An impact evaluation of strategic cyberattacks on autonomous vehicles: Safety, mobility, and energy consumption

Jose Acedo Aguilar, Fernando Sepulveda, and Shian Wang, *Member, IEEE*

***Abstract*— While security has always been an important factor in the transportation industry, the increasing development and availability of autonomous driving technologies have brought a higher level of importance to safety and security due to malicious cyberattacks. Autonomous vehicles (AVs) are prone to cyberattacks which may not only have negative effects on the vehicle but also further degrade the performance of traffic flow. Following our recent work, in this study we consider the adversarial fashion and stealthy nature of potential attacks on a platoon of vehicles to study their impacts on traffic performance. Specifically, we first present a general framework describing mixed traffic involving AVs and human-driven vehicles (HVs) based on car-following dynamics. Using this framework as the baseline scenario for simulating a platoon of 10 vehicles, we introduce a variety of linear and nonlinear attacks on AVs in additive and multiplicative fashion. The impacts of strategically designed attacks on traffic safety, mobility, and energy consumption are holistically examined, using metrics like time-to-collision (TTC), average speed variation (ASV), and fuel consumption (FC). A series of simulations are conducted across a range of AV market penetration rates (MPRs). Results show that strategically designed attacks tend to increase in impact with the growth of MPR, amplifying traffic instability and vehicle FC while remaining stealthy (without causing direct collisions). More severe, nonstrategic attacks result in greater levels of traffic oscillations and FC while also jeopardizing the safety of some vehicles, with collisions in certain scenarios. This study offers useful insights into understanding the impacts of strategic attacks on future automated transportation systems.**

I. Introduction

The integration of autonomous vehicles (AVs) into traffic will revolutionize future transportation systems by smoothing traffic flow [1], optimizing parking space allocation [2], and improving mobility and energy economy [3]. Although multiple benefits can arise from the introduction of AVs, this group of vehicles presents significant vulnerabilities against cyberattacks compromising traffic safety and efficiency [4], [5]. While fully automated vehicles have yet to be deployed at scale, the first generation of AVs, i.e., adaptive cruise control (ACC) vehicles are also subject to potential cyber threats [6]–[8]. With the advances of vehicle-to-everything (V2X) technologies, connected autonomous vehicles are expected to become more prevailing in the future [9]. Despite the promise of such emerging technologies, the presence of high levels of V2X connectivity and computational processes opens the door to malicious actors [10].

Malicious attacks can target different areas of a vehicle, such as the automotive controller, autonomous driving system, and V2X communication channel [10]. In [11], the authors were able to infiltrate several electronic control units, demonstrating the ease of affecting the unit and the capability of a perpetrator to gain control of the engine and breaks. In addition, attacks on connected vehicles have been analyzed in [12], where several possible attack strategies disrupt cooperative ACC at different layers of the system, either exploiting V2V communication or affecting the network of a vehicle platoon. Attackers might desire to control the state of several vehicles with an individual AV, destabilizing a large platoon of cars to cause a collision of considerable magnitude [13]. This shows that malicious actors tend to tailor specific attacks to achieve desired results.

Due to the intertwined relationship among vehicles in traffic flow, the influence of an attack will not only alter the behavior of its target but also impact the surrounding vehicles, resulting in a ripple effect to the bulk traffic [4], [12], [13]. While a few prior studies have assessed the impact of cyberattacks on ACC vehicles or AVs, they assumed constant or stochastic attacks [14]–[16], which may fail to characterize the malicious and stealthy nature of attackers. For instance, random attacks could act in favor of a compromised vehicle [16], contradicting with their malicious behavior. By contrast, in this study we holistically examine how strategically designed attacks on AVs may affect mixed traffic flow involving both human-driven vehicles (HVs) and AVs, leveraging newly synthesized malicious yet stealthy false data injection attacks on sensor measurements with a good degree of realism [7]. Specifically, we assess the impacts of such strategic attacks on traffic safety, mobility, and energy consumption. Various attack securities are considered across a range of AV market penetration rates (MPRs), defined as the ratio of AVs to the total number of vehicles on the road. The main contributions of this study are:

- Different from existing work mostly focusing on random attacks, we consider strategically designed attacks that tend to be stealthy, with a greater degree of realism.
- We holistically evaluate the impacts of strategically designed attacks on traffic safety, mobility, and energy consumption, across a range of MPRs of AVs.
- We present comprehensive numerical results illustrating the emerging impacts of strategic attacks on traffic flow. These results are expected to motivate the development of effective attack detection and mitigation strategies in future studies.

