Alberto Petrillo

Tutor: Stefania Santini

XXXI Cycle - II year presentation

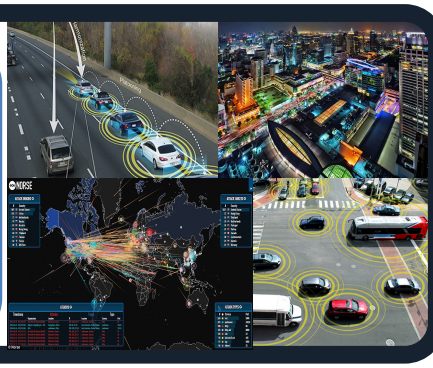
Cooperative Synchronization of multi-agent systems in presence of multiple communication time-varying delays: theory and applications

RESEARCH TOPIC

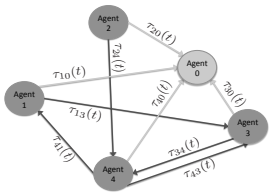
- Distributed Cooperative control for multi-agent systems in presence of communication impairments, such as multiple time-varying delays, packet losses and network vulnerabilities.
- Application of these control approaches to Intelligent Transportation System (ITS), e.g. autonomous ground vehicles in urban and extra-urban scenario, smart crossroads, smart cities, communication infrastructures, cloud vehicular networks and their cybersecurity.

MOTIVATIONS

- Collaborative Control of agents, sharing information through communication links (wired or wireless), is usually solved by assuming the communication network reliable, e.g. neglecting delays and security vulnerabilities.
- The aim of the research is designing secure control strategies that ensure the synchronization of all agent to a leader agent and that are resilient with respect to communication impairments arising in real communication networks.
- The idea is to tailor the theoretical results also with respect to some innovative ITS applications.



MULTI-AGENT SYSTEMS



- Each generic agent *i* is modelled as a LTI dynamical system:

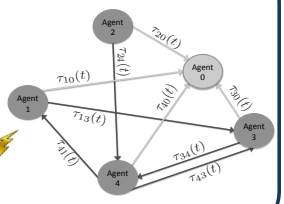
$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t, \tau_{ij}(t))$$
$$x_i(t) \in \mathbb{R}^N$$

- Each communication link is affected by its time-varying delays:

$$\tau_{ij}(t)$$

CYBER SECURITY VULNERABILITIES: MESSAGE FALSIFICATION ATTACKS

- An adversary listens to the messages wirelessly sent by a specific agent *i* on the communication network.
- After receiving each beacon, at $t = \bar{t}$, it manipulates and falsifies the content messages (by adding $\bar{x}_i$) in order to rebroadcast them.



$$t_{attack} = \bar{t}\ [s]$$
$$x_i(t) = x_i(t) + \bar{x}_i$$

PROPOSED SOLUTION

Algorithm 1: Distributed Resilient Adaptive Control

Data: Neighbors Information $x_j(t - \tau_{ij}(t))$
Result: Control Input $u_i(t - \tau_{ij}(t))$
Declarations

$$\varphi_{ij}(t) = [x_i(t - \tau_{ij}(t)) - x_j(t - \tau_{ij}(t))]; \quad \Delta_i = \sum_{j=0}^{N} \alpha_{ij};$$

$$\theta_i(t) = \frac{1}{\Delta_i} \sum_{j=0}^{N} \alpha_{ij}\varphi_{ij}(t).$$

Initialization $\mathcal{M} = \emptyset; \quad \eta = 1; \quad \delta = 0.5.$

Distributed Detection mechanism of malicious information and Updating of the malicious agents set $\mathcal{M}$

for $j = 0$ **to** N **do**
  Generate $\epsilon_{i,j}(t) = \|\theta_i(t) - \varphi_{ij}(t)\|$
  if $\exists k : \epsilon_{i,k}(t) > \delta$ *and* $\epsilon_{i,j}(t) < \delta\ \forall j \neq k$ **then**
    k *is malicious agent*:

$$m_\eta = k;$$
$$\eta = \eta + 1;$$

    Updating of the set of detected malicious agents:

$$\mathcal{M} = \mathcal{M} \cup \{m_\eta\}$$

  else if $\epsilon_{i,j}(t) < \delta\ \forall j$ **then**
    There is no malicious node in the communication network.
end

