Assessing the energy impacts of cyberattacks on low-level automated vehicles

Final Report

Raphael Stern

Department of Civil, Environmental,
and Geo- Engineering

University of Minnesota

CTS 23-05

CENTER FOR
TRANSPORTATION STUDIES
UNIVERSITY OF MINNESOTA

Technical Report Documentation Page

1. Report No.	2.	3. Recipients Accession No.
CTS 23-05		

4. Title and Subtitle	5. Report Date
Assessing the energy impacts of cyberattacks on low-level automated vehicles	August 2023
	6.

7. Author(s)	8. Performing Organization Report No.
Raphael Stern, Tianyi Li, Benjamin Rosenblad, Mingfeng Shang	

9. Performing Organization Name and Address	10. Project/Task/Work Unit No.
Department of Civil, Environmental, and Geo- Engineering University of Minnesota 500 Pillsbury Drive SE Minneapolis, MN 55455	CTS #2023019
	11. Contract (C) or Grant (G) No.

12. Sponsoring Organization Name and Address	13. Type of Report and Period Covered
Center for Transportation Studies University of Minnesota 440 University Office Plaza 2221 University Avenue SE Minneapolis, MN 55414	Final Report
	14. Sponsoring Agency Code

15. Supplementary Notes

https://www.cts.umn.edu/publications/researchreports/

16. Abstract (Limit: 250 words)

In this study, we investigate the potential impact of stealthy cyberattacks on automated or partially automated vehicles, and consider how they will influence traffic flow and fuel consumption. Specifically, we define stealthy cyberattacks on automated vehicles where driving behavior deviates only slightly from normal driving behavior. We use simulation analysis to consider different cyberattacks, and investigate their impact on traffic flow and aggregate fuel consumption of all vehicles in the traffic flow. We find that such attacks, while difficult to detect, may substantially degrade traffic flow, and, to a lesser extent, vehicle emissions across the traffic flow.

17. Document Analysis/Descriptors	18. Availability Statement
Automated vehicle control, Computer security; Driver support systems	No restrictions. Document available from: National Technical Information Services, Alexandria, Virginia 22312

19. Security Class (this report)	20. Security Class (this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	22	

ASSESSING THE ENERGY IMPACTS OF CYBERATTACKS ON LOW LEVEL AUTOMATED VHEICLES

FINAL REPORT

Prepared by:

Raphael Stern, Tianyi Li, Benjamin Rosenblad, Mingfeng Shang
Department of Civil, Environmental, and Geo- Engineering
University of Minnesota

AUGUST 2023

Published by:

Center for Transportation Studies
University of Minnesota
440 University Office Plaza
2221 University Avenue SE
Minneapolis, MN 55414

ACKNOWLEDGMENTS

The authors would like to thank the Center for Transportation Studies at the University of Minnesota for providing generous funding to support this research. In addition, the authors would like to thank Dr. Shi'an Wang at the University of Texas El Paso for extensive discussions that helped shape this work.

TABLE OF CONTENTS

LIST OF FIGURES

EXECUTIVE SUMMARY

Automated vehicles may be susceptible to compromise by malicious actors via cyberattacks. This is true both for fully automated vehicles, as well as driver assist vehicles with automation features such as adaptive cruise control.

In this study, we investigate the potential impacts of such attacks, and consider how they will influence traffic flow and fuel consumption. Specifically, we define stealthy cyberattacks on automated vehicles where driving behavior deviates only slightly from normal driving behavior. We use simulation analysis to consider different cyberattacks, and investigate their impact on traffic flow and aggregate fuel consumption of all vehicles in the traffic flow.

We find that while these cyberattacks may be quite disruptive to traffic flow, they may not have the same size disruption when considering fuel consumption. This work provides a first understanding of how stealthy cyberattacks on automated or partially automated vehicles may impact traffic flow and other aggregare flow measures.

CHAPTER 1: INTRODUCTION

Automated vehicles (AVs) are expected to reshape the landscape of future transportation systems thanks to the advancement of vehicular sensing, communicating, and computing capabilities, bringing promising benefits like enhanced traffic stability [1, 2], reduced energy consumption [3, 4], and optimized parking space allocation [5, 6]. Notably, these benefits are anticipated only when the future transportation system is safe and secure. However, AVs offer new opportunities for malicious actors to compromise the traffic flow [7]. For instance, cyberattacks can be launched to the control commands, sensor measurements, or onboard software [8] of AVs or partially automated vehicles like adaptive cruise control (ACC) vehicles in a stealthy manner, causing slight changes to vehicle driving behavior without being easily detected. However, these subtle changes could result in considerable disruption to normal traffic flow in the form of traffic congestion [9].