The remainder of this article is organized as follows. In Section II, we present a framework to describe mixed traffic flow. The design and analysis of malicious attacks on AVs

The authors are with the Department of Electrical and Computer Engineering, The University of Texas at El Paso, El Paso, Texas 79968 swang14@utep.edu (S. Wang)

are introduced in Section III. Section IV summarizes the numerical results, and the article is concluded in Section V.

II. Mixed Traffic Flow

A. Car-following model

Car-following models have been extensively used to describe microscopic traffic flow. Specifically, we consider a string of m vehicles denoted by the totally ordered set $\mathcal{M} = \{1, 2, 3, \cdots, m\},\ m > 1,\ m \in \mathbb{N}^+$. Following standard notations [17], for any vehicle $i \in \mathcal{M}$, let $x_i(t)$ and $v_i(t)$ denote its position and speed at time t, respectively. The resulting inter-vehicle spacing between vehicle i and its leader $i-1$ is given by $s_i(t) = x_{i-1}(t) - x_i(t) - l_{i-1}$ with l_{i-1} the length of vehicle $i-1$. Based on physics, the dynamics of any vehicle i is given by the following ordinary differential equations [17]:

$$\dot{x}_i(t) = v_i(t), \tag{1}$$

$$\dot{v}_i(t) = f(s_i(t), \Delta v_i(t), v_i(t)), \tag{2}$$

where the functional f relates the ith vehicle's acceleration to the variables s_i, Δv_i, and v_i, with Δv_i defined as

$$\Delta v_i(t) = \dot{s}_i(t) = v_{i-1}(t) - v_i(t). \tag{3}$$

Equations (1)–(2) indicate a general form of car-following dynamics widely adopted in the literature. While the variables present are time-dependent, for brevity we will omit the argument t wherever appropriate.

To differentiate the two types of vehicles in mixed traffic, we denote the totally ordered set of HVs and AVs by $\mathcal{H}$ and $\mathcal{A}$, respectively. Further, we distinguish the functional f of (2) as f_{HV} and f_{AV} accordingly, since human drivers tend to show different driving behaviors compared with AVs [18]. The resulting vehicle acceleration is written as

$$\dot{v}_i = \begin{cases} f_{\text{HV}}(s_i, \Delta v_i, v_i),\ \forall\ i \in \mathcal{H} & \text{(4a)} \\ f_{\text{AV}}(s_i, \Delta v_i, v_i),\ \forall\ i \in \mathcal{A} & \text{(4b)} \end{cases}$$

B. Human-driven vehicle dynamics

Following the framework shown above, here we present a concrete car-following model to characterize the dynamics of HVs, which will be used later for numerical study. Specifically, the intelligent driver model (IDM) [19] is selected due to its demonstrated ability to accurately capture the car-following behavior of human drivers.

Following the IDM, equation (4a) is written as

$$f_{\text{HV}} = a\left[1 - \left(\frac{v_i}{v_0}\right)^4 - \left(\frac{s^*(v_i, \Delta v_i)}{s_i}\right)^2\right],\ i \in \mathcal{H} \tag{5}$$

where

$$s^*(v_i, \Delta v_i) = s_0 + \max\left\{0, v_i T - \frac{v_i \Delta v_i}{2\sqrt{ab}}\right\}, \tag{6}$$

with a the maximum acceleration, b the comfortable braking deceleration, v_0 the desired speed, s_0 the minimum space gap, T the desired time headway, and l_{i-1} the length of vehicle $i-1$.

C. Autonomous vehicle dynamics

The well-known optimal velocity with relative velocity (OVRV) model is employed to represent the dynamics of AVs, as seen in many prior studies [1], [20], [21]. It has been shown to fit well to both simulated and real trajectories of vehicles equipped with ACC capabilities [20].

Following the OVRV model, equation (4b) is given by

$$f_{\text{AV}} = k_1\left(s_i - \eta - \tau v_i\right) + k_2 \Delta v_i,\ i \in \mathcal{A}, \tag{7}$$

where η denotes the jam distance, τ signifies the desired time gap, k_1 and k_2 are positive gains on the effective time gap and the relative speed, respectively.

