Secure Autonomous Platooning with Hybrid Vehicular Communication

Susumu Ishihara
Graduate School of Engineering, Shizuoka University
3-5-1 Johoku, Hamamatsu, Japan

Vince Rabsatt and Mario Gerla
Computer Science Department, UCLA
Los Angeles, U.S.A.

I. Introduction

Autonomous platoon control is a promising auto drive technology. It frees drivers from stressful driving tasks and offers a comfortable car trip experience. It is also expected to contribute to energy savings. Fig. 1(a) shows a typical architecture of an autonomous platoon system based on inter-vehicular communication (IVC), or cooperative adaptive cruise control (CACC). In addition to the sensor-based autonomous cruise control, in which each vehicle controls its velocity according to the distance and velocity of its direct leading vehicle, vehicles have a function to control their velocity according to the information from the leader of the platoon and their direct preceding vehicle. Since autonomous platoon control depends on wireless communication, its performance and safety are strongly affected by the control of message exchange within the platoon. Segata et al. have shown that combined use of a slotted scheduling mechanism and transmit power control is highly beneficial in radio-based CACC systems through realistic IVC and vehicle movement simulations [1]. In addition to improving the performance of message exchange protocols in normal situations, prevention of attacks on wireless communications, such as forged messages and jamming, is crucial. In this poster, we propose a solution to mitigate the risk of a jamming attack in an autonomous platooning system.

II. Securing Autonomous Platooning Systems with Hybrid Vehicular Communication

If vehicles have omni-directional antenna to receive radio signals from surrounding vehicles, they are prone to receiving jamming signals from malicious hosts. For example, if a vehicle driving near a platoon sends some radio signals to jam the communication between the leader of the platoon and followers, the following vehicles cannot receive the message from the leader, e.g. emergency brake, and fail to control their velocity according to the message. Though some measures for jamming attacks have been proposed, the radio communication between the leader and followers can be attacked as long as radio is used for the wireless communication.

Light and high frequency radio signals (we refer to them simply as light afterward) have much sharper directivity compared with microwave used by IEEE802.11p. Thus, if physical communication interfaces with high directivity are used for control message exchange in a platoon, it will be difficult for a malicious host that is not in close proximity to the platoon, to jam the platoon control message exchange.

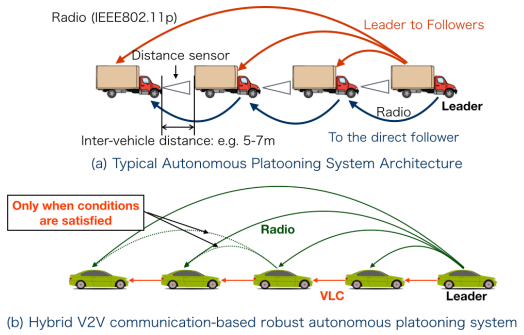

Fig. 1 VLC and Radio Hybrid Communication for Secure Autonomous Platoons

Recently, visible light communication technologies have been actively studied (e.g. [2]).

However, due to the sharp directivity, it is difficult to use light-based communication for direct communication between the leader of a platoon and followers other than the second vehicle. That is, light-based communication in a platoon has to be multi-hop. This leads long end-to-end delay.

To cover both shortcomings of light-based communication, delay, and radio-based communication, we propose a hybrid communication using both light and radio for autonomous platooning. As shown in Fig. 1(b), the leader vehicle sends its control message to its followers using both a visible light communication (VLC) interface and a radio interface. If a follower vehicle receives a new message from one of VLC and radio interfaces, it forwards the message to its direct follower via the VLC interface. However, if certain conditions are met, such as when the message delivery delay from the leader is larger than a specified threshold, the vehicle forwards the message via the radio interface as well. This operation is designed for shortening the end-to-end message delivery delay and improving the packet delivery ratio.

Currently, we are developing a simulation model of visible light communication that works with *Veins*, an IVC simulation platform. This model is used to estimate the performance of the proposed hybrid communication's robustness in preventing jamming attacks.

References

[1] M. Segata, et al., "Towards Inter-Vehicle Communication Strategies for Platooning Support," Nets4Cars 2014-Fall, pp.1–6, 2014.

[2] S-H Yu, et al., "Smart automotive lighting for vehicle safety," IEEE Comm. Mag. vol.51, no.12, pp.50–59, 2013.