Even subtle changes in vehicle driving behavior could have profound impacts on transportation systems [7, 8]. For example, it has been shown that even slight attacks on vehicle acceleration can result in stop-and-go traffic waves and increase crash risks without directly controlling vehicles to crash [10], compromising the safety of AVs. In addition to malicious attacks directly altering the control commands of AVs, sensor measurements provided by onboard LiDAR may be subject to false data injection attacks causing AVs to execute undesired maneuvers that can degrade their performance [11]. Even subtle attacks on a single vehicle can lead to substantial disruption in traffic flow [12], resulting in reduced traffic capacity and increased energy consumption and risk of rear-end collisions [9]. A detailed discussion on different attacks can be found in [7].

As seen in the aforementioned work, malicious cyberattacks could degrade the performance of vehicles being attacked, thereby jeopardizing the stability of traffic flow. Prior studies have mainly focused on investigating the influence of attacks on individual compromised vehicles from a microscopic perspective (at individual vehicle levels). In addition to studying the impact of attacks on individual vehicles, in this work we also quantitatively examine their impact on traffic flow from a macroscopic standpoint, considering the ripple effect of attacks on uncompromised vehicles. Further, we consider attacks occurring in distinct traffic conditions involving both uncongested and congested regimes, which allows for a more comprehensive understanding of cyberattack impacts on complex traffic dynamics. To this end, the main contributions of this study are summarized below:

- We consider candidate attacks to explore the possible impact of such attacks on traffic flow. Extensive experiments are conducted to quantify the energy impacts of each type of attack on both compromised and uncompromised vehicles.
- We consider potential attacks occurring in distinct traffic conditions involving both free flow and congested regimes, with a range of ACC market penetration rates (MPRs). This allows for a comprehensive understanding of cyberattack impacts on complex traffic dynamics, thereby inspiring the development of effective attack mitigation and traffic-control strategies in future studies.

This work is based on work presented at the IEEE Intelligent Vehicle Symposium in Anchorage, Alaska, in June 2023. Many components of this report also appear in the corresponding published manuscript.

The remainder of this report is structured as follows. In Chapter 2, we introduce the mathematical characterization of two types of attacks on ACC vehicles. In Chapter 3, the VT-Micro model is presented with a discussion on its re-calibration using modern vehicle trajectory data. We conduct a series of numerical experiments in Chapter 4 to examine the energy impacts of attacks on traffic flow. The simulation results are presented in Chapter 5. Discussion on the results and concluding remarks are given in Chapter 6.

CHAPTER 2: MATHEMATICAL MODELING OF CYBERATTACKS

2.1 CYBERATTACKS ON ADAPTIVE CRUISE CONTROL VEHICLES

Various forms of cyberattacks may be introduced to AVs or ACC vehicles in mixed-autonomy traffic [8]. In this Chapter, we focus on two common types of attacks that could pose a significant risk to ACC vehicles, namely malicious attacks on vehicle control commands and false data injection attacks on sensor measurements. While these attacks are distinct in nature, both could result in disruptive consequences to traffic flow [11]. In what follows, we will recall a mathematical modeling framework for candidate attacks in the context of car-following dynamics. Modeling these attacks is the first step towards understanding the energy impacts of attacks on ACC vehicles and traffic flow, even though the specifics of such attacks may vary. While the candidate attacks introduced may not necessarily be based on real attacks, the results could map possible attacks to the space-time diagrams in the context of car-following dynamics that is commonly used to describe ACC vehicle driving behavior.

2.2 CAR-FOLLOWING FRAMEWORK

To describe individual vehicle dynamics, microscopic car-following models are employed, where the acceleration of a vehicle is related to its own state and that of the preceding vehicle like inter-vehicle spacing and relative speed. The general form of vehicle acceleration is given by:

$$a(t) = f(\vartheta, s(t), v(t), \Delta v(t)), \tag{1}$$

where a is acceleration, s is inter-vehicle spacing between two consecutive vehicles, v is speed of the following vehicle, $\Delta v = v_l - v$ denotes the relative speed between the following vehicle (v) and the lead (preceding) vehicle (v_l), and ϑ is a vector of time-invariant model parameters. The time index t is omitted for brevity wherever appropriate.

2.3 TYPE I: MALICIOUS ATTACKS ON VEHICLE CONTROL COMMANDS

We first consider malicious attacks directly acting on vehicle control commands (termed Type I attacks in this study), modeled as random disturbances to vehicle acceleration. This will have a direct impact on vehicle driving behavior.

Considering Type I attacks on ACC vehicles, the resulting vehicle acceleration is compromised by a random signal (variable), ξ, describing the effect of attacks. Consequently, compromised ACC vehicles could exhibit anomalous driving behavior, such as extreme acceleration or deceleration, causing disruptions to traffic flow. Without loss of generality, attacks are assumed to be able to occur at any time instance. To this end, the resulting acceleration is given by [13]:

$$\begin{cases} a(t) = f(\boldsymbol{\theta}, s, v, \Delta v), & if\ unattacked \\ \tilde{a}(t) = f(\theta, s, v, \Delta v) + \xi, & if\ attacked \\ a(t), \tilde{a}(t) \in [\underline{a}, \overline{a}], \end{cases} \quad (2)$$

where $\tilde{a}(t)$ denotes acceleration of an ACC vehicle being attacked by Type I attacks; ξ, e.g., a Gaussian random variable, is the attack directly acting on vehicle control commands (acceleration); $\underline{a}$ and $\overline{a}$ are the lower and upper bounds of acceleration, respectively. While other statistical distributions could be applied to characterize potential attacks, we use a Gaussian distribution to describe their stochastic nature in this study [14].