III. Cyberattacks on Autonomous Vehicles

In this work, we focus on false data injection attacks on AV sensor measurements as seen in [4], [15], [21], while other forms of attacks could also be studied. Although most prior efforts are made to assess the impact of constant or random attacks on traffic flow [14], [15], our recent study [16] has shown that such attacks can be easily detected using the latest detection methods, e.g., generative adversarial networks. In contrast, we have synthesized a class of malicious and stealthy attacks in [7] leveraging the understanding of car-following driving behavior, which are shown to be stealthy against prominent detection approaches in the literature [22]. Hence, here we follow the recent work [7] to holistically examine the effects of strategically designed attacks on traffic performance, since they offer a greater degree of realism compared to those generated in a random fashion. In what follows, we will briefly present two types of attacks modeled in additive and multiplicative fashions.

A. Additive attacks on AV sensor measurement

As observed from equation (4b), the acceleration command executed by an AV relies on sensor measurements like spacing (s_i) and relative speed (Δv_i), which can be compromised by attacks [4], [15]. For $i \in \mathcal{A}$, let $\omega_{1,i}$ and $\omega_{2,i}$ denote the false data injection attacks on s_i and Δv_i, respectively. Hence, the resulting acceleration dynamics of any attacked AV becomes [15], [21]:

$$\dot{v}_i = f_{\text{AV}}(s_i + \omega_{1,i}, \Delta v_i + \omega_{2,i}, v_i),\ i \in \mathcal{A} \text{ attacked} \tag{8}$$

where $\omega_{1,i}$ and $\omega_{2,i}$ represent the attack signals.

By virtue of false data injection attacks, $\omega_{1,i}$ and $\omega_{2,i}$ are assumed to be launched based off AV sensor measurements perceived by the attackers, that is

$$\omega_{1,i} = g_1(s_i),\ \omega_{2,i} = g_2(\Delta v_i), \tag{9}$$

where g_1 and g_2 are differentiable functions with respect to their respective arguments, s_i and Δv_i. It is worth noting that they are not limited to any specific statistical distributions.

For attacks to remain malicious and stealthy, it follows from [7] that they can be drawn from the set $\mathcal{C}$:

$$\mathcal{C} \coloneqq \left\{g_1, g_2 : -1 < g_1' < 0,\ -1 < g_2' < 0\right\}, \tag{10}$$

where g_1' and g_2' are differentials with respect to their respective arguments. For details the reader is referred to [7].

Essentially, attacks taken from $\mathcal{C}$ ensure that i) an attacked vehicle still drives in a rational manner according to the rational driving constraints given in [17] since irrational driving behavior tends to get detected and identified more easily; ii) collisions shall be avoided for compromised AVs for similar reasons; iii) potential attacks have adverse effects on traffic flow considering their malicious nature. While attacks drawn from $\mathcal{C}$ tend to be malicious and stealthy, they can certainly be launched from its complement. However, those taken from outside of $\mathcal{C}$ are more likely to cause compromised AVs to drive irrationally and thus increase the risk of collisions, making them easier to detect [22].

B. Multiplicative attacks on AV sensor measurement

While attacks on AVs are commonly modeled in an additive manner shown above, from a mathematical perspective their impact on vehicle dynamics could also be represented in a multiplicative fashion. Following [23], we briefly present the framework of modeling multiplicative attacks on AV sensor measurement for technical completeness. Specifically, the effective acceleration dynamics of an AV, $i \in \mathcal{A}$, under such attack, is written as

$$\dot{v}_i = f_{\text{AV}}(s_i \cdot g_1(s_i), \Delta v_i \cdot g_2(\Delta v_i), v_i), \tag{11}$$

where $g_1(s_i)$ and $g_2(\Delta v_i)$ are the multiplicative attacks on spacing and relative speed. Following [23], a set of potential multiplicative attacks are given by

$$\mathcal{D} := \big\{g_1, g_2 : 0 < g_1 + s \cdot g_1' \leq 1, \\ 0 < g_2 + \Delta v \cdot g_2' \leq 1\big\}. \tag{12}$$

The reader is referred to [23] for more details. Clearly, multiplicative attacks offer an additional way to compromise the sensor measurements of an AV, while maintaining the consistency with the assumption that attacks are initiated based off the actual sensor measurements perceived.

