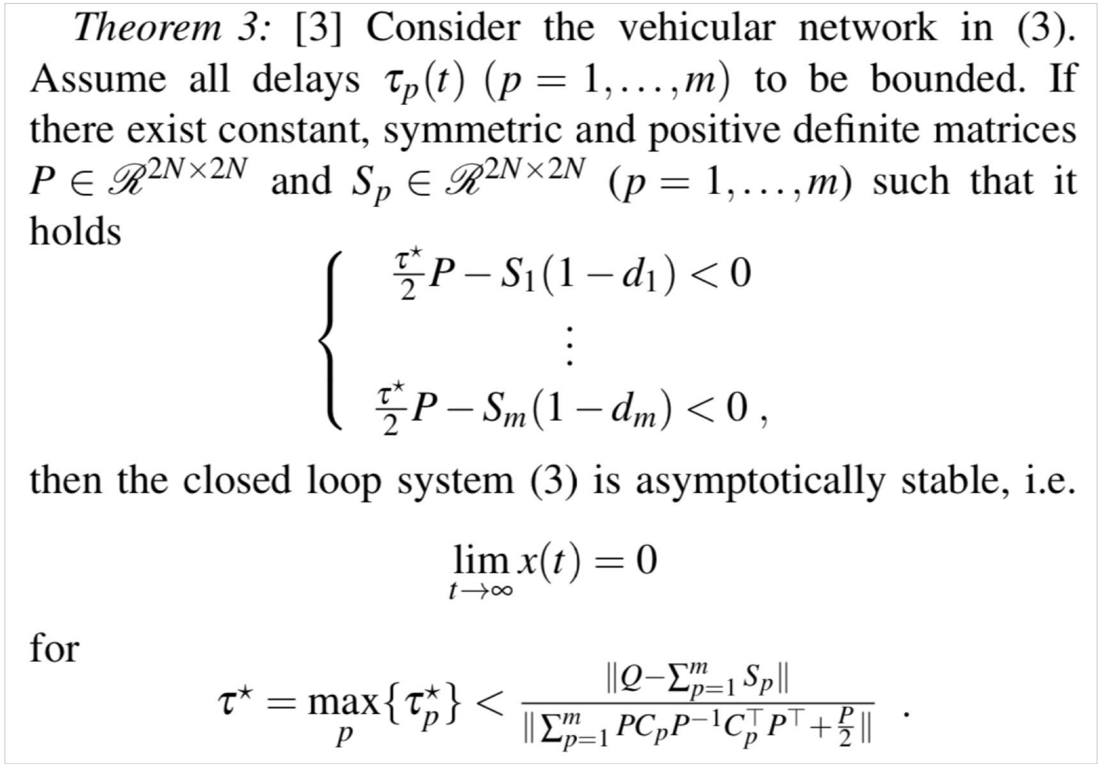
In order to update the set of malicious vehicles, each vehicle i, during travelling collects all the information sent by all vehicles in its communication range and:

1. **constructs a belief about the average distance;**
2. **computes the actual inter-vehicle distance;**
3. **initializes the initial condition for the set of malicious vehicle, the value for the threshold and an index variable;**
4. **computes the difference between the actual distance and the belief;**
5. **detects the malicious vehicle j if the difference is grater than the threshold;**
6. **isolates the malicious vehicle discarding the malicious information.**

Resilient Cooperative Control Strategy: Stability Analysis

- **The closed-loop dynamics is:**

$$\boxed{\dot{\bar{x}}(t) = A_0\bar{x}(t) + \sum_{p=1}^{m} A_p\left(\bar{x}(t-\tau_p(t))\right)} \quad \textit{(3)}$$



Theorem 3: [3] Consider the vehicular network in (3). Assume all delays $\tau_p(t)$ $(p = 1,\dots,m)$ to be bounded. If there exist constant, symmetric and positive definite matrices $P \in \mathscr{R}^{2N\times 2N}$ and $S_p \in \mathscr{R}^{2N\times 2N}$ $(p = 1,\dots,m)$ such that it holds

$$\begin{cases} \frac{\tau^\star}{2}P - S_1(1-d_1) < 0 \\ \vdots \\ \frac{\tau^\star}{2}P - S_m(1-d_m) < 0\,, \end{cases}$$

then the closed loop system (3) is asymptotically stable, i.e.

$$\lim_{t\to\infty} x(t) = 0$$

for

$$\tau^\star = \max_p\{\tau_p^\star\} < \frac{\|Q - \sum_{p=1}^m S_p\|}{\|\sum_{p=1}^m PC_pP^{-1}C_p^\top P^\top + \frac{P}{2}\|}\ .$$

[3] Petrillo, Alberto, Antonio Pescapé, and Stefania Santini. "A collaborative approach for improving the security of vehicular scenarios: The case of platooning." Computer Communications122 (2018): 59-75.