2.4 TYPE II: FALSE DATA INJECTION ATTACKS ON SENSOR MEASUREMENTS

The second common type of cyberattacks is false data injection attacks on sensor measurements (termed Type II attacks) [15] due to the fact that ACC vehicles need to use onboard sensors to measure the relative speed and spacing to the preceding vehicle. This type of attack could occur to data acquisition algorithms (software) or data collection sensors (hardware) of ACC vehicles, resulting in corrupted data of car-following dynamics. Since Type II attacks do not directly act on acceleration, attacked ACC vehicles likely experience less extreme driving behavior compared to the case of Type I attacks. However, attacked vehicles could still exhibit anomalous behavior. This process can be described in the following abstract form:

$$\tilde{A} = A + \boldsymbol{\Lambda}, \quad (3)$$

where $A = [s, \Delta v]^{\mathsf{T}}$ is the measurement vector of relative speed and inter-vehicle spacing, *A* form of *A* resulting from a vector of attack signals $\boldsymbol{\Lambda}$ affecting only attacked vehicles. Considering car following dynamics, this process is mathematically described as [13]:

$$\begin{cases} a(t) = f(\boldsymbol{\theta}, s, v, \Delta v), & if\ unattacked \\ \tilde{a}(t) = f(\theta, s + \lambda_1, v, \Delta v + \lambda_2), & if\ attacked \\ a(t), \tilde{a}(t) \in [\underline{a}, \overline{a}], \end{cases} \quad (4)$$

where λ_1 and λ_2 are false data injection attacks on ACC measurements. It follows from (3) and (4) that $\boldsymbol{\Lambda} = [\boldsymbol{\lambda_1}, \boldsymbol{\lambda_2}]^{\mathsf{T}}$ for any ACC vehicle being attacked. As in (2), vehicle acceleration is physically bounded by $\underline{a}$ and $\overline{a}$.

CHAPTER 3: QUANTIFYING THE ENERGY IMPACTS OF ATTACKS ON ACC VEHICLES

Being complementary to previous work focusing on the impacts of attacks on traffic stability, in this study we examine the energy impacts of such attacks on traffic flow considering distinct traffic conditions. To achieve this quantitatively, an accurate mathematical model is required for estimating vehicle energy consumption. A series of vehicle energy consumption models have been developed with different modeling structures. In general, these models can be categorized as macroscopic and microscopic models. Macroscopic models are often used for estimating network-level fuel consumption using average aggregate network parameters [16], such as the COPERT model using an average vehicle speed for estimation [17]. By contrast, microscopic models calculate the fuel consumption rate using instantaneous measurements of explanatory variables, such as vehicle power, acceleration, and speed [16]. For example, the widely used VT-Micro Model [18] uses individual vehicle speed and acceleration for calculating instantaneous fuel consumption.

As mentioned in Chapter 2.1, cyberattacks can impact driver behavior, resulting in perturbed individual vehicle acceleration and speed. Hence, we adopt the VT-Micro Model described above, that can capture the instantaneous fuel consumption of a vehicle using its instantaneous speed and acceleration. This model was developed based on chassis dynamometer measurements of three light-duty trucks and five light-duty automobiles, with fuel consumption rates collected at the Oak Ridge National Laboratory [19]. Specifically, the mathematical model is given by [18]:

$$\ln(FC) = \begin{cases} \sum_{i=0}^{3}\sum_{j=0}^{3} L_{i,j}\, v^i a^j & \forall\, a \geq 0 \\ \sum_{i=0}^{3}\sum_{j=0}^{3} M_{i,j}\, v^i a^j & \forall\, a < 0, \end{cases} \tag{5}$$

where FC denotes the fuel consumption rate and L_{ij} and M_{ij} are regression parameters.

The VT-Micro Model is a regression model composed of a combination of linear, quadratic, and cubic speed and acceleration terms. The model is constructed separately for positive and negative acceleration regimes to account for the differences in fuel consumption rate sensitivity to speed between acceleration and braking modes. Further, natural logarithm is used to ensure that the model produces non-negative fuel consumption rates [17].

The model parameters L_{ij} and M_{ij} are calibrated from experimental vehicles. The model parameter values were first calibrated by Ahn et al. [18]. However, the experimental vehicles were manufactured in the 1990s, and the model parameter values may not be able to characterize currently commercially available vehicles. Thus, we use recently published parameter values for a 2010 Honda CR-V [20, 21].