IV. Numerical Results

In this section, we present a series of numerical results to show the impacts of strategically designed attacks on mixed traffic flow. Car-following dynamics described in Section II and cyberattacks on AVs presented in Section III were used for simulations in `Python`. Three metrics were considered to measure an attack's effects on a platoon: average speed variation (ASV), fuel consumption (FC), and safety. ASV [24] provides insights into how much speed changes on average across the event in question, allowing us to quantify the level of traffic smoothness. FC is computed with the extensively used VT-Micro model [25], which calculates the measure of effectiveness (MOE), providing data on instantaneous FC (L/s). This regression model only requires instantaneous acceleration (km/h/s) and speed (km/h) as inputs, with a detailed description given in [25]. With abrupt changes in driving behavior, the safety of vehicles can be jeopardized. In order to quantify the risk that vehicles present of a rear-end crash the time-to-collision (TTC) index is calculated [26]. TTC provides the amount of time left for a vehicle to make contact with another. For a comprehensive safety evaluation,

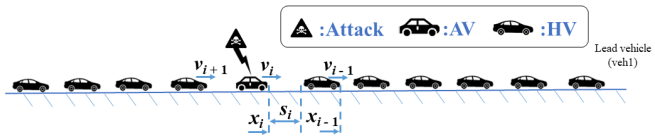
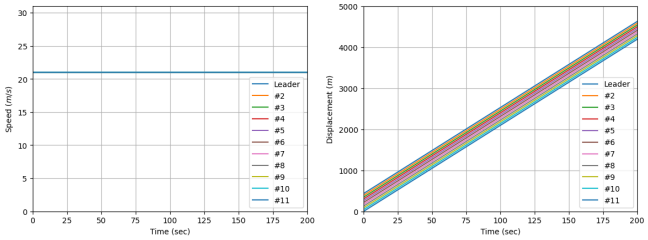


Fig. 1: Illustration of a string of 10 vehicles following a leader, with AVs under cyberattack.



(a) Speed vs. Time (b) Vehicle position vs. Time

Fig. 2: Vehicle speed and displacement in the absence of attacked AVs.

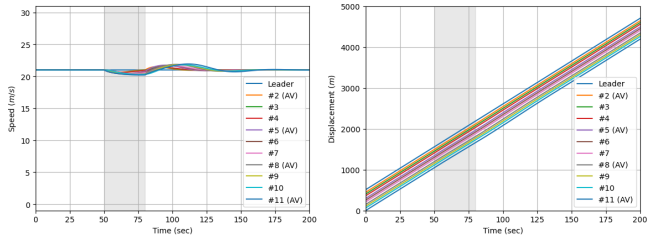
we define thresholds between 1.5–4.0 seconds, with intervals of 0.5 seconds, to calculate TTC and determine if a vehicle is in danger. We later describe the TTC index as the platoon's average percentage of time where vehicles are at risk of collision, and compare it under multiple MPRs.

For the simulation, we present a platoon of 11 vehicles composed of a leader, AVs, and HVs, depending on the traffic mixture. Different MPRs were tested, from 0% to 100% in intervals of 20%. The simulation setup follows the one presented in Fig. 1, where a leader follows a predetermined trajectory for 200 seconds. A detailed description of the normal trajectory of the vehicles in the absence of attacks is shown in Fig. 2. Similar to [4], [7], [15], [21] only longitudinal dynamics on a straight track are considered for simulations. The path performed by the leader is that of a straight line with a constant speed of 21 m/s and remains the same for all MPRs as well as for the four attacks presented in this study. To avoid having unrealistic accelerations or speeds we limited the range of both values in the following form [7]: $a_i \in [-2.5, 1.4]$ m/s^2 and $v_i \in [0, 30]$ m/s, $i \in \mathcal{M}$. Once an attack is considered, it takes place between 50–80 seconds of the event. HVs interact with the preceding vehicles based on the IDM model presented in Section II, while AVs follow the dynamics under attack shown in Section III. The model parameters used for simulation are taken from Table I of [7].

Four distinct attacks of varying magnitudes and natures were considered for simulations to understand the impact on mixed traffic. Initially, we consider two stealthy additive attacks, from the set $\mathcal{C}$, on AVs, i.e., a nonlinear attack in Scenario A and a slightly harsher linear alteration in Scenario B. Scenario C presents an additive attack outside of $\mathcal{C}$ defined in Section III. Finally, Scenario D showcases a multiplicative attack that severely impacts sensor readings. For simplicity, all AVs are assumed attacked across those four scenarios.

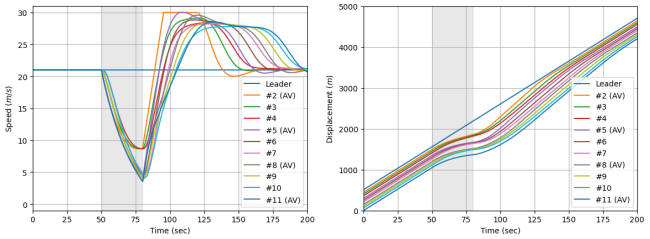
A. Scenario A

The first scenario presents a nonlinear additive attack as described in Section III-A, selected from the set $\mathcal{C}$ in



(a) Speed vs. Time (b) Vehicle position vs. Time

Fig. 3: Speed and displacement of Scenario A at 40% MPR.