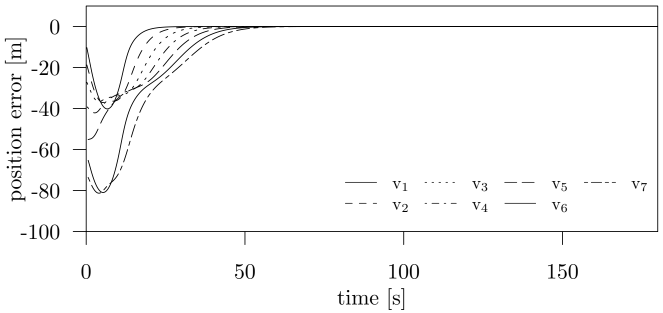
Resilient cooperative control strategy: Numerical Analysis

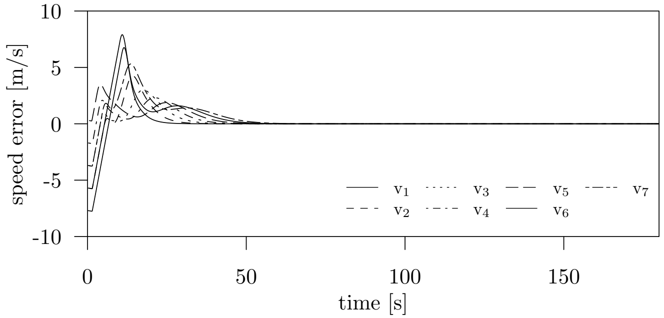
We consider a platoon composed of 7 vehicles plus a leader that travels on a single lane and share information via a non-reliable communication network.

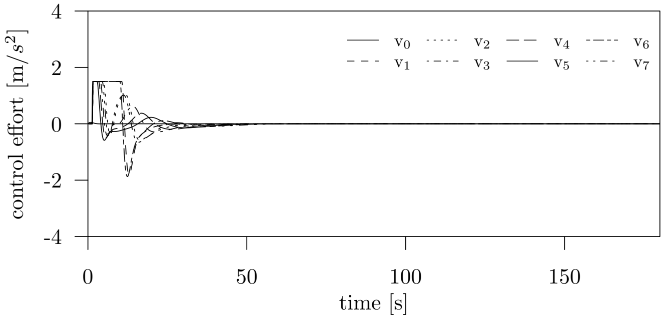
The exemplar analysis has been carried out for maintaining tight formation manoeuvre where the platoon has to reach and maintain the reference leader speed while maintaining the desired spacing policy.

The analysis is conducted for different communication topologies.

- Nominal Behaviour: Without Attacks



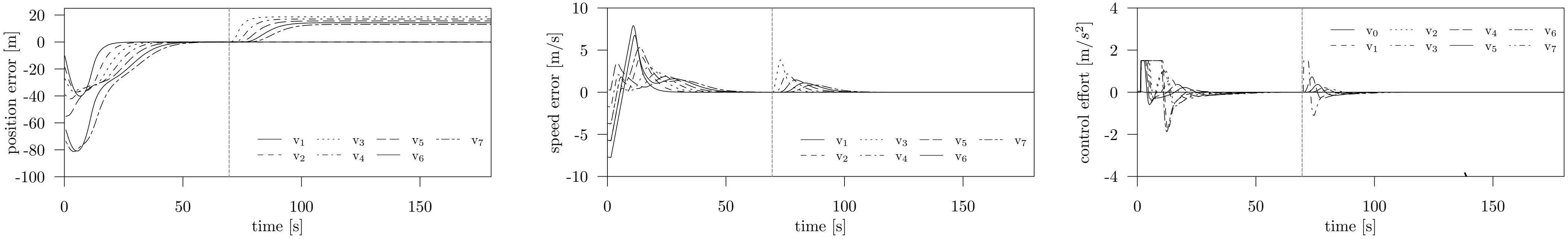




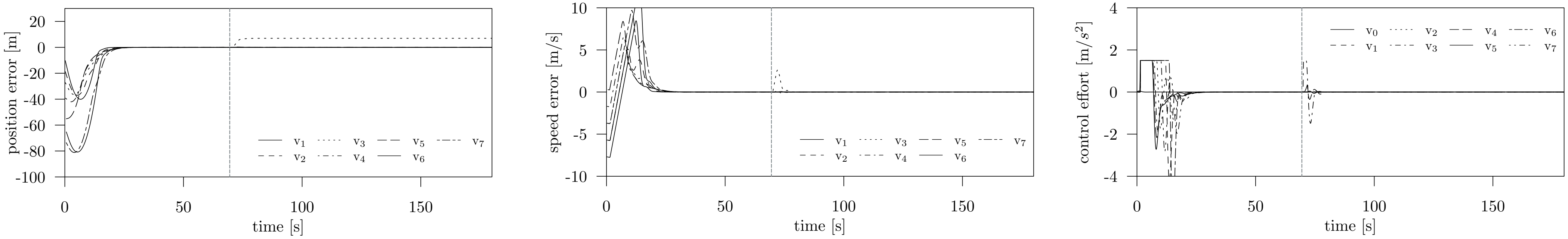
Numerical Analysis: Spoofing attack

The internal adversary takes the control of the third vehicle and imposes a constant offset of 3.5 [m/s^2] to its current acceleration value from t >70 [s].