CHAPTER 4: SIMULATION AND EXPERIMENT

In this Chapter, we introduce the simulation we used to conduct all the experiments in this study. Next, we present our fuel consumption experiment.

4.1 RING ROAD SIMULATION

We simulate cyberattacks introduced in Chapter 2.1 in the context of car-following experiments conducted with MATLAB 2021a on a computer with an Intel i7-9750 CPU @ 2.6 GHz processor. The two types of attacks are studied via a ring-road experiment. Fig. 1 shows the experimental setup involving mixed traffic, where HVs, normal ACC vehicles, and attacked ACC vehicles are in green, blue, and red, respectively. As seen in prior studies [22, 23, 2], the intelligent driver model (IDM) [24] with different model parameter values is widely used to describe the driving behavior of HVs and ACC vehicles, given by:

$$f(\boldsymbol{\theta}, s, v, \Delta v) = \alpha \left[1 - \left(\frac{v}{v_d} \right)^{\delta} - \left(\frac{\hat{s}(v, \Delta v)}{s} \right)^2 \right], \tag{6}$$

where

$$\hat{s}(v, \Delta v) = \eta + \tau v - \frac{v \Delta v}{2\sqrt{\alpha \beta}} \tag{7}$$

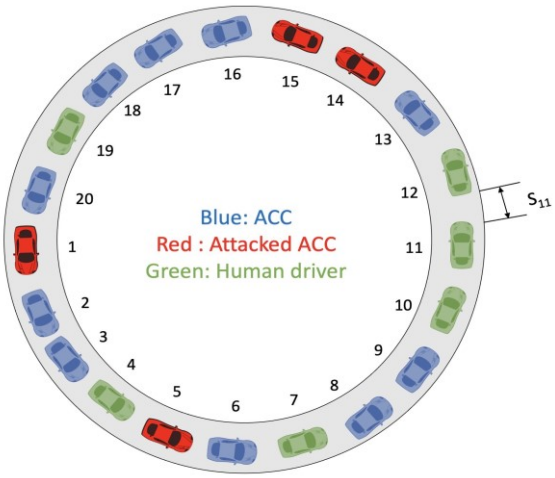


Figure 1: For illustration, ring simulation is conducted in this study. Note that vehicles are randomly distributed as human-driven vs. ACC vs. attacked ACC vehicles.

The vector of model parameters, ϑ, is defined as $\vartheta = [\alpha,\beta,\delta,\eta,\tau,v_d]^\top$, where α is the maximum acceleration, β is the comfortable deceleration, δ is an acceleration exponent, η is the jam distance, τ is the time gap, and v_d is the desired speed. For ACC vehicles, the calibrated model parameter values are taken as $\vartheta_{\text{ACC}} = [0.6,5.2,15.5,6.3,2.2,44.1]^\top$ from [25]. The study shows that modeling ACC vehicles using the IDM can fit ACC driving data well [25], based on calibration using field experiments data of ACC vehicles [26]. For human drivers, the corresponding IDM parameter values are adopted from [27], where $\vartheta_{\text{Human}} = [1.06,2,4,3.4,1.26,30]^\top$.

In this study, the simulation is conducted with 20 vehicles driving on a ring track to simulate traffic flow without boundary conditions. The initial inter-vehicle spacing between any two consecutive vehicles is set equal to the total length of the track divided by the number of vehicles. In other words, vehicles are evenly distributed along the road at the beginning of the simulation. There are 20 vehicles in total, with 50% being ACC vehicles as an example for illustration. Among the 10 ACC vehicles, half are randomly chosen to be attacked by Type I or Type II attacks. We consider two scenarios, namely Scenario 1 and Scenario 2, corresponding to free flow and congested conditions, respectively. This is further illustrated in Fig. 2, showing an analytical estimate of the fundamental diagrams for mixed traffic flow. This is obtained based on the reciprocal relationship between traffic density and average equilibrium spacing of heterogeneous traffic, as seen also in [28, 29]. Since the simulation experiments are conducted with various ACC market penetration rates, the percentage for attacked ACC vehicles, i.e., 50%, is fixed for convenience. However, follow-up studies may consider a wider range of MPRs and traffic densities. It is worth noting that each attack scenario is examined independently, and only one type of attack is considered in each simulation. Furthermore, it is important to note that all experiments are collision-free, as the focus is on assessing the energy impacts of the stealthy attack.

