The Disbanding Attack: Exploiting Human-in-the-loop Control in Vehicular Platooning *

Ali Al-Hashimi[1], Pratham Oza[2], Ryan Gerdes[2], and Thidapat Chantem[2]

[1] Utah State University, Logan UT 84321, USA
[2] Virginia Tech, Arlington VA 22203, USA
ali.2014@aggiemail.usu.edu
{prathamo,rgerdes,tchantem}@vt.edu

Abstract. Due to advances in automated vehicle technology and inter-vehicle communication, vehicular platoons have attracted a growing interest by academia and industry alike, as they can produce safe driving, regularize traffic flow, and increase throughput. Research has demonstrated, however, that when platoons are placed in an adversarial environment, they are vulnerable to a variety of attacks that could negatively impact traffic flow and produce collisions and/or injuries. In this work, we consider an attack that seeks to exploit human-in-the-loop control of compromised vehicles that are part of a platoon. Specifically, we demonstrate that should a human operator need to suddenly take control of a platooned vehicle, significant upstream effects, which threaten the safety of passengers in other vehicles, may be induced. To counter this so-called disbanding attack, we present an optimal centralized mitigation approach. Due to scalability, security, and privacy concerns, such an approach may not be practical in reality. Hence, we also propose a decentralized mitigation algorithm that reduces excessive speed changes and coordinates inter-platoon behaviors to minimize the attack impacts. Our algorithm is compared to the aforementioned optimal approach and is shown to produce nearly equivalent results while requiring fewer resources. Experimental results on a hardware testbed show that our countermeasure permits graceful speed reductions and can provide safety, i.e., no collisions.

Keywords: vehicular platoons, attacks on vehicular platoons, mitigation of attacks.

1 Introduction

Vehicular platooning is an automation technology wherein a number of vehicles are grouped together to follow each other closely and safely. This technology has been shown to provide a safe and comfortable experience that will ultimately allow passengers to focus on tasks other than driving [11]. It also enables vehicles

* This grant was supported in part by NSF under grant number CPS-1658225.

to safely navigate at a closer distance, compared to human-driven vehicles, which improves traffic throughput and reduces congestion [29], and can help to improve fuel consumption [21]. Vehicle platooning is an example of a cyber-physical system (CPS) since it requires an integration of computation, communication, and monitoring capabilities to control a physical process. Adaptive Cruise Control (ACC) and Cooperative Adaptive Cruise Control (CACC) are the most well-known control strategies used to form and maintain platoons. ACC operation consists of using locally available information to generate appropriate acceleration commands to maintain a preset inter-vehicle separation and speed (longitudinal control). CACC, on the other hand, is an extension of ACC that employs vehicle-to-vehicle (V2V) communication, so that vehicles may exchange state information, and is able to achieve smaller inter-vehicle separations [27].

The Society of Automotive Engineers (SAE) and the National Highway Traffic Safety Administration (NHTSA) have defined levels of vehicular automation. Based on their criteria, vehicle manufacturers have been able to produce vehicles with level 2, e.g., BMW, and Ford ,or level 3, e.g., Tesla, capabilities [32]. In level 2, automated vehicles can generate both longitudinal (accelerating/decelerating) and lateral (steering) control commands. This level also requires humans to monitor the road and readiness to assume control if needed. Level 3 provides more automated functionalities in terms of generating control commands and monitoring the driving environment, though it also requires human driver readiness to assume control [7]. Platooning without human oversight, a level 4 technology, is not yet a reality due to the lack of robustness in V2V communications, the cost and number of sensors required to monitor the environment, and unresolved questions regarding unexpected maneuvers on the part of other vehicles on the road [2]. Therefore, current platooning automation technology falls into the category of level 2 or level 3, and human attention is still required in the platooned vehicles in case they need to take control of the vehicles.