(a) Speed vs. Time (b) Vehicle position vs. Time

Fig. 5: Speed and displacement of Scenario B at 40% MPR.

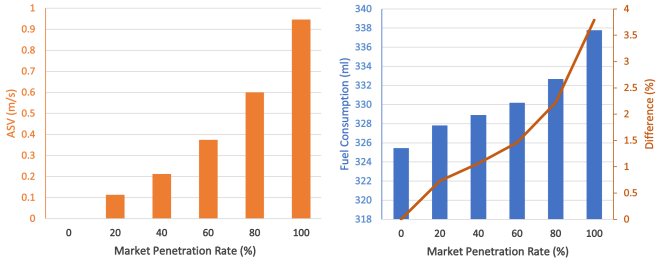


Fig. 4: ASV and FC under multiple MPRs in Scenario A.

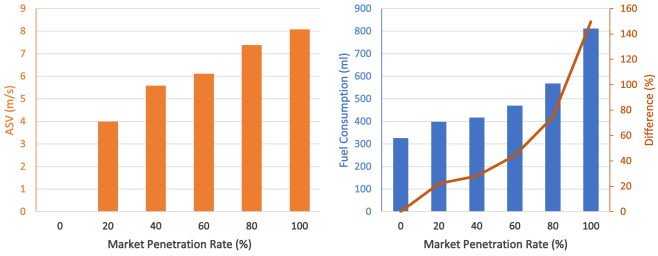
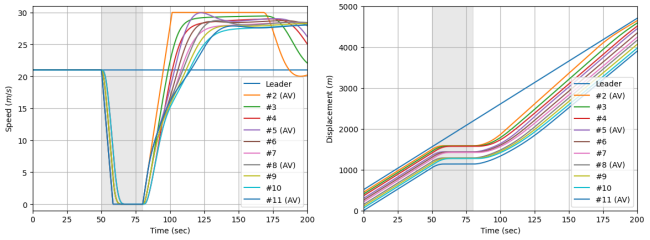


Fig. 6: ASV and FC under multiple MPRs in Scenario B.

order for it to be considered stealthy. For this scenario, the nonlinear attack takes the form: $g_1(s) = 0.1\sin(s) - 0.1s$ and $g_2(\Delta v) = 0.1\sin(\Delta v) - 0.1\Delta v$ [23]. An attack of low magnitude is created due to the low alterations of this nonlinear function resulting in small changes in measurement data. Fig. 3 displays plots of vehicle speed and position data at an MPR = 40%, with the grey area marked when the attack event takes place. As seen in Fig. 4, with more AVs under attack within a platoon, higher speed oscillations are observed in terms of ASV, resulting in increased FC. When considering a full platoon of AVs under attack the average FC increases by 3.79%. In terms of safety, at no point in time, MPR or TTC threshold is any of the vehicles in the platoon at risk. While the lack of risk caused by the attack can be seen as something positive for the involved users, it could also result in an attack harder to identify by the drivers, successfully keeping itself stealthy [7].

B. Scenario B

A different attack, slightly more severe, is taken from $\mathcal{C}$ and used for the present scenario. Different from the one seen in Scenario A, Scenario B is conformed by a linear additive attack where $g_1(s) = -0.9s$ and $g_2(\Delta v) = -0.9\Delta v$ [7]. When comparing the baseline scenario shown in Fig 2 with the results obtained at an MPR of 40% in Fig. 5a, the speed can be seen to drop significantly from 21 m/s, due to the severity of the attack. The considerable slowdown creates a significant space between the leader and the following vehicles shown in Fig. 5b. The space created between the first two vehicles causes the follower to accelerate to the maximum speed, after the attack, to reach the leader and continue following it at the desired speed. Increased aerodynamic loads and high accelerations result in greater levels of FC as described in Fig. 6. Similar to the results in Scenario A, FC grows with the rise in MPR,



(a) Speed vs. Time (b) Vehicle position vs. Time

Fig. 7: Speed and displacement of Scenario C at 40% MPR.