- **Spoofing attacks effects: Mitigation mechanism is disabled**



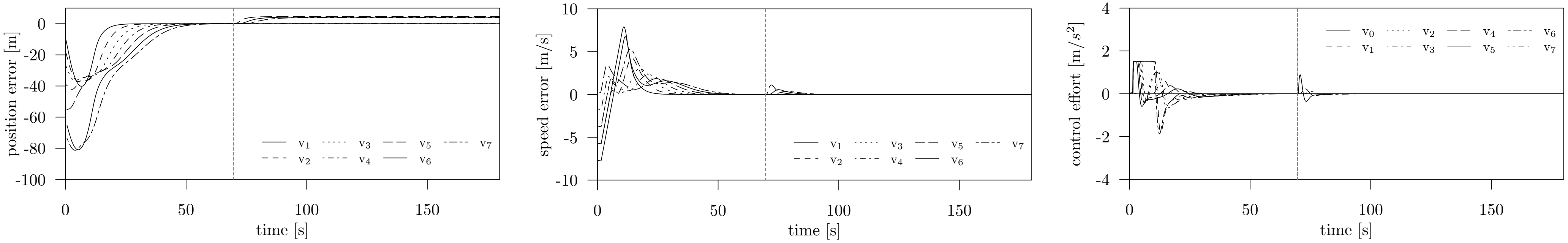
- **Spoofing attack mitigation**



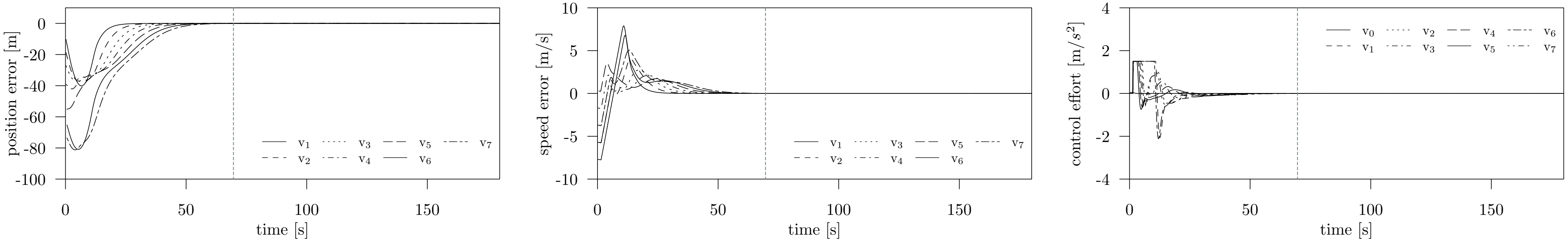
Numerical Analysis: Message Falsification attack

The internal adversary attacks the fourth vehicle and manipulates the position field of the beacons to be sent by adding a value of +5 [m] to its current position value from t >70 [s].

- **Message Falsification effects: Mitigation mechanism is disabled**



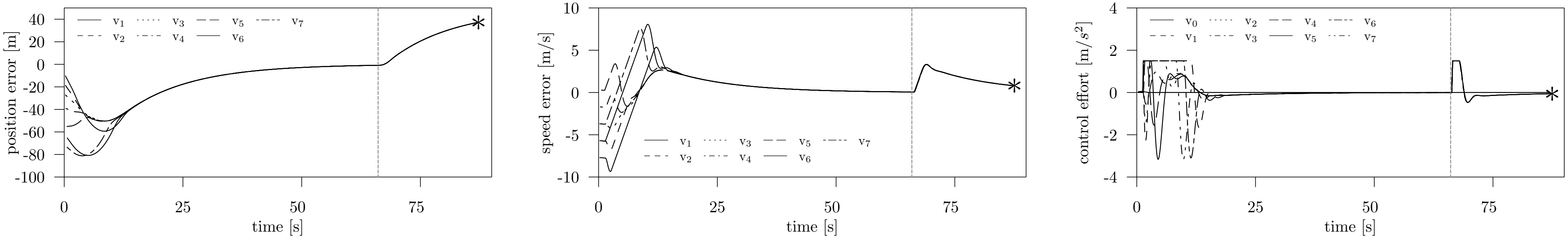
- **Message Falsification mitigation**



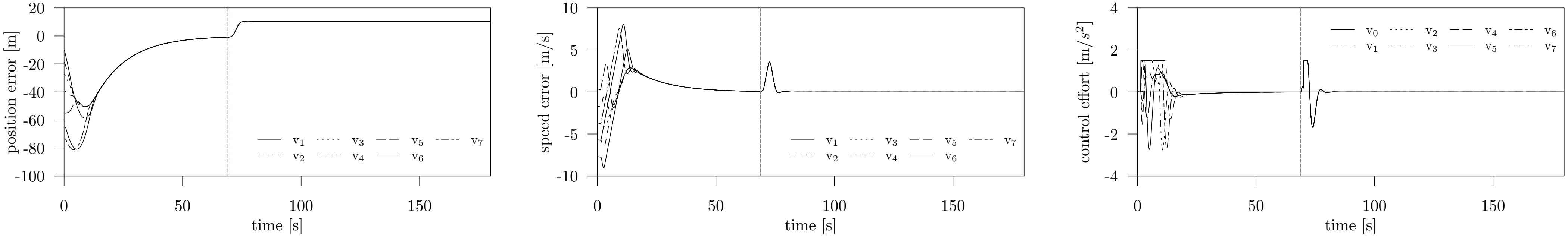
Numerical Analysis: special case of Spoofing Attack on the whole vehicles within the platoon

The internal adversary begins a spoofing attacks on all vehicles within the platoon from t >70 [s].