Transition of control is defined as the process of switching control, of an automated vehicle, to a human driver when the automated system cannot handle certain situations; e.g., a vehicle emerging from a side road abruptly and merging onto a highway without notice, oncoming traffic turning left to enter a side road and crossing an automated vehicle's path, a car parking on the road and partially blocking the roadway [23, 32], or a technical failure in one or more components of the vehicle's automation system [36]. Such failures could stem from the deliberate manipulation of the automated system components such as sensors, actuators, or inter-vehicle communication [4]. A number of previous studies analyzed human driver behaviors post transition of control and their results have shown that some drivers apply maximum deceleration to handle certain situations, e.g., avoid colliding with preceding vehicles [22, 17]. These studies also determined the time required to ensure a safe transition [15, 23].

A platooning CPS (typically) employs a distributed controller that uses information from both local sensors and those obtained through inter-vehicle communications or connections to external networks [24]. As a result, a platooning CPS has a large attack surface by which an attacker could induce disruptive

and/or fatal behaviors [16, 12, 13, 31, 14]. Attacks mounted against a platooning CPS can lead to the disruption of the steady-state operation (i.e., desired inter-vehicle separation and relative speed) and produce harmful effects, such as collisions or uncomfortable acceleration/deceleration, which could lead to, for example, chronic traffic jams. Also, attacks on platooned vehicles could induce a transition of control which, in turn, will disband (dissolve) the platoon since the latter is no longer automated nor complies with platooning control laws. While the security of platooning CPS has been studied from many perspectives, so far the exploitation of the human element has been left unexplored.

In the current work we examine, from an adversarial perspective, the aftereffects of automated vehicles transitioning their control to humans. Particularly, we are interested in analyzing the upstream effects of all vehicles in a platoon transitioning control to human operators (a process we refer to as the platoon disbanding) due to a system failure resulting from an attack. Although disbanding may seem a sensible fail-safe solution to prevent attackers from achieving their objective of influencing automated vehicles, we will show that transition of control can be leveraged to undermine the operation of surrounding vehicles, cause collisions, and/or induce massive congestion. The main contributions are:

- We study the effect of a "disbanding attack" that involves transition of control of multiple vehicles in a platoon. We show the harmful impacts such an attack can induce, especially how it can cause upstream (non-attacked) platoons to experience slowdowns and collisions.
- We define the disbanding attack by formulating it as an optimization problem where the objective is to maximize the deviation in vehicles' speeds, as a proxy for slowdowns and increased chances of colliding, by selecting platoon(s) to be disbanded and time(s) of disbanding.
- To mitigate the aftermath of such an attack, we formulate an optimal solution using a Model Predictive Control (MPC) technique. However, since the optimal approach is not scalable in practice, as it is centralized and information and communication intensive, we also propose a heuristic algorithm to be used locally by vehicles of intact (non-attacked) platoons. Our findings indicate that our algorithm produces nearly equivalent results in terms of reducing speed changes and avoiding accidents.
- We also demonstrate the validity of the above attack and the suggested heuristic countermeasure using experiments on a hardware testbed consisting of a motion capture system and small mobile robots acting as vehicles.

1.1 A motivating example

Let us consider a scenario where multiple vehicular platoons are traveling in the same direction on a highway. Although they may not be heading to the same destination, platoons drive and follow one another in order to reap platooning benefits of optimizing traffic flow and reducing congestions. While the platoons are operating at a steady-state, a malicious party utilizes one of the existing external attack techniques [31, 19] in order to cause accidents. For example, the