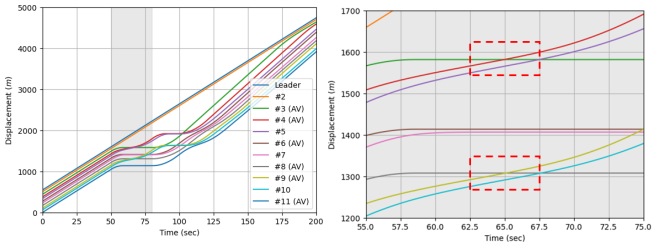
but due to the magnitude of this attack, significantly greater FC is reached, increasing by almost 150% at the maximum MPR. With harder breaks and accelerations, ASV reaches higher values indicating greater speed oscillations. Similar to the previous scenario, at no moment in time is any of the vehicles at risk of collision, meaning that safety is maintained under the dimension of this attack to remain stealthy [7].

C. Scenario C

Scenario C aims at characterizing severe non stealthy attacks outside from $\mathcal{C}$. The additive attack designed consists of $g_1(s) = -2s$ and $g_2(\Delta v) = -2\Delta v$ [7]. As shown in Fig. 7a, it is possible to observe that during the attack period, all vehicles behind the leader reach a complete stop caused by the intense deceleration of the affected AVs. Similar to the previous scenario, the space between the leader and the second car increases significantly, resulting in the following vehicles accelerating and maintaining an elevated speed for a long period of time. At greater MPRs, this attack is the only one that presents elevated values of risk due to collisions as shown in Table I and Fig. 8 highlighting the moment where two different AVs make contact with the preceding car. With a collision present, values for ASV and FC are

TABLE I: Safety results for Scenario C, shown as the percentage of time that vehicles in the platoon are at risk, under multiple MPRs and TTC thresholds.

θ	MPR					
	0%	20%	40%	60%	80%	100%
1.5s	0%	0%	0%	2.31%	3.43%	1.14%
2.0s	0%	0%	0%	2.36%	3.50%	1.17%
2.5s	0%	0%	0%	2.48%	3.61%	1.19%
3.0s	0%	0%	0%	2.65%	3.76%	1.22%
3.5s	0%	0.09%	0.13%	2.83%	3.9%	1.25%
4.0s	0%	0.18%	0.27%	2.99%	4.06%	1.28%



(a) Vehicle position vs. Time (b) Zoom on collision during attack

Fig. 8: Crash present in Scenario C at an MPR = 60%.

rendered invalid due to the unrealistic description of the trajectory after the incident. A crash would result in all the vehicles after the incident stopping since only longitudinal dynamics are considered in the simulation. Collisions in the simulation scenario are caused not only by the severity of the attack but also by the positioning of AVs in the platoon. Crashes were only observed to occur between the first two AVs in a smaller AV group, where a group refers to two or more adjacent AVs on the platoon. Collisions occur due to the characteristics of the attack presented in Section III-A. On a closer look at Fig. 8b one can see that only the second AV in a group reaches a collision, while the single AV in the sixth position remains safe. Similar results under MPRs higher than 60% are obtained, where in a group of AVs, only the second collides with the preceding AV. This is better described in Fig. 9 with a 100% MPR, where a large group of AVs follow the leader, and only the second AV collides with the first during the attack. Impacts are present in this attack due to its nature, when the affected AV's spacing is considerably small to the preceding vehicle and the speed is greater than the car in front, the attacked AV tends to accelerate, causing a rear-end collision. TTC results are presented in Table I. At low MPRs, before collisions and at conservative time thresholds, a few instances of risk from the HVs are present in the platoon. At higher MPRs, AV crashes are described by the relatively high values present at small time thresholds. Fig. 9 helps describe the lower risk percentages at 100% MPR in Table I when compared to 60% and 80%. Since accidents were observed to occur only in AV groups in this scenario, at mixtures greater than 50% HVs split AVs into more groups creating greater crashes, while at 100% only one AV group exists following the leader. More AV groups result in higher levels of risk across the platoon.

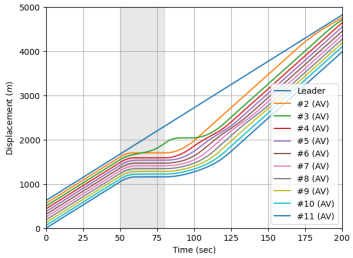
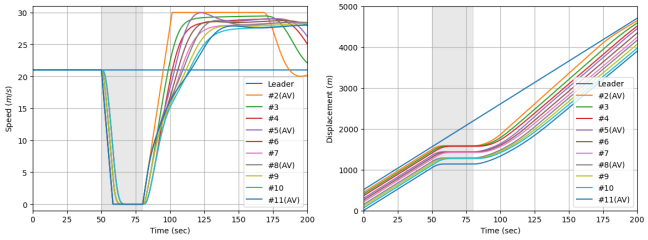


Fig. 9: Displacement for Scenario C at an MPR = 100%.



