Poster: Vehicle-to-Infrastructure Security for Reduced Speed Work Zone

Patrick Mendoza
University of California, Berkeley
Berkeley, California, USA
patmendoza6745@berkeley.edu

Tashfique Choudhury
University of Florida
Gainesville, Florida, USA
choudhury.t@ufl.edu

Sandip Ray
University of Florida
Gainesville, Florida, USA
sandip@ece.ufl.edu

ABSTRACT

We consider the cybersecurity challenges arising from communications between autonomous vehicles and smart infrastructures. In particular, we consider coordination between vehicles and Reduced Speed Work Zones (RSWZ). Malicious or tampered communications between these entities can have catastrophic consequences. We discuss methods for the analysis of such attacks. In particular, we show how to generate configurable, effective vehicular trajectories for exploring such attacks and how to utilize such trajectories in identifying impactful attacks and evaluating defenses.

CCS CONCEPTS

• **Security and privacy** → **Intrusion/anomaly detection and malware mitigation**; • **Computer systems organization** → *Real-time systems.*

KEYWORDS

Connected Vehicle, Work Zone, Cyber Attack, Trajectory, Security

ACM Reference Format:

Patrick Mendoza, Tashfique Choudhury, and Sandip Ray. 2023. Poster: Vehicle-to-Infrastructure Security for Reduced Speed Work Zone. In *The Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc '23), October 23–26, 2023, Washington, DC, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3565287.3617980

1 INTRODUCTION

Global transportation is getting revolutionized by the rise of Connected Autonomous Vehicles (CAVs) equipped with advanced technologies, enabling them to self-navigate. These vehicles include the ability to communicate with other vehicles (V2V), various infrastructure components (V2I), and various other connected devices (V2IoT). This connectivity, cumulatively referred to as V2X is foundational for the future of autonomous vehicles.

A critical application of V2I communications in CAV is the interface with RSWZ. The interface has arisen in response to the critical demand for expanding urban centers and progressive transportation frameworks. Vehicles can integrate real-time data from work zone infrastructures via V2I communication mechanisms, allowing them to respond to shifts in advance, assure safe navigation, and boost smooth traffic movements. Unfortunately, the V2I communication can expose major cybersecurity vulnerabilities. For instance, a rogue or malicious RSWZ component can send misleading messages to vehicles; even if all the components are benign, the communication is susceptible to attacks whereby a malicious third party can intercept the communication and send wrong or misleading messages to either of the communicating agents.

A critical challenge in the study and analysis of cyber-attacks on V2I communication is the absence of an infrastructure for generating realistic scenarios. In particular, the scenarios must enable exploration of various corner cases of communication, comprehension of various cyber-attacks and their impact, and evaluation of defense mechanisms. Note that this is impossible with real datasets since the amount of such data is limited, and they are constrained to the specific parameter values that were realized during data collection. Indeed, to our knowledge, there is no extensive dataset incorporating vehicular trajectory and communication information with RSWZ.

In this paper, we show how to create and analyze a real-time trajectory generation model that highlights the dynamics of a CAV in action specifically targeting the communication between the CAV and the RSWZ. Using incoming V2I signals, the CAV is designed to either reduce its speed or come to a complete stop. Note that such a flexible trajectory generation tool is non-trivial, since it needs to account for both benign scenarios as well as the reaction of the CAV to various malicious communications. We discuss the challenges involved and our approach to addressing these challenges.

2 BACKGROUND AND RELATED WORK

Vehicle trajectory generation is critical in autonomous driving because it allows vehicles to negotiate complex traffic settings such as the RSWZ by precisely predicting vehicle trajectories.