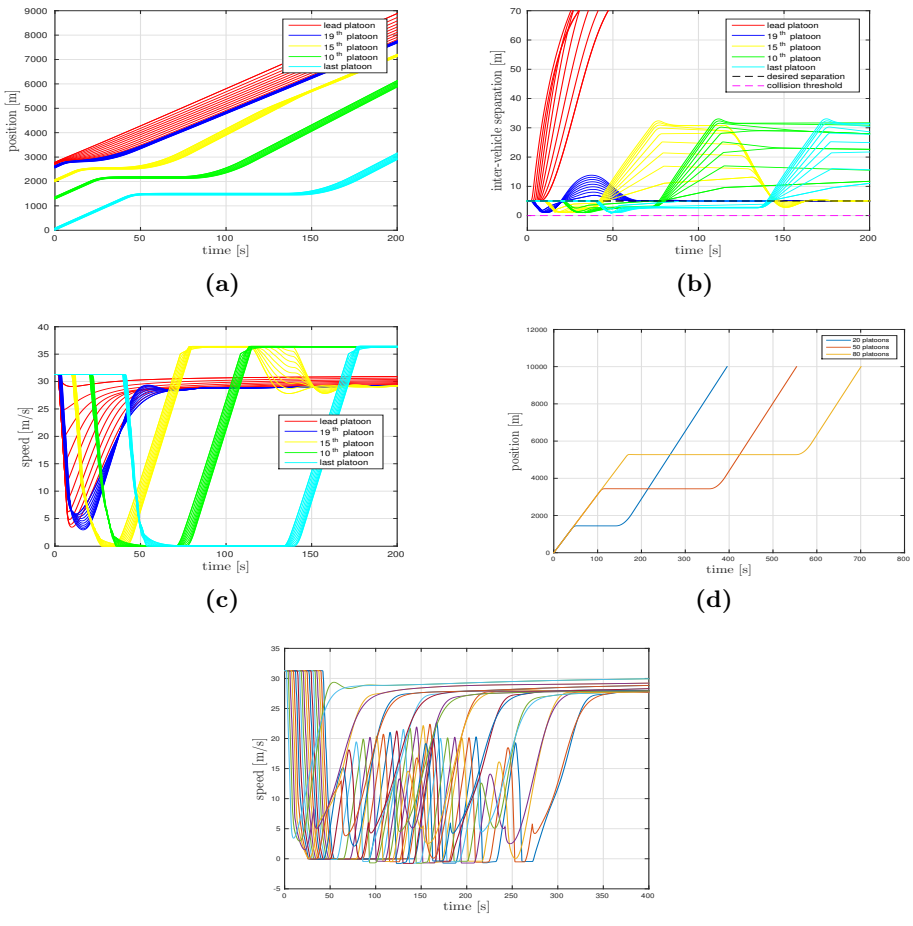


Fig. 1. a) Position profiles of the platoons shown in the legend. The lead platoon started disbanding at t = 2 s. b) Inter-vehicle separation profiles of the platoons shown in the legend. The lead platoon started disbanding at t = 2 s. c) Speed profiles of the platoons shown in the legend. The lead platoon started disbanding at t = 2 s. d) Position profile of the rear vehicle in the platoons formation, whose size is shown in the legend. e) Speed profiles of the rear vehicles belonging to a twenty-platoon formation when multiple platoons start disbanding at different time instances.

attacker could install units on the roadside that are able to jam the sensors of multiple vehicles or modify the sensor measurements so that the targeted vehicles start behaving irregularly [25]. At this point, either the automation system will suffer a failure and, as a result, informs the driver, by sounding an auditory alarm for example [22], or the attack is detected by a mechanism, already designed for such purpose, or by a passenger, who observes an erratic behavior in the vehicle's

motion. In any case, the driver must assume control of the vehicle and apply the brakes [36]. As a result, the attacked platoon is effectively disbanded as the vehicles no longer comply with platooning laws and the mounted attack fails to achieve its goals. However, intact upstream platoons, which were not the goal of the mounted external attack, will also exhibit unexpected behavior as a result of disbanding such as slowing down and coming to a complete stop, which creates discomfort for passengers, or even colliding.

Figure 1a shows the position profiles of a selected platoon, out of 20, whose indices are shown in the legend. Each platoon has ten vehicles. The lead (20^{th}) platoon (red), which constitutes 5% of the total number of vehicles, transitions its control after being attacked at t = 2 s. We can see how the lead platoon begins disbanding when the inter-vehicle separations, shown in Figure 1b, are no longer 5 m (the desired separation) and the platoon manages to avoid accidents. Also, Figure 1c indicates that the vehicles of the disbanded platoon initially slow down and then begin to speed up. In response to the lead platoon being disbanded, we can see in Figure 1c that the following (still automated) 19^{th} intact platoon (blue) also begins to slow down. In addition, Figure 1b shows that the inter-vehicle separation of the 19^{th} platoon is also affected as it decreases when slowing down happens, but not below 0 m, starts increasing to above 10 m when speeding up happens, and eventually reaches to 5 m after almost one minute.

