Computer Communications 122 (2018) 59–75

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

A collaborative approach for improving the security of vehicular scenarios: The case of platooning

Alberto Petrillo[a], Antonio Pescapé[*,a], Stefania Santini[a,b]

[a] Department of Electrical Engineering and Information technologies (DIETI), University of Naples Federico II, Naples 80125, Italy
[b] CNR - Italian National Research Council, Institute for Research on Engines (IM), Naples 80125, Italy

ARTICLE INFO

Keywords:
Resilient control
Cyber-security control
V-2-X cyber security
Vehicular networks
Connected autonomous vehicles
Platooning

ABSTRACT

Autonomous vehicles platooning has received considerable attention in recent years, due to its potential to significantly benefit road transportation, improving traffic efficiency, enhancing road safety and reducing fuel consumption. The Vehicular ad hoc Networks and the de facto vehicular networking standard IEEE 802.11p communication protocol are key tools for the deployment of platooning applications, since the cooperation among vehicles is based on a reliable communication structure. However, vehicular networks can suffer different security threats. Indeed, in collaborative driving applications, the sudden appearance of a malicious attack can mainly compromise: (i) the correctness of data traffic flow on the vehicular network by sending malicious messages that alter the platoon formation and its coordinated motion; (ii) the safety of platooning application by altering vehicular network communication capability. In view of the fact that cyber attacks can lead to dangerous implications for the security of autonomous driving systems, it is fundamental to consider their effects on the behavior of the interconnected vehicles, and to try to limit them from the control design stage.

To this aim, in this work we focus on some relevant types of malicious threats that affect the platoon safety, i.e. application layer attacks (Spoofing and Message Falsification) and network layer attacks (Denial of Service and Burst Transmission), and we propose a novel collaborative control strategy for enhancing the protection level of autonomous platoons. The control protocol is designed and validated in both analytically and experimental way, for the appraised malicious attack scenarios and for different communication topology structures. The effectiveness of the proposed strategy is shown by using PLEXE, a state of the art inter-vehicular communications and mobility simulator that includes basic building blocks for platooning. A detailed experimental analysis discloses the robustness of the proposed approach and its capabilities in reacting to the malicious attack effects.

1. Introduction

In these years, it is has been shown that the deployment of platoons of autonomous vehicles may lead to many benefits: fuel efficiency increase, road safety improvement and travel duration, while decreasing traffic congestion, pollution, and stress for passengers [1]. Furthermore, platooning allows people to be more productive when traveling and offers greater mobility to more individuals.

To achieve platooning via autonomous cooperative driving, vehicles need to communicate with each other and this is made possible through vehicular ad hoc networks (VANETs) [2]. In these networks a cyber attack can lead to dangerous implication for safety, privacy and, moreover, for the public perception and consideration of vehicles platoon [3].

Therefore, the subject of this paper is the evaluation of network attacks on vehicles platoon and the development of a novel collaborative control strategy to cope with them.

Past studies on VANETs security vulnerabilities focus their attention on an accurate classification of malicious attacks and the solutions to mitigate them at communication level [4]. However, while security in sensing and communication has been extensively investigated in the technical literature, security in control has been recently indicated as a key ingredient that has to be added for enhancing the protection level of the normal operation of a physical process. Special attention has been recently raised with respect to control solutions for cyber-physical systems in vehicular networks, where the complexity of transportation systems, and of high mobility vehicular systems, pushes to find tailor-made solutions depending from the specific application, such as platooning (e.g. see [5,6]). Since security is a crucial point in platooning control system design, in this work we present a meticulous study on

* Corresponding author.
E-mail addresses: alberto.petrillo@unina.it (A. Petrillo), pescape@unina.it (A. Pescapé), stefania.santini@unina.it (S. Santini).

https://doi.org/10.1016/j.comcom.2018.03.014
Received 3 October 2016; Received in revised form 24 October 2017; Accepted 18 March 2018
Available online 22 March 2018
0140-3664/

platoon behavior when a cyber threat acts and we propose a distributed collaborative control strategy which is able to both counteract communication impairments, such as time-varying multiple delays, and to attenuate malicious effects on platoon behavior. The proposed distributed control approach also leverages a real-time voting technique to achieve the complete mitigation of some of the most critical effects due to malicious attacks.

This does not imply that we aim to substitute other solutions for security, such as the cryptographic ones [7] that work at the information level to avoid that the content of the information can be somehow altered. Our aim is to provide further countermeasures to detect, mitigate and, if possible, counteract cyber threats that may alter driving decision at control level so to help increasing the overall security of the ensemble of the connected vehicles.

The main contribution of this work is twofold. First, differently from literature, we propose a collaborative control strategy specifically designed to take into account cyber threats, as messages manipulation attacks and communication capability attacks. The proposed approach is, hence, able to guarantee the cooperative driving of the vehicles platoon in the presence of malicious attack on the communication network by promptly counteracting them. Furthermore, the closed-loop vehicular network is analytically derived and the effectiveness of the control algorithm is theoretically proven via the stability analysis.