Considerable research has been dedicated to the domain of realistic trajectory generation within urban environments. Many simulators, such as Simulation of Urban MObility (SUMO) [6] and Cars Learning to Act (CARLA) [4], aid in the generation of typical autonomous vehicle trajectories. Pérez *et al.*[8] introduced diverse techniques, including straight sketches, Bezier curves, circumference parameter equations, and fuzzy logic controllers, aimed at enhancing trajectory tracking in urban settings. Another avenue of exploration involves neural network architectures, as exemplified by Cai *et al.*[2], who proposed a novel approach utilizing spatiotemporal features extracted from front car images. Their custom neural network architecture, the VTGNet, integrates components such as

MobiHoc '23, October 23–26, 2023, Washington, DC, USA

ACM ISBN 978-1-4503-9926-5/23/10…$15.00
https://doi.org/10.1145/3565287.3617980

MobileNet-V2 for feature extraction and LSTMs, along with a self-attention mechanism for trajectory prediction. Similarly, Atmeh *et al.*[1] advocate a neural network composition incorporating a Recurrent Neural Network and two Feedforward Neural Networks.

While Machine Learning has garnered prominence in autonomous driving, Dever *et al.*[3] outlined the feasibility of generating parameterized classes of viable system trajectories through interpolation algorithms, offering a computationally efficient real-time trajectory generation approach. Addressing efficiency concerns, Zhang *et al.*[10] devised a two-phase optimization procedure encompassing a differential curvature-based driving guideline generation followed by an optimal trajectory computation. Fassbender *et al.*[5] presented a trajectory generation strategy relying on on-board sensors and Sequential Quadratic Programming.

Nolte *et al.*[7] advocated model predictive control (MPC) in a two-staged manner for vehicle trajectory generation. Alternatively, kinematic models, as demonstrated by Minh Vu *et al.*[9], harnessed position quintic polynomial, speed quartic polynomial, and symmetric polynomial functions for trajectory synthesis. Our approach draws inspiration from this paper, employing kinematic representation of vehicle states.

3 APPROACH AND DISCUSSION

Algorithm 1 gives a high-level overview of our trajectory generation tool. Note that it only provides a structure and overall control flow of the algorithm; many details have been elided in the presentation for pedagogical reasons. The key idea of the algorithm is to account for the communication from RSWZ for the vehicle to determine whether to accelerate or decelerate. However, the amount of acceleration/deceleration is governed by two factors:

- **Kinematics:** We employed kinematic equations to accurately model the vehicle's state throughout its trajectory. Within this framework, we integrate specific parameters, including the vehicle's velocity at the previous time step, the current time step within the trajectory's duration, and the vehicle's preceding actions, such as acceleration or deceleration.
- **Pseudorandomness:** The pseudo-random approach is employed to dictate the various actions the vehicle would "take", such as accelerating rapidly or gradually. This randomness was infused into the acceleration patterns the vehicle exhibited.

Our trajectory simulation is organized into three distinct phases: acceleration, random trajectory, and deceleration.

- During the acceleration phase, we establish four distinct acceleration scenarios to capture the vehicle's initial acceleration at the onset of the trip. This phase is limited to a maximum duration of 25% of the entire trip's duration, ensuring a smooth transition into the subsequent phases.
- Transitioning to the random trajectory phase, the vehicle's actions are determined by a combination of pseudo-randomness and rule-based parameters. This phase offers the vehicle the flexibility to execute various actions, including rapid or gradual acceleration, fast or slow deceleration, or maintaining a consistent speed. During this random trajectory phase, the V2I communications become crucial. If the V2I communication issues an "RS", the vehicle should decelerate if its current speed is over the speed limit and then navigate through the work zone at the desired velocity. Conversely, if the communication signals an "S" command, the vehicle must decelerate to a halt, remain stationary for the given duration, and then resume its journey. In cases where no V2I instructions are received, the vehicle should travel at a steady speed, though there may be random instances of acceleration or deceleration.
- The final phase, comprising the last 10% of the trip's duration, involves the deceleration phase. Here, the vehicle executed a controlled deceleration to gradually reduce its speed to 0 m/s, ensuring a safe conclusion to the simulated trip.