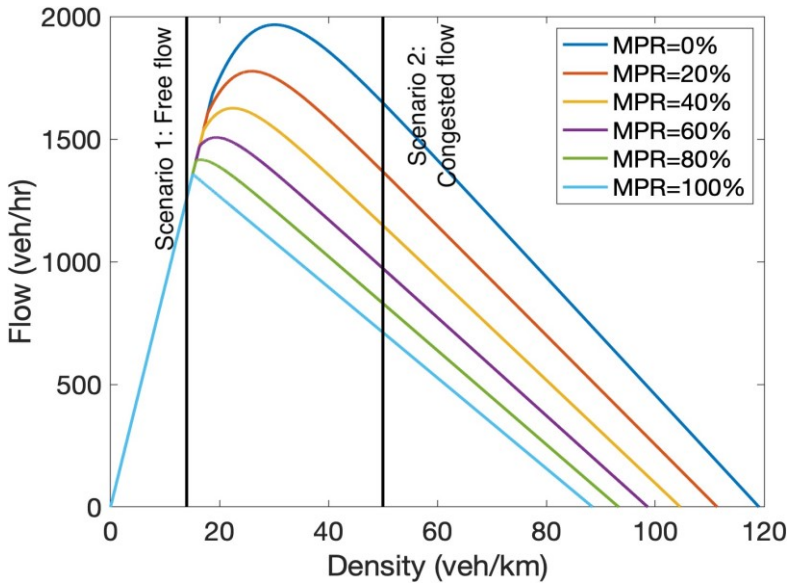


Figure 2: Fundamental diagrams of mixed traffic flow at different market penetration rates (%) of ACC vehicles. Two simulation scenarios are considered at different traffic conditions. Scenario 1: free-flow condition (14 veh/km) and Scenario 2: congested flow condition (50 veh/km).

4.2 FUEL CONSUMPTION EXPERIMENTS

As seen in Chapter 4.1, the simulation provides the acceleration, speed, spacing, and position profiles of all 20 simulated vehicles. Using these trajectories and equation (5), one can compute the fuel consumption of human-driven vehicles, ACC vehicles, and attacked ACC vehicles separately, thereby calculating the average fuel consumption (AFC) of all vehicles under all attack scenarios. This computation is carried out for both free flow conditions (density = 14 veh/km) and congested conditions (density = 50 veh/km). To vary traffic density, we fix the number of vehicles at 20, and adjust the ring length to 0.4 km and 1.4 km for congested conditions and free flow conditions, respectively. The AFC, in L/100km, is calculated as:

$$AFC = \frac{\sum_{t=t_0}^{T} \sum_{k=1}^{K} FC_{k,t}\, \Delta t}{\sum_{k=1}^{K} (P_{k,t} - P_{k,0})} \tag{8}$$

where T is the final time step in the simulation, i.e., 54,000; K is the last vehicle index in the simulation; $FC_{k,t}$ is the instantaneous fuel consumption rate of vehicle k at time step t; $P_{k,T}$ and $P_{k,0}$ are the positions of vehicle k at the final time step and initial time step, respectively. Vehicle trajectories are simulated over a period of 30 minutes. The AFC computation begins at 5 minutes, i.e., t_0=9000, in the simulation to exclude the warm-up period. For each traffic scenario, we conduct 10 Monte Carlo simulations and compute the resulting average fuel consumption.

CHAPTER 5: NUMERICAL RESULTS

The experimental results are shown in Fig. 3-Fig. 7. Fig. 3 illustrates the microscopic observation of traffic density distribution as a function of individual vehicle acceleration, speed, and inter-vehicle spacing. The data distribution of acceleration and spacing under the Type I attack has the largest variance. Type II attacks are observed to not change the driving behavior significantly, except for a few outliers in the acceleration. These findings are consistent with the fact that Type I attacks act directly on vehicle acceleration, while Type II attacks do not.

Fig. 4 and Fig. 5 show the space-time diagrams of vehicle trajectory for the free-flow and congested conditions, respectively. HVs, normal ACC vehicles, and attacked ACC vehicles correspond to green, blue, and red trajectories, respectively. It is observed that the position of attacked ACC vehicles tend to deviate from their normal ranges, especially under Type I attack, while the trajectory of unattacked vehicles mostly remains normal. In addition, compared to Type II attacks, Type I attacks appear to impact traffic flow to a greater extent. This is expected since Type I attacks act directly on vehicle acceleration.

Fig. 6 shows the fuel consumption results under free flow conditions, including the average fuel consumption of all vehicles (Fig. 6a), unattacked ACC vehicles (Fig. 6b), attacked ACC vehicles (Fig. 6c),

