Secure and Resilient Vehicular Platooning

Ryan M. Gerdes and Kevin Heaslip
Virginia Tech
Arlington, VA 22203, USA
rgerdes,kheaslip@vt.edu

Ming Li
University of Arizona
Tuscon, AZ 85721, USA
lim@email.arizona.edu

Rajnikant Sharma, and Chris Winstead
Utah State University
Logan, UT 84322, USA
first.last@usu.edu

Introduction

The goal of the project is to provide a secure foundation for a transportation system that increasingly relies on the cooperation, connectedness, and automation of vehicles to achieve increases in safety, efficiency, and capacity. The financial losses attributable to congestion in America's transportation infrastructure are more than $1 trillion annually and the parallel loss of life in vehicle collisions is 40,000 deaths per year. Cooperative, autonomous vehicles are expected to increase the throughput of vehicles; reduce emissions, fuel consumption, and injuries; extend personal transportation to the disabled and elderly; and lessen the number and size of roadways.

Vehicular Platooning

Automated vehicle platoons are linear groups of vehicles acting in unison and travelling in a close-following formation (Figure 1). The feasibility of platooning has been demonstrated recently by the SARTRE, ARGO, and KONVOI projects.

Expected benefits of platooning include:

- lessening of congestion (10,000 vehicles per hour per lane [vphpl], as opposed to the 1,800-2,200 vphpl of traditional highway lanes).
- reducing the number and severity of accidents (e.g. small vehicle separations prevent build-up of large relative velocities during emergency braking)
- decrease in emissions due to reduced drag

These benefits are negated or reduced when autonomous vehicles operate without platooning.

Previous work on platooning assume that vehicle operators:

- share a common set of goals and
- are willing to follow the same rules to achieve those goals

In contrast, our research considers an adversarial environment with colluding attackers attempting to degrade the safety and efficiency of the system.

Proposed Research

This project leverages a multi-disciplinary group, composed of security, transportation, control, and communication researchers to secure an automated transportation system that is available to all vehicles, trusted or not, that may experience impaired connectivity. The team is:

1. developing a secure and resilient control regime for automated vehicles,
2. building a framework based on the physical layer to enable vehicles to establish peer trust, and
3. providing a trusted infrastructure the ability to securely gather and disseminate traffic and environmental data to vehicles for optimal route planning and accident avoidance.

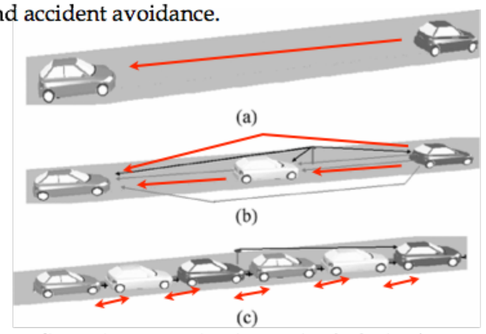

Figure 1: Platoon configurations to maintain spacing/velocity (arrows denote information flow). (a) predecessor: speed-dependent headway, used by adaptive cruise control systems, (b) predecessor + leader: constant spacing w/networking, for cooperative adaptive cruise control, and (c) predecessor + follower: constant spacing w/o networking.

Secure Vehicular Control

Connectedness, in the form of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication will increase the benefits of platooning, however:

- the deployment of these technologies at critical mass is not expected until nearly 2030
- Automakers have promised autonomous vehicles by 2020 or sooner.

To substantially improve transportation safety, capacity, and efficiency these vehicles must employ platooning without networking.

While platoon control has been studied extensively, existing work has not considered if and how an attacker could exploit the innate operation of the control algorithms to decrease platoon safety and efficiency.

To illustrate the vulnerability of existing work, we devised an attack [1] wherein two colluding attackers are able to force a platoon to collapse in on itself by modifying their control gains and causing the platoon to become unstable (Figure 2). We've also shown that the efficiency gains of platooning can be eliminated through unnecessary braking and accelerating by an attacker (surrounding vehicles expend 20% to 300% percent more energy than they would otherwise) [2].

Current work is focused on the designing of countermeasures, including the possible use of dynamic gain scheduling for vehicles in a platoon. It is hoped that by obfuscating the exact gains of other vehicles, an attacker would be prevented from calculating their own gain to achieve resonance.

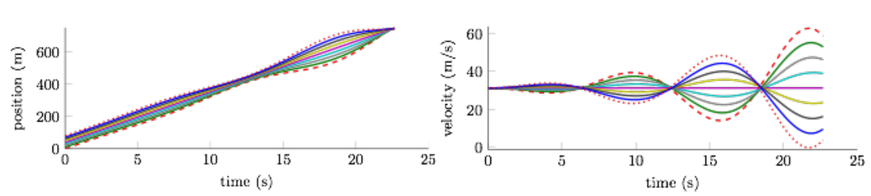

Figure 2: Attackers in control of vehicles at the front and back of the platoon (dotted and dashed lines) are able to introduce an instability by modifying only their controllers. By accelerating and braking at the correct frequency, the attackers cause the front half of the platoon to collide with the back. The simulated platoon dynamics are based on a popular bidirectional approach utilizing a proportional-derivative controller.

