Collaborative control strategy for connected autonomous vehicles in the presence of communication delays and cyber-attacks

Alberto Petrillo[1] and **Stefania Santini**[1,2]

[1] *Department of Electrical Engineering and Information Technology (DIETI), University of Naples Federico II, Italy (e-mail: alberto.petrillo,stefania.santini@unina.it)*
[2] *CNR - Italian National Research Council, Institute for Research on Engines (IM), Italy*

In recent years, Intelligent Transportation Systems (ITS) led to many benefits in terms of pollution and safety. In particular, it has been shown that the deployment of autonomous connected vehicles, moving in platoon formation and maintaining an optimal inter-vehicular spacing policy, may improve the traffic flow by increasing road capacity, by mitigating traffic congestion while decreasing pollutants emissions (Coelingh and Solyom, 2012; Wan et al., 2016). To achieve platooning via cooperative driving control strategies, vehicles need to communicate with each other through vehicular ad hoc networks (VANETs) and the IEEE 802.11p communication protocol is the de facto vehicular networking standard. For the safe and correct application functioning, cooperation among vehicles has to be based on reliable communication structure to avoid that any vehicle in formation collides with the vehicle ahead. However vehicular networks can suffer from the presence of unavoidable communication delay as well as from possible security threats affecting the application and network layers. Traditional security systems like encryption/decryption methods may be able to protect the connected vehicles from external malicious attacker (Al-Kahtani, 2012). However when the adversary is an insider member of the network, it possesses a valid recognition certificate. Thus the cryptographic system control is not enough to solve this cyber threat (Zhu et al., 2009).

In this latter case, the platooning control strategy design plays an important role in robustness and security issues. In fact, although information security has developed advanced technologies and tools that can prevent and react to attacks, security in control strategy design is important, since an opponent, attacking the cyber infrastructure, can interfere the normal operation of physical process (Guan et al., 2016). In order to make safer the platooning application, the possible cyber threats compromising the cooperative driving have to be taken into account in control protocol design. Motivated by this reason, in this work we design a collaborative, consensus-based, control strategy able to both counteract communication impairments, such as the usual time-varying communication delays, and mitigate the effects of cyber attacks on the platoon behavior. The proposed strategy is validated via PLEXE, a high-fidelity simulator that allows the platoon investigation by coupling vehicle dynamics with realistic wireless network simulations. A comprehensive analysis discloses the robustness of the proposed approach and its capabilities in reacting to the malicious attack effects.

[1] Al-Kahtani M. S., Survey on security attacks in vehicular ad hoc networks (vanets), *6th International Conference on Signal Processing and Communication Systems (ICSPCS), IEEE*, 1–9, 2012.
[2] Coelingh E., Solyom S., All aboard the robotic road train, *Spectrum, IEEE* **49**(11):34–39, 2012.
[3] Guan X., Yang B., Chen C., Dai W., Wang Y., A comprehensive overview of cyber-physical systems: from perspective of feedback system, *IEEE/CAA Journal of Automatica Sinica* **3**(1):1–14, 2016.

[4] Wan N., Vahidi A., Luckow A., Optimal speed advisory for connected vehicles in arterial roads and the impact on mixed traffic, *Transportation Research Part C: Emerging Technologies*, 2016.

[5] Zhu H., Lu R., Shen X., Lin X., Security in service-oriented vehicular networks, *Wireless Communications, IEEE* **16**(4):16–22, 2009.