(a) Speed vs. Time (b) Vehicle position vs. Time

Fig. 10: Speed and displacement of Scenario D at 40% MPR.

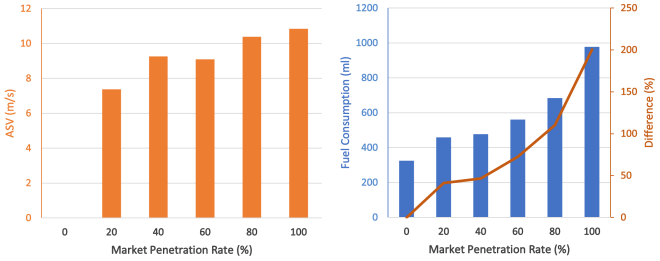


Fig. 11: ASV and FC under multiple MPRs in Scenario D.

D. Scenario D

This last scenario presents a multiplicative attack, where the data injection gets multiplied with the spacing and speed difference readings as described in Section III-B. For this scenario we consider $g_1(s) = -0.5s$ and $g_2(\Delta v) = -0.5\Delta v$. While it is not necessarily taken from $\mathcal{D}$, it follows the attack mechanism presented in Section III-B. This case presents a severe attack similar in magnitude to the one presented in Scenario C, as shown in Fig. 10, without the safety concerns of the previous attack. With a lack of incidents in Scenario D, greater impacts on traffic smoothness and FC are reached as shown in Fig. 11. Both ASV and average FC are observed to reach the greatest values of all the scenarios considered. It is noted that ASV at 40% MPR is slightly greater than at 60% MPR. This is due to AV distribution on the platoon, considered to be evenly distributed to obtain results as an average of all the different combinations. FC reaches an increase of 200.46% at 100% MPR, the greatest of all the scenarios. As mentioned previously, this attack does not cause any collisions and contains lower percentages of time at risk as described in Table II. A pattern can be seen where risk increases closer to 50% MPR and decreases farther from it. The vehicles at greater risk of collisions were observed to

TABLE II: Safety results for Scenario D, shown as the percentage of time that vehicles in the platoon are at risk, under multiple MPRs and TTC thresholds.

θ	MPR					
	0%	20%	40%	60%	80%	100%
1.5s	0%	0%	0%	0%	0%	0%
2.0s	0%	0%	0%	0%	0%	0%
2.5s	0%	0%	0%	0%	0%	0%
3.0s	0%	0%	0%	0%	0%	0%
3.5s	0%	0.09%	0.13%	0.13%	0.09%	0%
4.0s	0%	0.18%	0.27%	0.27%	0.18%	0%

be the HV behind the attacked AVs, therefore, the resulting TTC value depends on the amount of vehicle mixture. It is important to mention that even though the attack was similar in magnitude to the one in Scenario C, no crash is present in Scenario D, due to the nature of the attack making all AVs affected break at the same time and at a similar magnitude.

V. Concluding Remarks

The introduction of AVs promises to revolutionize the future of transportation reducing travel time, traffic instability, and energy consumption. While several benefits can be obtained, potential vulnerabilities remain as challenges for their adoption, which could greatly jeopardize privacy and safety. A data injection attack can modify AV sensor readings, consequently affecting platoon behavior. More importantly, a strategically designed attack can pass unnoticed, resulting in sizeable effects on traffic flow.

A series of four different attacks, with varying degrees of severity are simulated to assess the impact of cyberattacks on AVs at different MPRs. Simulation results show that greater MPRs result in higher disruptions on FC, traffic smoothness, and safety, to the point where even collisions occur due to the characteristics of certain attacks. Through simulations, this study demonstrates that strategically designed stealthy attacks can significantly degrade traffic performance. The study effectively showcases a novel approach to understanding the severe impacts of strategic attacks on a platoon across a range of metrics. While this study has examined the impact of attacks on AV longitudinal dynamics, lateral movements could also be considered in the future. The introduction of sophisticated yet stealthy attacks calls for the development of effective identification and mitigation strategies to counteract the malicious intentions of the third party involved.

References

[1] S. Wang, R. Stern, and M. W. Levin, "Optimal control of autonomous vehicles for traffic smoothing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 4, pp. 3842–3852, 2022.

[2] S. Wang, M. W. Levin, and R. J. Caverly, "Optimal parking management of connected autonomous vehicles: A control-theoretic approach," *Transportation Research Part C: Emerging Technologies*, vol. 124, p. 102924, 2021.