- **Spoofing effect: Mitigation mechanism is disabled**

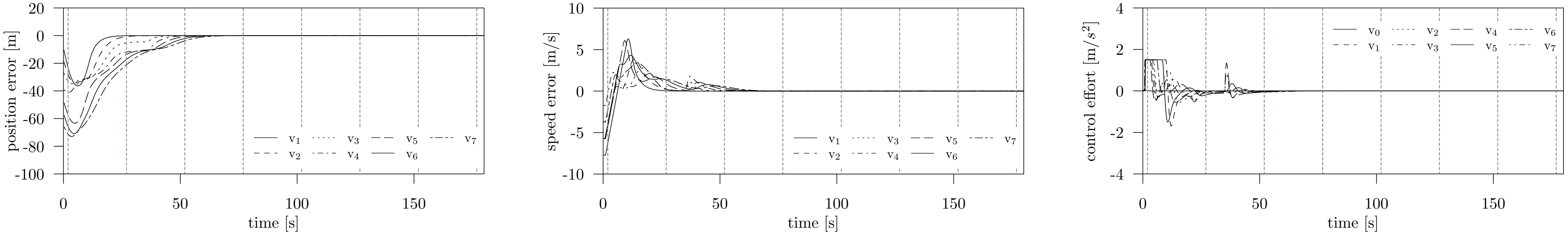


- **Spoofing mitigation**

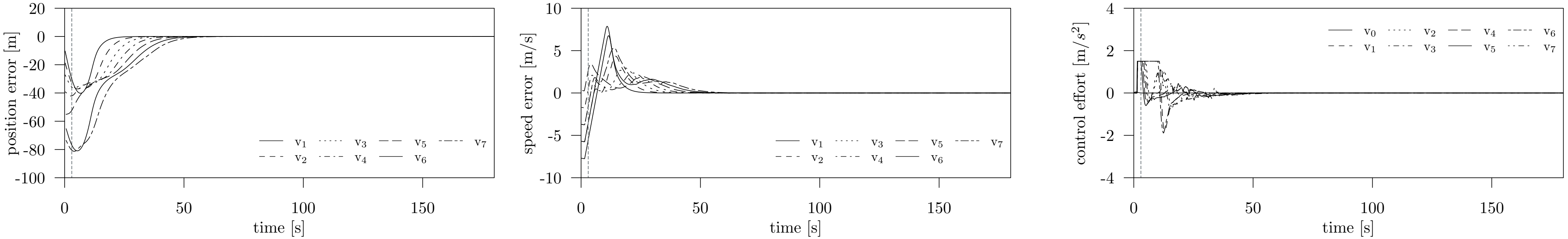


Numerical Analysis: DoS and Burst Attacks

- **DoS: the third vehicle gets only the 70% of the exchanged information among vehicles t=2[s] every 25 [s].**

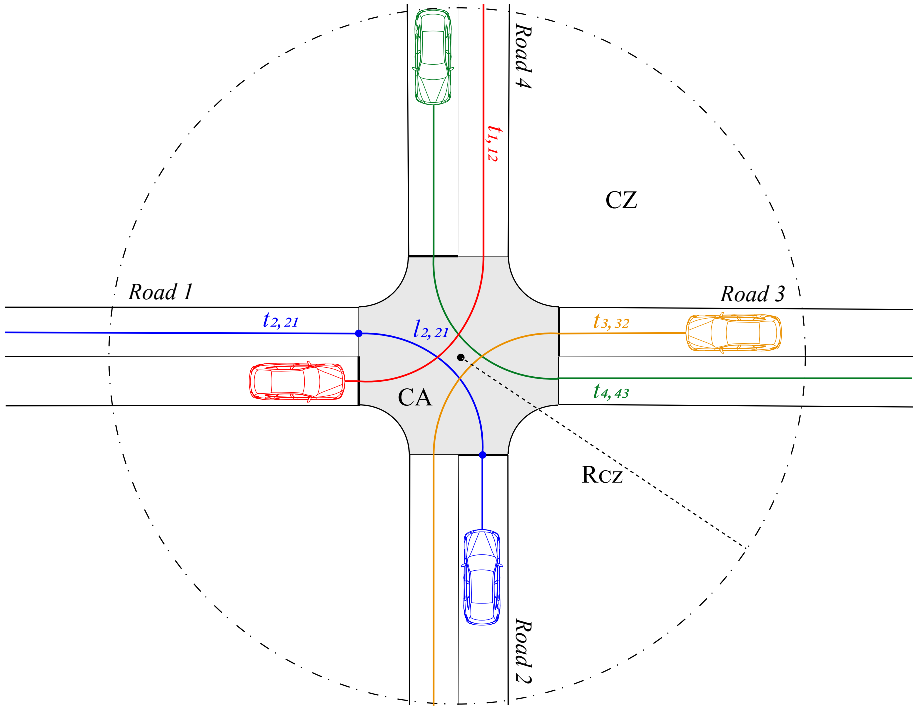


- **Burst: the adversary disperses all the packets exchanged among vehicles with a loss rate that randomly varies between 40% and 60% from t=2.**



Cooperative driving at traffic junction

Let consider N vehicles autonomously driving along different two-lane roads leading into a traffic junction, regulated neither by traffic lights or ordinary traffic rules.