Algorithm 1 Pseudocode for Trajectory Calculation

```
Initialize velocity (v), acceleration (a), position (x), and time (t) arrays, and pseudorandom number generator.
Initialize entry 0 of velocity array with init_v
for i = acc_t_start to acc_t_end do
    Update trajectory information
end for
Initialize a dictionary for V2I communications
while i < ran_t_end do
    if i in v2i then
        Read in V2I communication
        if comm[0] == 'RS' then
            Decelerate the vehicle if needed and traverse the Work Zone
        else if comm[0] == 'S' then
            Decelerate the vehicle to a stop and wait for the specified duration
        end if
        Store the V2I communication
    else
        if counter % 20 == 0 then
            Apply an acceleration based on certain conditions
        else
            Maintain previous acceleration
        end if
        Update trajectory information
    end if
end while
for i = dec_t_start to dec_t_end do
    Decelerate the vehicle to a stop by the end of the trip
end for
```

Note that the trajectory generation framework integrates V2I communication, leveraging both Reduced Speed (RS) and Stop (S) V2I messages. These messages convey crucial instructions to the vehicle regarding its control strategies in response to specific situations. The integration enables us to explore the influence of V2I communications on CAV's trajectories, encompassing both legitimate and potentially malicious interactions.

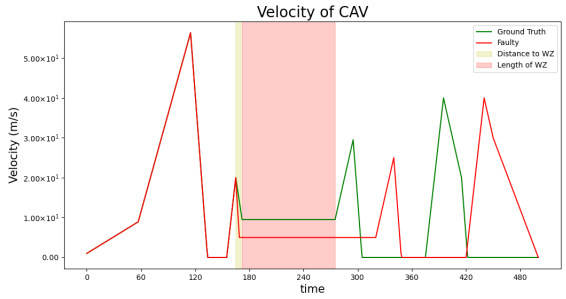

Figure 1: Reduce Speed Attack Scenario

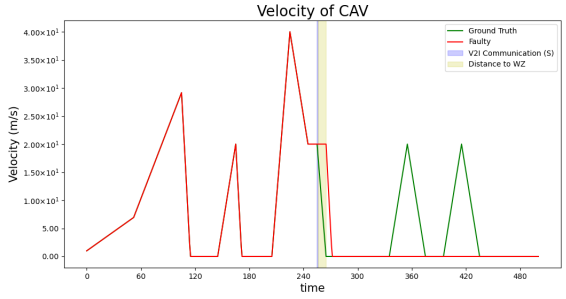

Figure 2: Ignore Stop Attack Scenario

4 ATTACK EXPLORATION

We developed a diverse array of methods to illustrate the spectrum of V2I attacks feasible within CAV trajectories. Central to our investigation are seven distinct parameters that attackers could maliciously manipulate. These parameters are summarized in table 1. The attacks, depending on the different parameter settings, varied from entirely ignoring V2I communication to minor tweaks like altering the distance to the work zone in a Reduced Speed V2I message or changing the stop duration at the work zone in a Stop V2I message. This wide range of parameter changes covers a broad array of potential attack situations, revealing the vulnerabilities and potential consequences of malicious V2I communications within CAV trajectories.

Fig. 1 depicts the velocity of the CAV during both compromised and standard trajectories in a Reduced Speed Attack Scenario. At 175 seconds, an 'RS' signal is sent to the CAV. In the attack situation, the speed in the work zone is manipulated to 5 m/s, in contrast to the normal 10 m/s, as illustrated by the red curve. Fig. 2 displays the CAV's velocity for both compromised and standard trajectories during a Stop Attack Scenario. At 260 seconds, an "S" signal is relayed to the CAV. The attack involves disregarding the "S" signal completely, as highlighted by the red curve. Here, the CAV persists at a speed of 20 m/s, neglecting the Work Zone's directive, leading to an eventual crash.

Table 2 showcases several methods through which the V2I communication can be compromised. It's important to mention that this table doesn't cover all potential attack scenarios; we've focused on highlighting the most common and impactful attacks.

