Thesis Project Portfolio

Strategic Safety-Critical Attacks Against an Advanced Driver Assistance System

(Technical Report)

Ethics of Autonomous Vehicles: Standards and Enforcement of Rational Behavior

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Haotian Ren

Spring, 2022

Department of Charles L. Brown Department of Electrical and Computer Engineering

Table of Contents

IV. Foundational Texts and Primary Resources

Sociotechnical Synthesis

Autonomous vehicles, also known as self-driving cars, are vehicles that can operate without human intervention. They use a variety of sensors and software to perceive their environment and make decisions on their own. The development of autonomous vehicles has been ongoing for several decades, but recent advancements in technology, including machine learning, artificial intelligence, and sensor technology, have brought us closer to a future where autonomous vehicles are a common sight on our roads. Several major automakers, including Tesla, GM, and Ford, have invested heavily in autonomous vehicle technology and have released vehicles with varying degrees of autonomous capabilities. These vehicles can perform tasks such as self-parking, adaptive cruise control, and lane-keeping assistance. In addition to traditional automakers, several tech companies, including Google's Waymo, Uber, and Lyft, are also developing autonomous vehicles.

Despite the progress made, there are still several challenges to overcome before autonomous vehicles become widespread. These include technological hurdles such as improving sensor technology and developing more advanced artificial intelligence algorithms. Additionally, there are legal and ethical issues surrounding autonomous vehicles, including liability in the event of an accident and concerns about the impact on jobs in the transportation industry.

In my technical project, I worked within a team to study the robustness of a state-of-the-art autonomous driving system that has been used commercially. We have trained models to attack this autonomous driving system and find ways to discover and prevent such attacks. We used an orthogonal model-driven approach to the above data-driven techniques. Instead of focusing on exploring the entirety of the fault parameter space, we focus on a systematic characterization of the effect of the values of the parameter space (e.g., start time and duration of faults) in conjunction with the dynamic state of the vehicle to identify the most opportune system contexts to launch the attacks. Our study shows that the proposed Context-Aware strategy judiciously selects the most opportune start times and durations for attacks and is efficient in exploiting the safety-critical states of ADAS(Autonomous Driving Assistant System). We also

find that lane invasions are common and can happen even without injecting faults, that the forward collision warning is not activated at all during attacks, and that the steering angle is the most vulnerable target. Our experimental results further highlight the importance of driver alertness for timely intervention and hazard prevention and the importance of robust automated safety mechanisms at the latest computational stage, just before execution on actuators. Overall, this autonomous driving system is vulnerable to some specific types of attacks, given enough information about the context of the vehicle, for example, the vehicle's speed, the distance from the leading vehicle, etc.

While the technologies used on autonomous vehicles develops fast, there come various ethical concerns. Some are worrying about whether autonomous vehicles can make moral decisions, others are discussing liability issues if an accident happens. In my STS research, ethics about autonomous vehicles are explored. Since this is a broad topic, my research focuses on the question: whether autonomous vehicles can make rational decisions. The article introduces the history of autonomous vehicles first, showing why it is important to start thinking about the ethics of this technology. The famous trolley problem is used to give audiences an idea of ethical dilemma. Though such a scenario engages moral decisions, the scope of this paper stays on rational decisions. Policies and standards from both the government and top associations and organizations in this field are then analyzed to see how far we have gone on the road to ensure that autonomous vehicles can behave rationally. Finally, benchmarks and possible methods are mentioned as an enforcement to those standards and policies. The whole idea of the research is to give an answer to whether it's possible to make autonomous vehicles behave ethically and provide a picture of what efforts have been made to realize this goal.

The ethics of autonomous vehicles is complicated and there are more aspects waiting to be explored. Except from ethics involved on the road, ethics related to society are also unneglectable, like the displacement of jobs in the transportation industry. Overall, the development of autonomous vehicles is still ongoing, and it is difficult to predict exactly when they will become a common sight on our roads. However, it is clear that the technology is rapidly advancing, but we are only getting closer than ever to a

future where autonomous vehicles are a reality if we take ethical issues carefully into account at the same time.