Computation of the control input $u_i(t, \tau_{ij}(t))$

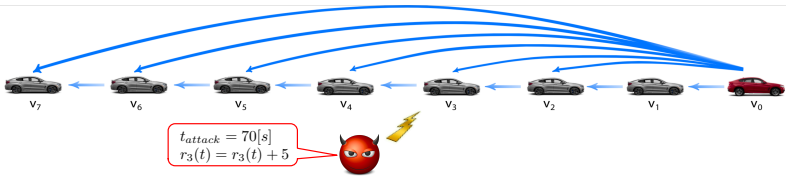
$$u_i = -\sum_{\substack{j=0 \\ j \notin \mathcal{M}}}^{N} \alpha_{ij}\kappa_{ij}^{\top}(t)\left(x_i(t - \tau_{ij}(t)) - x_j(t - \tau_{ij}(t))\right),$$

$$\kappa_{ij}(t) = [\kappa_{ij,1}(t),\ \kappa_{ij,2}(t);\ \cdots\ ;\ \kappa_{ij,n}(t)]^{\top},$$

$$\dot{\kappa}_{ij,k}(t) = \zeta_{ij,k}|x_{i,k}(t - \tau_{ij}(t)) - x_{j,k}(t - \tau_{ij}(t))|^2$$

PLATOONING APPLICATION

- Let consider a platoon of 7 vehicles plus a leader (vehicle 0) imposing the reference behaviour for the ensemble in presence of message falsification attack and communication impairments.
- The aim is to guarantee that each vehicle tracks the leader speed of *20 [m/s]*, while preserving a desired inter-vehicle distance of *15 [m]*.



$$t_{attack} = 70[s]$$
$$r_3(t) = r_3(t) + 5$$

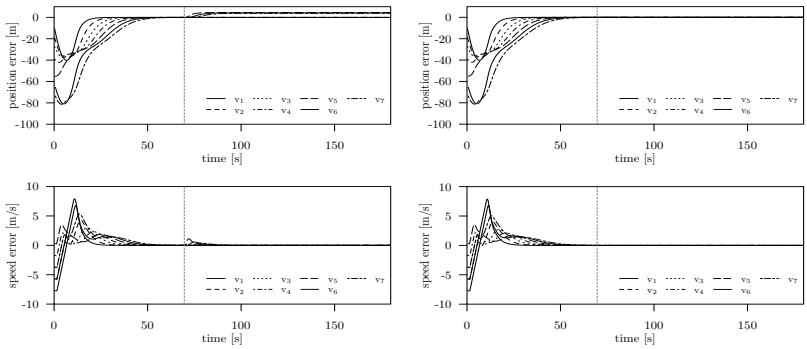


Fig. 1: Effects of message falsification attack in nominal conditions. The malicious attack begins at t = 70 [s] as highlighted by the vertical gray dash line.

Fig.2: Message falsification attack. The malicious attack begins at t = 70 [s] as highlighted by the vertical gray dash line.

FUTURE WORKS

- Extension of the analysis to other malicious cyber threats that may compromise the functionalities of communication networks.
- Design of robust controllers able to solve the synchronization problem also in presence of parameters uncertainties on the agent dynamical system.

REFERENCES

[1] Giovanni Fiengo, Alberto Petrillo, Alessandro Salvi, Stefania Santini and Manuela Tufo, "A control strategy for reducing traffic waves in delayed vehicular networks." *Decision and Control (CDC), 2016 IEEE 55th Conference on*. 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." *Models and Technologies for Intelligent Transportation Systems (MT-ITS), 2017 5th IEEE International Conference on*. IEEE, 2017.

[3] Alberto Petrillo, Alessandro Salvi, Stefania Santini, Antonio Saverio Valente, "Adaptive synchronization of linear multi-agent systems with time-varying multiple delays", Journal of the Franklin Institute (2017), doi: 10.1016/j.jfranklin.2017.10.015