Second, the proposed collaborative strategy is implemented in PLEXE [8], and we carry out a comprehensive experimental analysis with eight cars in a realistic highway (10 km long) considering different cyber attacks scenarios and different communication network topologies in which the leading vehicle is globally reachable. The communication delay in the control protocol, instead, is intrinsically modeled in Veins with a realistic communications device (IEEE 802.11p card) implementation [9]. The experimental analysis shows the main security vulnerabilities effects on the platoon motion and illustrates the robustness of the collaborative control strategy with respect to the most common malicious attacks.

The paper is structured as follows. In Section 2, the scenario under investigation, the motivation and the literature overview are presented. Then in Section 3, we present the closely related works to better illustrate the advantages of the proposed approach with respect to the state-of-the-art. In Section 4, after introducing the notation and the mathematical background, the problem statement and the control algorithm are formulated and mathematically described. The closed-loop delayed network is derived and its stability is then proven by providing the analytical conditions for convergence via a Lyapunov–Krasovskii approach. In Section 5, after describing the considered network/traffic scenario and attacks, we present the experimental results - including realistic features such as vehicles masses and inertia and actuation lags - and we show the performance and the robustness of the proposed approach in counteracting malicious threats, hence confirming the theoretical derivation. Finally, conclusions are drawn in Section 6.

2. Scenario and motivation

In this work, we consider an autonomous platoon of N vehicles traveling on a single lane and sharing information such as speed and position, through a non reliable V2V wireless communications, in order to achieve cooperative driving.

In literature, most studies on vehicles platooning focus their attention on the control strategy design [10–13] under the main assumption that the communication structure is reliable. However, similarly to other open and dynamic networks, vehicular ad hoc networks are affected by different security threats [14]. Countless studies on security issues in VANETs are presented in [7,15–19], where several tools, helpful in building a secure vehicular network, have been exposed. One of the most proposed solution consists in exploiting authentication/validation mechanism for the messages exchanged among vehicles in order to remove from communication network the adversary, disabling its communication capability. In addiction, the works [4,20,21] present an accurate categorization of all the possible malicious attacks on VANETs and of the eventual countermeasures allowing their prevention.

Although all these works discuss the cyber attacks implications and propose network layer countermeasures, none of them considers the effects of malicious attacks on vehicular networks of connected vehicles equipped with a longitudinal control. Only recently, the security vulnerabilities problem on vehicles platooning has been addressed in [5,6,22–28]. These works suggest how important is, in control protocol design, to take into account the eventual cyber attacks on vehicular platooning network in order to improve its safety.

Motivated by this reason, we focus our attention on different situations in which the correct communication among autonomous vehicles is compromised and, based on this analysis, we propose a novel distributed collaborative strategy that guarantees the platoon formation in adversarial environment and that allows to promptly react to malicious attacks.

We exploit the classic approach where the control design starts with a simplified model of the system to be controlled. A more accurate system model (as the one within PLEXE) is instead exploited in the simulation to test the effectiveness of the strategy with respect to disturbances, uncertainties, and realistic dynamics, of both the vehicles and the communication channel, that are not modeled during control design phase.

According to this methodology, in our analytical derivation the ensemble of the connected vehicles is represented as a dynamical multi-agent network [29] where each vehicle is a node of a graph and each link accounts for the presence of communication between two generic vehicles. In order to treat the effect of the vehicular networks, i.e. based on the IEEE 802.11p protocol, our mathematical framework considers that each communication link, that connects a pair of agents, is affected by a different time-delay that accounts for actual conditions, or possible impairments, of the communication channel. This implies that information can be received by each vehicle with a different time-varying delay and that the distributed collaborative control protocol leverages outdated information for driving the longitudinal motion of the platoon.

3. Related work

The literature on cyber attacks to vehicular networks is both wide and variegate. In this section, first we focus our attention on attacks to vehicular networks of interest for platooning, then we focus on countermeasures for this application scenario.

3.1. Malicious attacks to vehicular networks

In this section, we provide an overview of the most relevant types of malicious threats that may compromise the functionalities of cooperative driving systems (e.g., see [22,30,31] and references therein). Indeed, with respect to autonomous driving applications, a malicious node can affect: (i) the correct data traffic flow by sending malicious messages; (ii) the safety by altering vehicular network communication capability; (iii) the vehicle privacy by listening to legitimate messages. Before introducing different cyber security scenarios, we first define the adversary typology [32]. An adversary can be an insider, i.e. an authenticated member of the network possessing a certified public key, or an outsider, i.e. a network intruder. If the adversary does not get benefit from the attack, but it aims to harm the network members, it is said malicious, while it is defined rational if it seeks personal benefit. Furthermore, the adversary is defined active if it generates packet or signals, whereas it is defined passive if it realizes an eavesdropping attack.

In our vehicular scenario, application layer attacks affect the correct operating of the cooperative driving by altering the messages exchanged among vehicles to reach and maintain a common motion. Specifically, in a spoofing attack the adversary impersonates a vehicle,