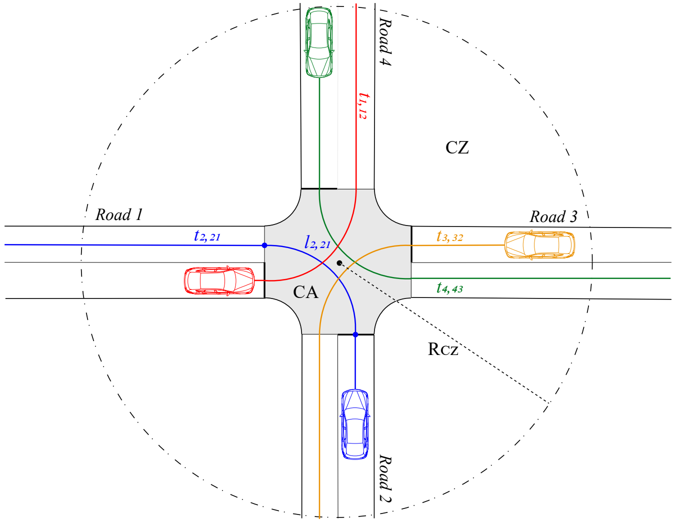
- Conflicting Area (CA) is the intersection core area where collisions could occur.
- Cooperation Zone (CZ) is the area in which vehicles exchange information about their state information

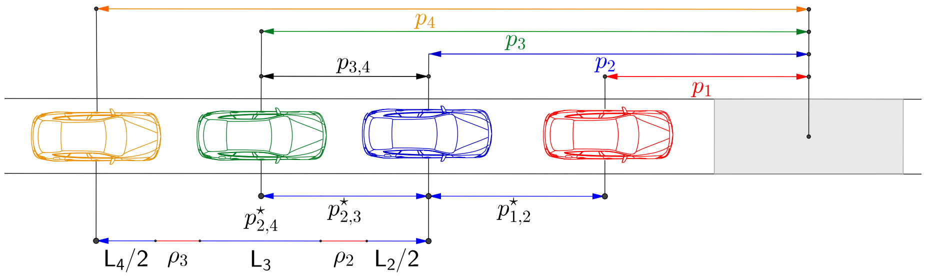
The aim is:

i. to regulate the motion of each vehicle so to cross the CA in mutually exclusive way, hence avoiding collisions;

ii. to guarantee the safe crossing despite communication impairments.

Cooperative driving at traffic junction as Virtual Platoon





- **Vehicles approaching a traffic junction can be organized as a virtual platoon.**
- **Vehicles within the platoon are ordered on the basis of their position w.r.t. CA, i.e. $p_i(t)$.**
- **The vehicles ordering corresponds to a crossing order, so that the closest vehicle crosses first.**
- **Collisions are prevented by imposing a desired spacing policy within the virtual formation and a common velocity.**
- **Each vehicle is described by the following dynamical systems:**

$$\begin{aligned}\dot{r}_i(t) &= v_i(t)\\ \dot{v}_i(t) &= \frac{1}{M_i}u_i(t)\end{aligned}$$

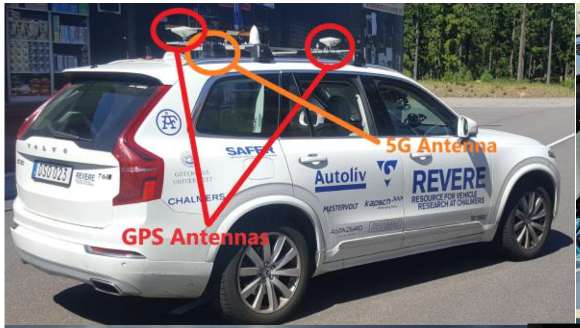
Cooperative driving control strategy at traffic junction

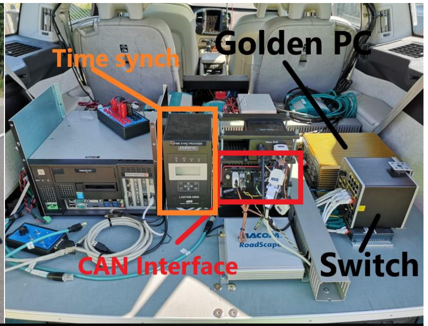
For safety reason, we propose a nonlinear finite-time control strategy so that formation is guaranteed before the first vehicle access the CA:

$$\boxed{u_i(t) = -\sum_{j=1}^{N} a_{ij} sig(p_i(t-\tau_{ij}(t)) - p_j(t-\tau_{ij}(t)) - p_{ij}^{\star})^{\frac{2\alpha}{1+\alpha}} - \sum_{j=1}^{N} a_{ij} sig(v_i(t-\tau_{ij}(t)) - v_j(t-\tau_{ij}(t)))^{\alpha}}$$