[3] W. Sun, S. Wang, Y. Shao, Z. Sun, and M. W. Levin, "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*, vol. 142, p. 103764, 2022.

[4] C. Dong, H. Wang, D. Ni, Y. Liu, and Q. Chen, "Impact evaluation of cyber-attacks on traffic flow of connected and automated vehicles," *IEEE Access*, vol. 8, pp. 86 824–86 835, 2020.

[5] T. Li, B. Rosenblad, S. Wang *et al.*, "Exploring energy impacts of cyberattacks on adaptive cruise control vehicles," in *2023 IEEE Intelligent Vehicles Symposium*. IEEE, 2023, pp. 1–6.

[6] S. Wang, "Planning, operation, and management of automated transportation systems: A control-theoretic approach," Ph.D. dissertation, University of Minnesota, Minneapolis, MN, December 2022.

[7] ——, "A novel framework for modeling and synthesizing stealthy cyberattacks on driver-assist enabled vehicles," in *2023 IEEE Intelligent Vehicles Symposium*. IEEE, 2023, pp. 1–6.

[8] S. Wang, M. Shang, and R. Stern, "Analytical characterization of cyberattacks on adaptive cruise control vehicles," *IEEE Transactions on Intelligent Transportation Systems*, 2024.

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

[10] J. Petit and S. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2014.

[11] K. Koscher, A. Czeskis, F. Roesner *et al.*, "Experimental security analysis of a modern automobile," in *2010 IEEE Symposium on Security and Privacy*. IEEE, 2010, pp. 447–462.

[12] M. Amoozadeh, A. Raghuramu, C.-N. Chuah *et al.*, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 126–132, 2015.

[13] S. Dadras, 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*, 2015, pp. 167–178.

[14] F. Wang and Y. Chen, "Resilient flocking control for connected and automated vehicles with cyber-attack threats," *ASME Letters in Dynamic Systems and Control*, vol. 1, no. 3, 2021.

[15] P. Wang, X. Wu, and X. He, "Modeling and analyzing cyberattack effects on connected automated vehicular platoons," *Transportation Research Part C: Emerging Technologies*, vol. 115, p. 102625, 2020.

[16] T. Li, M. Shang, S. Wang *et al.*, "Detecting stealthy cyberattacks on automated vehicles via generative adversarial networks," in *IEEE 25th International Conference on Intelligent Transportation Systems*. IEEE, 2022, pp. 3632–3637.

[17] R. E. Wilson and J. A. Ward, "Car-following models: Fifty years of linear stability analysis-a mathematical perspective," *Transportation Planning and Technology*, vol. 34, no. 1, pp. 3–18, 2011.

[18] Y. Ye, J. Sun, and J. Sun, "Car-following characteristics of commercially available adaptive cruise control systems and comparison with human drivers," *Transportation Research Record*, 2022.

[19] M. Treiber, A. Hennecke, and D. Helbing, "Congested traffic states in empirical observations and microscopic simulations," *Physical Review E*, vol. 62, no. 2, pp. 1805–1824, 2000.

[20] V. Milanés, S. E. Shladover, J. Spring *et al.*, "Cooperative adaptive cruise control in real traffic situations," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 1, pp. 296–305, 2013.

[21] S. Wang, M. W. Levin, and R. Stern, "Optimal feedback control law for automated vehicles in the presence of cyberattacks: A min-max approach," *Transportation Research Part C: Emerging Technologies*, vol. 153, p. 104204, 2023.

[22] T. Li, S. Wang, M. Shang, and R. Stern, "Can cyberattacks on adaptive cruise control vehicles be effectively detected?" in *2024 IEEE Intelligent Vehicles Symposium*. IEEE, 2024, pp. 323–328.

[23] S. Wang, "An analytical framework for modeling and synthesizing malicious attacks on ACC vehicles," *arXiv:2401.06916*, 2024.

[24] S. Wang, M. Shang, M. W. Levin, and R. Stern, "A general approach to smoothing nonlinear mixed traffic via control of autonomous vehicles," *Transportation Research Part C: Emerging Technologies*, vol. 146, p. 103967, 2023.

[25] K. Ahn, H. Rakha, A. Trani, and M. Van Aerde, "Estimating vehicle fuel consumption and emissions based on instantaneous speed and acceleration levels," *Journal of Transportation Engineering*, vol. 128, no. 2, pp. 182–190, 2002.

[26] J. C. Hayward, "Near miss determination through use of a scale of danger," 1972.