Table 1: Attackable Parameters for V2I Communication

Reduced Speed (RS)	Stop (S)
V2I communication ("RS")	V2I communication ("S")
Distance to Work Zone (dist_to_WZ)	Distance to Work Zone (dist_to_WZ)
Length of Work Zone (len_of_WZ)	Duration of stop at Work Zone (duration)
Reduced Speed in Work Zone (reduced_speed)	

Table 2: Summary of Attack Scenarios

Term	Attack Scenario Definition
eq	Benign Scenario
stop	Perturb the Distance to (dist_to_WZ) and Duration of the Stop (duration) at the Work Zone.
dur_wz_stop	Perturb the Duration of the Stop (duration) at the Work Zone.
dwz_stop	Perturb the Distance (dist_to_WZ) to the Work Zone.
rswz	Perturb the Distance to (dist_to_WZ), Length of (len_of_WZ), and Speed Value (reduced_speed) in Work Zone.
lwz_rs	Perturb the Length of (len_of_WZ) Work Zone.
dwz_rs	Perturb the Distance to (dist_to_WZ) Work Zone.
swz_rs	Perturb the Reduced Speed Value in Work Zone.

5 CONCLUSION

In this paper, we explored the problem of cybersecurity of CAVs interacting with infrastructure components in RSWZ. To our knowledge our work is the first such exploration platform for cybersecurity implications of RSWZ and CAV coordination. We demonstrated the challenges in designing flexible trajectories to enable such exploration and our approach to address these problems. We showed how to explore cyber-attacks using the generated trajectories.

In future work, we will advance our trajectory generation tool and explore more cyber-attacks. We will also explore the integration of the algorithm with driving and automotive simulators to enable more intuitive interface.

Acknowledgments. This research has been partially supported by National Science Foundation under Grant No. REU-2150136.

REFERENCES

[1] Atmeh, G., and Subbarao, K. A dynamic neural network with feedback for trajectory generation. *IFAC-PapersOnLine 49*, 1 (2016), 367–372. 4th IFAC Conference on Advances in Control and Optimization of Dynamical Systems ACODS 2016.

[2] Cai, P., Sun, Y., Wang, H., and Liu, M. Vtgnet: A vision-based trajectory generation network for autonomous vehicles in urban environments. *IEEE Transactions on Intelligent Vehicles 6*, 3 (2021), 419–429.

[3] Dever, C., Mettler, B., Feron, E., Popovic, J., and McConley, M. Nonlinear trajectory generation for autonomous vehicles via parameterized maneuver classes. *Journal Of Guidance, Control, And Dynamics 29*, 2 (2006).

[4] Dosovitskiy, A., Ros, G., Codevilla, F., Lopez, A., and Koltun, V. CARLA: An open urban driving simulator. In *Proceedings of the 1st Annual Conference on Robot Learning* (2017), pp. 1–16.

[5] Fassbender, D., Heinrich, B. C., Luettel, T., and Wuensche, H.-J. An optimization approach to trajectory generation for autonomous vehicle following. In *2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)* (2017), pp. 3675–3680.

[6] Lopez, P. A., Behrisch, M., Bieker-Walz, L., Erdmann, J., Flötteröd, Y.-P., Hilbrich, R., Lücken, L., Rummel, J., Wagner, P., and Wiessner, E. Microscopic traffic simulation using sumo. In *The 21st IEEE International Conference on Intelligent Transportation Systems* (2018), IEEE.

[7] Nolte, M., Rose, M., Stolte, T., and Maurer, M. Model predictive control based trajectory generation for autonomous vehicles — an architectural approach. In *2017 IEEE Intelligent Vehicles Symposium (IV)* (2017), pp. 798–805.

[8] Pérez, J., Godoy, J., Villagrá, J., and Onieva, E. Trajectory generator for autonomous vehicles in urban environments. In *2013 IEEE International Conference on Robotics and Automation* (2013), pp. 409–414.

[9] Vu, T. M., Moezzi, R., Cyrus, J., Hlava, J., and Petru, M. Feasible trajectories generation for autonomous driving vehicles. *Applied Sciences 11*, 23 (2021).

[10] Zhang, Y., Sun, H., Zhou, J., Hu, J., and Miao, J. Optimal trajectory generation for autonomous vehicles under centripetal acceleration constraints for in-lane driving scenarios. In *2019 IEEE Intelligent Transportation Systems Conference (ITSC)* (2019), pp. 3619–3626.