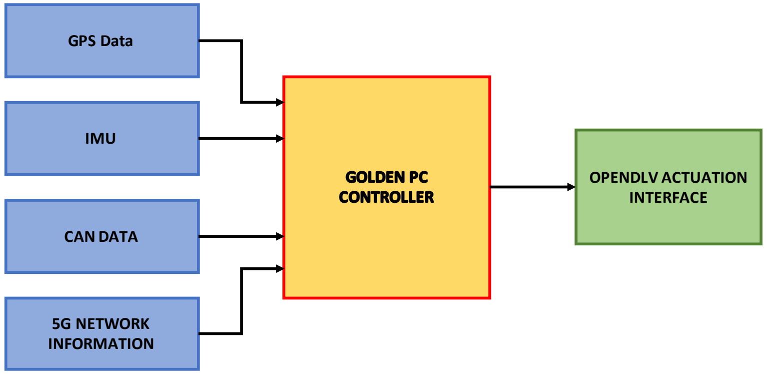
- ***Sig*** **Function** $sig(x)^{\alpha} = sign(x)|x|^{\alpha}$
- **Communication time-varying delay** $\tau_{ij}(t)$
- **Network topology** a_{ij}
- **Desired spacing between each pair of vehicles** $p_{ij}^{\star}$
- **Control gains** α

Cooperative driving at traffic junction via 5G Communication Network: Experimental Validation Setup





3 autonomous vehicles are exploited: 1) Volvo Car XC90; 2) Volvo Car S90; 3) Volvo Truck FH16.



GPS Data

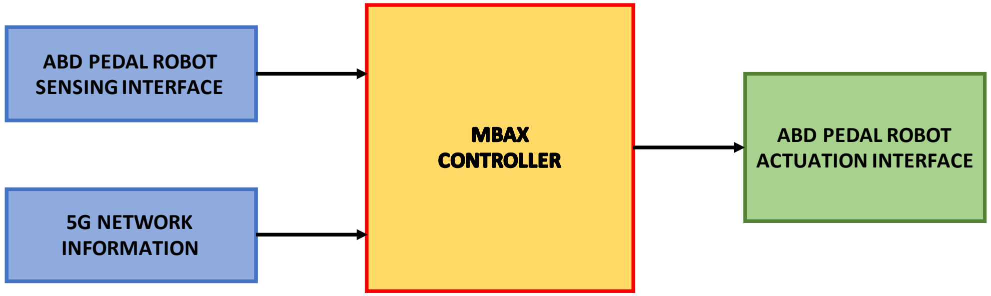
IMU

CAN DATA

5G NETWORK INFORMATION

GOLDEN PC CONTROLLER

OPENDLV ACTUATION INTERFACE

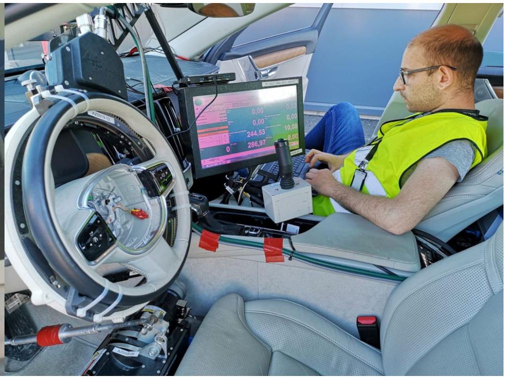


ABD PEDAL ROBOT SENSING INTERFACE

5G NETWORK INFORMATION

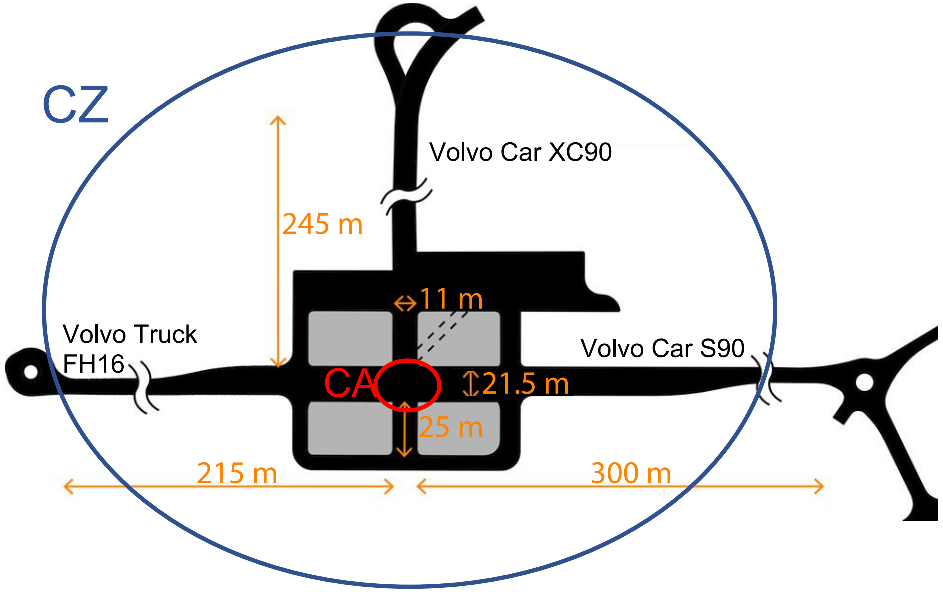
MBAX CONTROLLER

ABD PEDAL ROBOT ACTUATION INTERFACE



Cooperative driving at traffic junction via 5G Communication Network: Experimental results