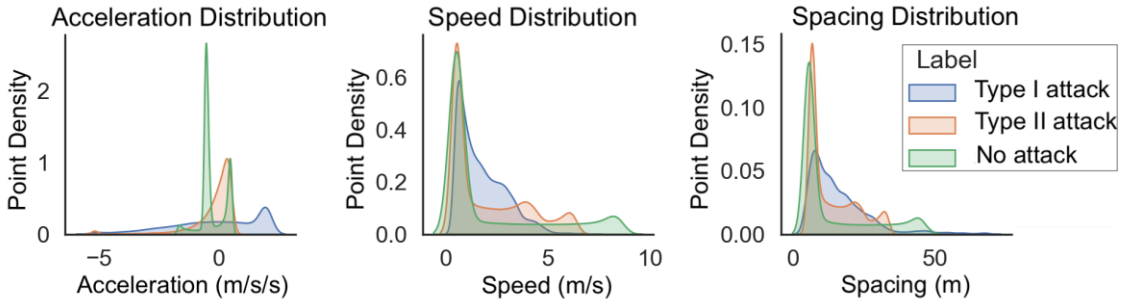
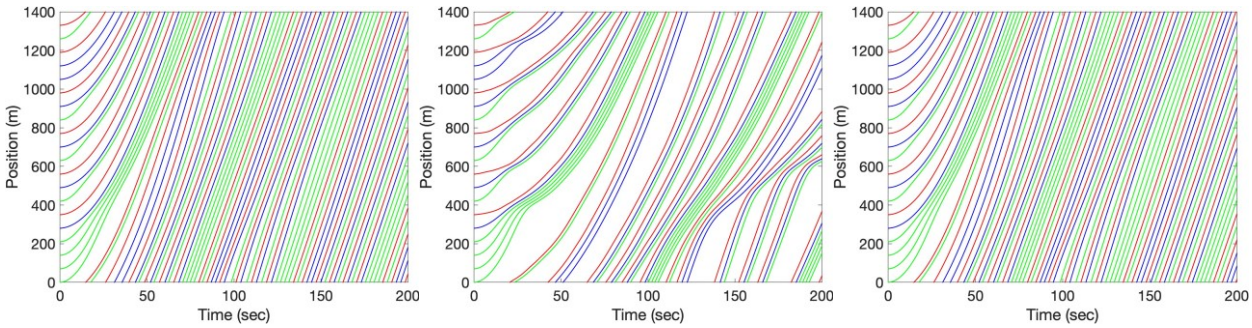
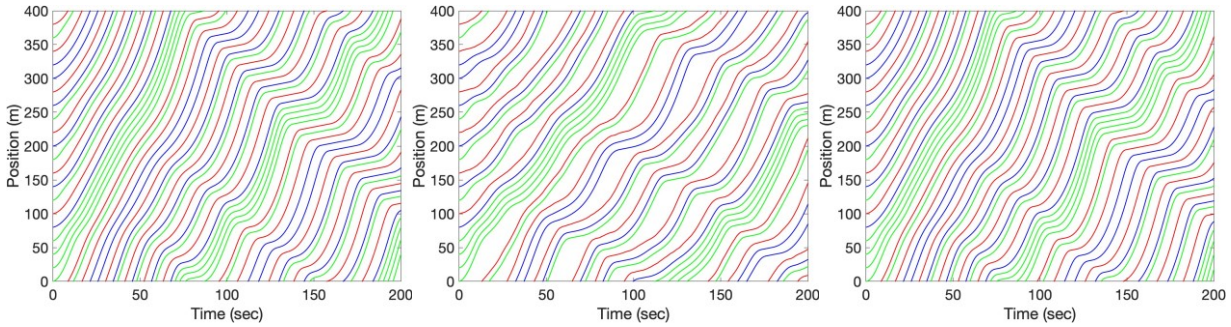


Figure 3: Density distribution of acceleration, speed, and spacing under Type I attack, Type II attack, and normal cases.



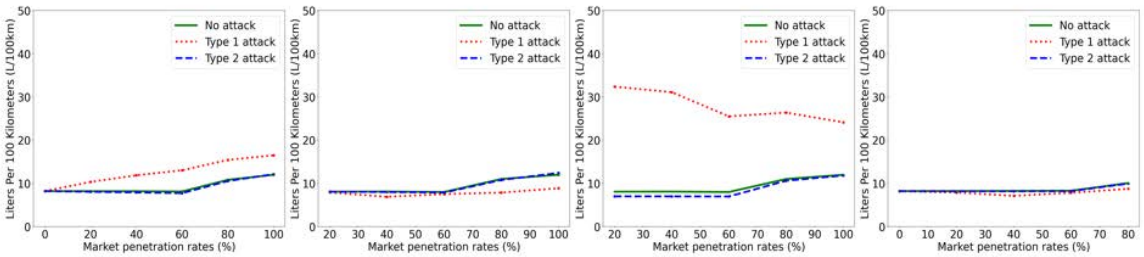
(a) Normal scenario (b) Type I attack (c) Type II attack

Figure 4: Vehicle trajectories in mixed traffic under free flow conditions (14 veh/km) at MPR = 60%. (Human-driven vehicles, normal ACC vehicles, and attacked ACC vehicles correspond to green, blue, and red trajectories, respectively).