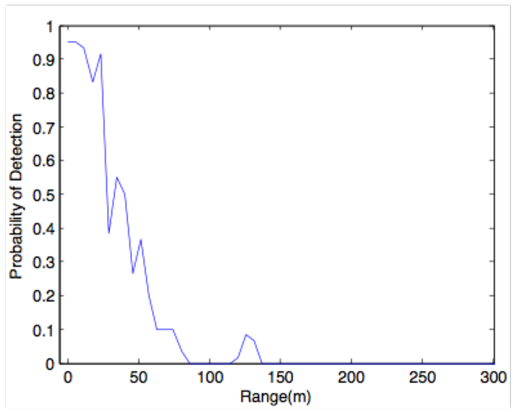

Figure 3: Radar spoofing: probability of detecting attacker at given range. Actual range 120 m with the attacker spoofing 15 m. System resolves attacker range as 15 m.

Secure Localization and Sensing for Transportation

Vehicle positions/actions must be verified to prevent the dissemination of bogus information for both safety and efficiency. However, secure localization under the assumption of mobility has not been as thoroughly studied as the static case.

In [3] we proposed and validated a distance decreasing attack on a type of radar (frequency-modulated continuous wave) commonly employed in vehicle automation systems. It was shown that an attacker able to ancticipate the characteristics of a victim's radar signal could reduce apparent distance by arbitrary amounts (Figure 3). Secondary localization sources are being considered to corroborate/replace traditional radar.

We also proposed [4] an interference-based approach for the secure verification of vehicle position, velocity, and acceleration (PVA) claims. To verify their PVA vehicles are required to reply to messages that are obscured by noise outside a given local (Figure 4). We showed that the probability of defeating such a system was less than 2%. Comparable approaches for PVA verification based on secure bilateration and trilateration could be defeated with 25% and 10% probability [5].

Secure V2V for Platooning

Optimizing traffic flow and decreasing the prevalence of accidents requires V2V communication so that vehicles in different platoons can coordinate their movements. It is essential that vehicles be able to trust the information they receive from other vehicles.

Our proposed framework allows V2V equipped vehicles to establish peer trust via physical layer resources and observed actions. Based on these primitives we can create:

1. trusted vehicle digital identities and
2. trustworthy incident/status reports

without pre-shared keys or a trusted infrastructure.

To build trusted identies for V2V we showed [6] that it is possible to establish authenticated secret keys and identities without any pre-shared secrets over a wireless channel by countering signal cancellation. Our approach has quantitative security guarantees and includes game-theoretic modelling of attacker behavior.

Conclusion

The proposed research will advance the knowledge in many fields: secure and resilient control, VANET security, trust establishment and management, physical-layer security, decision theory, and secure protocol design.

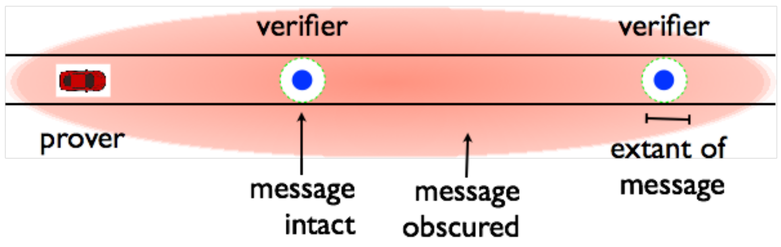

Figure 4. An interference based approach for secure localization that relies on the fact that a message that can only be received at position x at time t proves presence at x at t. The prover collects nonces and transmits them to a trusted infrastructure to prove its position claim.

References

1. S. Dedras, R. M. Gerdes, and R. Sharma, "Vehicular Platooning in an Adversarial Environment," In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2015), 2014 (accepted).
2. R. M. Gerdes, C. Winstead, and K. Heaslip, "An efficiency-motivated attack against autonomous vehicular transportation," in Proceedings of 29th Annual Computer Security Applications Conference (ACSAC 2013), 2013.
3. R. Chauhan, R. M. Gerdes and K. Heaslip, "Demonstration of a False-data Injection Attack Against an FMCW Radar," In Proceedings of Embedded Security in Cars Conference (ESCAR 2014), 2014.
4. B. Deka, R. M. Gerdes, M. Li, and K. Heaslip, "Friendly Jamming for Secure Localization in Vehicular Transportation," in Proceedings of 10th International Conference on Security and Privacy in Communication Networks (SECURECOMM 2014), 2014.
5. B. Deka, R. M. Gerdes, M. Li, and K. Heaslip, "Poster: Analysis and Comparison of Secure Localization Schemes for Intelligent Transportation Systems," in Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS2014), 2014.
6. Y. Hou, M. Li, R. Chauhan, R. M. Gerdes and K. Zeng, "Message Integrity Protection over Wireless Channel by Countering Signal Cancellation: Theory and Practice," In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2015), 2014 (accepted).