Experimental tests have been carried out at AstaZero Test Track (near Gothenburg, Sweden), in the city Area, in collaboration with Chalmers University of Technology and Ericsson



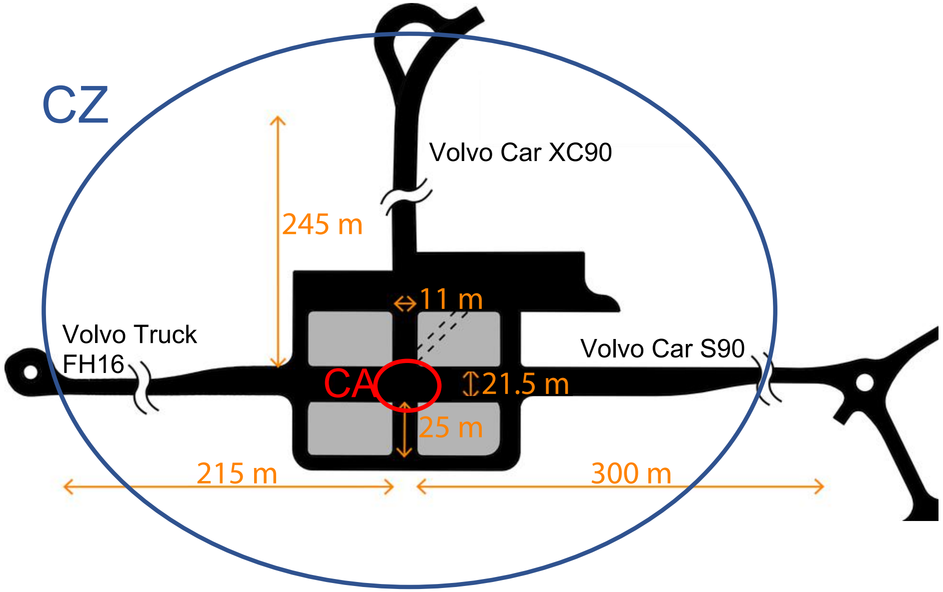
CHALMERS UNIVERSITY OF TECHNOLOGY

Alberto Petrillo

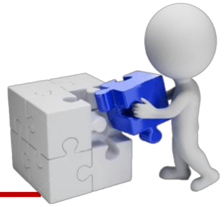
ERICSSON

Cooperative driving at traffic junction via 5G Communication Network: Experimental results

Experimental tests have been carried out at AstaZero Test Track (near Gothenburg, Sweden), in the city Area, in collaboration with Chalmers University of Technology and Ericsson



Conclusions



- During my PhD, I have have focused my attention on two open control problems both in cooperative driving application literature and in the general context of networked control systems:
  1. to design distributed cooperative control algorithms able to cope with multiple time-varying communication delays and packet losses;
  2. to design resilient secure distributed control algorithms able to counteract both security vulnerabilities and time-delays.
- To address the challenge 1 we propose:
  - i. adaptive synchronization-based controller;
  - ii. nonlinear finite-time controller.
- To address the challenge 2 we propose:
  - i. a novel distributed collaborative consensus-based strategy leveraging a mitigation mechanism of security vulnerabilities.
- Analytical, numerical and experimental results have confirmed the effectiveness of the proposed control strategies.

Products

Journal Papers

[1]Alberto Petrillo, Alessandro Salvi, Stefania Santini, Antonio Saverio Valente, Petrillo. Adaptive synchronization of linear multi-agent systems with time-varying multiple delays. *Journal of the Franklin Institute*, *354*(18), 8586-8605.

[2]Alberto Petrillo, Alessandro Salvi, Stefania Santini, Antonio Saverio Valente. “Adaptive multi-agents synchronization for collaborative driving of autonomous vehicles with multiple communication delays”. *Transportation research part C: emerging technologies*, *86*, 372-392.

[3]Alberto Petrillo, Antonio Pescapé and Stefania Santini. “A collaborative approach for improving the security of vehicular scenarios: The case of platooning”. *Computer Communications*, *122*, 59-75.

Conference Papers

[1]Giovanni Fiengo, Alberto Petrillo, Alessandro Salvi, Stefania Santini and Manuela Tufo, "A control strategy for reducing traffic waves in delayed vehicular networks." *55th IEEE Conference on Decision and Control (CDC), 2016*. IEEE, 2016.

[2]Alberto Petrillo, Antonio Pescapé and Stefania Santini. "A collaborative control strategy for platoons of autonomous vehicles in the presence of message falsification attacks." *5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS).*IEEE, 2017.