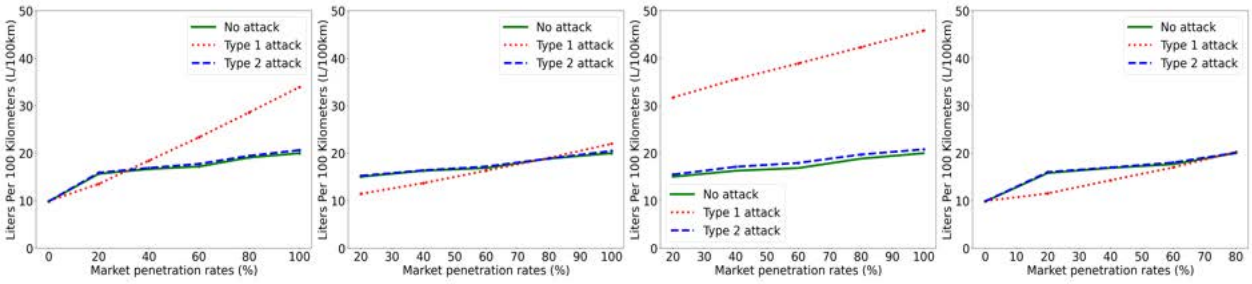
(a) Normal scenario (b) Type I attack (c) Type II attack

Figure 5: Vehicle trajectories in mixed traffic under congested conditions (50 veh/km) at MPR = 60%. (Human-driven vehicles, normal ACC vehicles, and attacked ACC vehicles correspond to green, blue, and red trajectories, respectively.)



(a) All vehicles (b) Unattacked ACC vehicles (c) Attacked ACC vehicles (d) human-driven vehicles

Figure 6: Fuel consumption at various ACC vehicle market penetration rates under free flow conditions (14 veh/km).



(a) All vehicles (b) Unattacked ACC vehicles (c) Attacked ACC vehicles (d) Human-driven vehicles

Figure 7: Fuel consumption at various ACC vehicle market penetration rates under congested conditions (50 veh/km).

and human-driven vehicles (Fig. 6d). By contrast, Fig. 7 demonstrates the fuel consumption results under congested conditions. Note that all the AFC results are obtained based on 10 Monte Carlo simulations.

It is observed from Fig. 6a and Fig. 7a that Type I attacks result in a significant increase in average fuel consumption for both free flow and congested scenarios. In addition, fuel consumption tends to get worse as the MPR (proportion of attacked vehicles) increases. Notably, the average fuel consumption of the attacked vehicles in the free flow scenario exhibits a decreasing trend as the MPR increases (Fig. 6c), which is likely due to large spacing allowing for higher vehicle speeds. Moreover, the average fuel consumption of unattacked vehicles (both ACC and human-driven vehicles) is not significantly affected by attacks on traffic flow, compared to the non-attacked scenarios.

CHAPTER 6: CONCLUSION

Based on the simulation results discussed in Chapter 5, it is observed that the two types of candidate attacks introduced to ACC or partially automated vehicles may only adversely impact the fuel consumption of the compromised vehicles and may not translate to significantly higher emissions across the fleet. This suggests that traffic flow may be robust to simple attacks of this nature concerning fuel consumption.

As mentioned before, Type I attacks act directly on vehicle acceleration, which tends to result in more fuel consumption compared to Type II attacks. This is even worse for congested traffic conditions. Therefore, the future effort is needed for developing effective attack mitigation and traffic-control strategies in accordance with the behavior of attacked ACC vehicles and the interplay among vehicles (more significant in congested traffic regimes). Moreover, additional comprehensive simulation analysis is needed to further study when attacks may impact fuel consumption and emissions such as CO, HC, and NOx.

REFERENCES

[1] S. Cui, B. Seibold, R. Stern, & D. B. Work. (2017). Stabilizing traffic flow via a single autonomous vehicle: Possibilities and limitations. *2017 IEEE Intelligent Vehicles Symposium*, 1336–1341.

[2] S. Wang, R. Stern, & M. Levin. (2022). Optimal control of autonomous vehicles for traffic smoothing. *IEEE Transactions on Intelligent Transportation Systems*, *23*(4), 3842–3852.

[3] Z. Wadud, D. MacKenzie, & P. Leiby. (2016). Help or hindrance? The travel, energy and carbon impacts of highly automated vehicles. *Transportation Research Part A: Policy and Practice*, *86,* 1–18.

[4] W. Sun, S. Wang, Y. Shao, Z. Sun, & M. W. Levin. (2022). Energy and mobility impacts of connected autonomous vehicles with co-optimization of speed and powertrain on mixed vehicle platoons. *Transportation Research Part C: Emerging Technologies*, *142,* 103764.

[5] D. J. Fagnant & K. Kockelman. (2015). Preparing a nation for autonomous vehicles: opportunities, barriers, and policy recommendations. *Transportation Research Part A: Policy and Practice*, *77,* 167–181.

[6] S. Wang, M. W. Levin, & R. J. Caverly. (2021). Optimal parking management of connected autonomous vehicles: A control-theoretic approach. *Transportation Research Part C: Emerging Technologies*, 124, 102924.