[3]Marco Di Vaio, Guido Guizzi, Alberto Petrillo and Stefania Santini. “Fleets Management of Cooperative Connected Automated Vehicles in Manufacturing Processes.” CIISE 2017 -Conferenza INCOSE Italia su Systems Engineering 2017.

[4] Giovanni Fiengo, Dario Giuseppe Lui, Alberto Petrillo, Stefania Santini and Manuela Tufo. “Distributed Leader-Tracking for Autonomous Connected Vehicles in Presence of Input Time-Varying Delay”. *26th Mediterranean Conference on Control and Automation (MED)*. IEEE,2018.

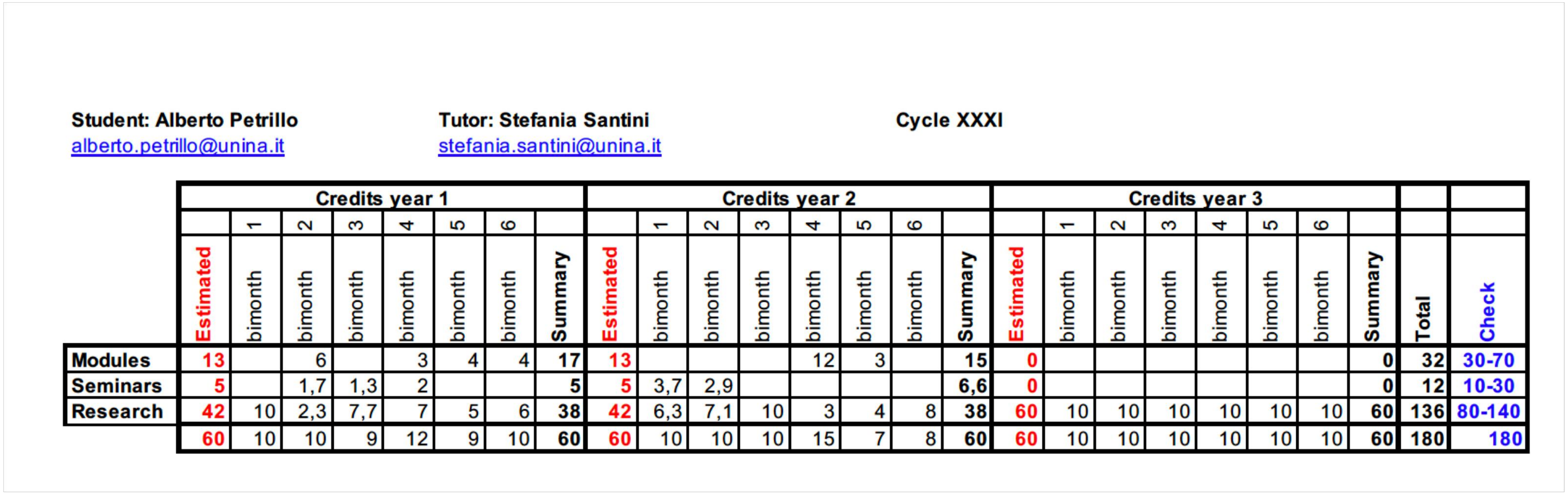
[5] Marco Amodeo, Marco Di Vaio, Alberto Petrillo, Alessandro Salvi, Stefania Santini. “Optimization of fuel consumption and battery life cycle in a fleet of Connected Hybrid Electric Vehicles via Distributed Nonlinear Model Predictive Control”. *European Control Conference (ECC) 2018.* To appear.

[6] Marco Di Vaio, Alberto Petrillo and Stefania Santini. “On the Robustness of a Distributed Adaptive Synchronization Protocol for Connected Autonomous Vehicles with Multiple Disturbances and Communication Delays”. *57th IEEE Conference on Decision and Control (CDC).* Accepted.

[7] Diego Iannuzzi, Stefania Santini, Alberto Petrillo and Procolo Ivan Borrino. “Design Optimization of Electric Kart for Racing Sport Application”. *5th ESARS-ITEC*.IEEE 2018. Accepted.

[8] Francesco Flammini, Stefano Marrone, Roberto Nardone, Valeria Vittorini, Stefania Santini and Alberto Petrillo. “Towards Railway Virtual Coupling”. *5th ESARS-ITEC*.IEEE 2018. Accepted.

PhD Activity



Student: Alberto Petrillo
alberto.petrillo@unina.it

Tutor: Stefania Santini
stefania.santini@unina.it

Cycle XXXI

	Credits year 1								Credits year 2								Credits year 3									
		1	2	3	4	5	6			1	2	3	4	5	6			1	2	3	4	5	6			
	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary	Total	Check
Modules	13		6		3	4	4	17	13				12	3		15	0							0	32	30-70
Seminars	5		1,7	1,3	2			5	5	3,7	2,9					6,6	0							0	12	10-30
Research	42	10	2,3	7,7	7	5	6	38	42	6,3	7,1	10	3	4	8	38	60	10	10	10	10	10	10	60	136	80-140
	60	10	10	9	12	9	10	60	60	10	10	10	15	7	8	60	60	10	10	10	10	10	10	60	180	180

Thank you!

alberto.petrillo@unina.it