[7] S. Parkinson, P. Ward, K. Wilson, & J. Miller. (2017). Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Transactions on Intelligent Transportation Systems*, *18*(11), 2898–2915.

[8] J. Petit & S. E. Shladover. (2014). Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *16*(2), 546–556.

[9] C. Dong, H. Wang, D. Ni, Y. Liu, & Q. Chen. (2020). Impact evaluation of cyber-attacks on traffic flow of connected and automated vehicles. *IEEE Access*, *8,* 86824–86835.

[10] Y. Wang, E. Sarkar, W. Li, M. Maniatakos, & S. E. Jabari. (2021). Stop-and-go: Exploring backdoor attacks on deep reinforcement learning-based traffic congestion control systems. *IEEE Transactions on Information Forensics and Security*, *16*, 4772–4787..

[11] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, & Y. Chen. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention*, *148,* 105837.

[12] Z. H. Khattak, B. L. Smith, & M. D. Fontaine. (2021). Impact of cyberattacks on safety and stability of connected and automated vehicle platoons under lane changes. *Accident Analysis & Prevention*, *150,* 105861.

[13] T. Li, M. Shang, S. Wang, M. Filippelli, & R. Stern. (2022). Detecting stealthy cyberattacks on automated vehicles via generative adversarial networks. *2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC)*, 3632–3637.

[14] F. Van Wyk, Y. Wang, A. Khojandi, & N. Masoud. (2019). Real-time sensor anomaly detection and identification in automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *21*(3), 1264–1276.

[15] Y. Li, Y. Tu, Q. Fan, C. Dong, & W. Wang. (2018). Influence of cyber-attacks on longitudinal safety of connected and automated vehicles. *Accident Analysis & Prevention, 121,* 148–156.

[16] H. Rakha, K. Ahn, and A. Trani. (2003). Comparison of mobile5a, mobile6, vt-micro, and cmem models for estimating hot-stabilized light-duty gasoline vehicle emissions. *Canadian Journal of Civil Engineering*, *30*(6), 1010–1021.

[17] W. F. Faris, H. A. Rakha, R. I. Kafafy, M. Idres, & S. Elmoselhy. (2011). Vehicle fuel consumption and emission modelling: An in-depth literature review. *International Journal of Vehicle Systems Modelling and Testing, 6*(3–4), 318–395.

[18] K. Ahn, H. Rakha, A. Trani, & M. Van Aerde. (2002). Estimating vehicle fuel consumption and emissions based on instantaneous speed and acceleration levels. *Journal of Transportation Engineering*, *128*(2), 182–190.

[19] M. Zhou, H. Jin, & W. Wang. (2016). A review of vehicle fuel consumption models to evaluate eco-driving and eco-routing. *Transportation Research Part D: Transport and Environment*, *49*, 203–218.

[20] C. Lu, J. Dong, & L. Hu. (2019). Energy-efficient adaptive cruise control for electric connected and autonomous vehicles. *IEEE Intelligent Transportation Systems Magazine, 11*(3), 42–55.

[21] J. Dong & L. Hu. (2017). Investigation of the link between macroscopic traffic flow characteristics and individual vehicle fuel consumption.

[22] A. Talebpour & H. S. Mahmassani. (2016). Influence of connected and autonomous vehicles on traffic flow stability and throughput. *Transportation Research Part C: Emerging Technologies*, *71*, 143– 163.

[23] M. Shang & R. E. Stern. (2021). Impacts of commercially available adaptive cruise control vehicles on highway stability and throughput. *Transportation Research Part C: Emerging Technologies*, *122,* 102897.

[24] M. Treiber, A. Hennecke, & D. Helbing. (2000). Congested traffic states in empirical observations and microscopic simulations. *Physical Review E, 62*(2), 1805.

[25] F. de Souza & R. Stern. (2021). Calibrating microscopic car-following models for adaptive cruise control vehicles: Multiobjective approach. *Journal of Transportation Engineering, Part A: Systems*, *147*(1).

[26] G. Gunter, D. Gloudemans, R. E. Stern, S. McQuade, R. Bhadani, M. Bunting, ... & D Work. (2020). Are commercially implemented adaptive cruise control systems string stable? *IEEE Transactions on Intelligent Transportation Systems*, *22*(11), 6992–7003.

[27] A. Kesting & M. Treiber. (2008). Calibrating car-following models by using trajectory data: Methodological study. *Transportation Research Record*, *2088*(1), 148–156.

[28] X. Shi & X. Li. (2021). Constructing a fundamental diagram for traffic flow with automated vehicles: Methodology and demonstration. *Transportation Research Part B: Methodological*, *150,* 279–292.

[29] J. Zhou & F. Zhu. (2020). Modeling the fundamental diagram of mixed human-driven and connected automated vehicles. *Transportation research part C: Emerging Technologies*, *115,* 102614.