The same effect that was induced in the 19^{th} platoon will propagate through the rest of the following platoons. For example, the 15^{th} platoon (yellow) started decelerating until all vehicles completely stopped, as shown in Figure 1c, for almost 30 seconds and then the platoon's lead vehicle started accelerating, reaching maximum speed of 36 m/s, in order to decrease the gap with respect to the preceding 16^{th} platoon (not shown in plots) and eventually slowed down, as it is approaching the preceding platoon, after almost two minutes (These action of accelerating/decelerating result from the adopted automation control laws responding to the behavior of the preceding platoon). We can also see the same behavior in Figure 1b where the inter-vehicle separation of the 15^{th} platoon decreased, increased, and then settled at 5 m. The same pattern also shows on the 10^{th} (green) and last (cyan) platoons but longer times were needed to regain the inter-vehicle separations and speeds. For this specific case of disbanding attack, 10 minutes were needed such that all of the affected platoons were able to re-establish (recover) the desired separations and speeds. Furthermore, figure 1d shows the absolute position of the last vehicle in the traffic stream, for different number of platoons, when the lead platoon was disbanded. We can see that as the number of platoons increases, the vehicle stops for a longer time and then resumes moving. Furthermore, the string of 20, 50, and 80 platoons, needed 10, 25, and 43 minutes, respectively, to recover. In summary, we can see in these plots that disbanding one platoon could make the following platoons respond irregularly such that they stop-and-go which in turn creates discomfort for passengers, traffic jams, inefficient use of the road, and fuel waste.

Alternatively, being aware of such effects, the attacker can target more than one platoon systematically and produce worse impacts such as multiple stop-

and-go behaviors. For example, the attacker can induce disbanding by targeting every other platoon, out of twenty, at regular intervals, with 30 s increments (Figure 1e). For the speed profiles shown in Figure 1e, 65%, 45%, and 37.5% of the intact platoons were forced to stop-and-go once, twice, and three times, respectively. Also, 55% of the vehicles, in the intact platoons, suffered collisions.

1.2 Related work

The objective of vehicular platooning is to combine multiple vehicles and design the proper controllers to maintain a desired separation and speed [6]. A large amount of work can be found in literature addressing how to achieve that objective. Also, different spacing policies are proposed to implement control laws that regulate the relative spacing either in front of vehicle (unidirectional control) or on both front and rear of vehicle (bidirectional control) [27]. This is achieved using either only locally sensed information or with the addition of (V2V) communication [34]. Communication schemes are proposed in [3] to transmit messages between adjacent vehicles. Also, it is possible to exchange vehicles' information by establishing vehicle-to-infrastructure (V2I) communication with road units designed for that purpose [10]. In this work, we adopt a proportional-derivative controller from [34] to form our platoons with the presence of a forward-looking V2V communication in order to implement our suggested attack mitigation (Section4).

Vehicular platoons security has been the focus of extensive research in literature. For example, [13] presents a number of insider attacks that target the vehicles' CACC controllers and suggests detection schemes for those attacks. Another insider attack work is [12] where the attacker's controlled vehicle is able to modify its controller's gains such that generated commands induce instability in the entire platoon. [16] shows that it is possible for a malicious vehicle in the platoon to increase the energy consumption unnecessarily in the neighboring vehicles by misbehaving. In [14], it is shown that multiple attacker vehicles can operate within the platoon and coordinate their behavior in order to produce instability that could lead to accidents. Alternately, other work investigate external attacks where local range and range-rate sensors are targeted, to misinform the vehicle of the surrounding vehicles' information to negatively impact road efficiency and passengers' comfort and safety [31, 19]. Similar to the security related works above, we also present a possible vulnerability in vehicular platoons and analyze its impacts on platoon safety. However, ours is the first work that considers the effect the presence of human control in the platoon can produce. Specifically, we try to answer: "what happens if control of multiple vehicles transition to human because to disruption of their automated systems?" or "what happens if a passenger decides to assume command of a vehicle after observing irregular behavior, owing to an already mounted attack, in its motion?". Naturally, once a human driver starts controlling the vehicle, brakes will be applied in an attempt to slow down the vehicle [36]. While such an action is helpful in avoiding accidents, it will also generate instability in the following non-attacked platoons that could lead to collisions.

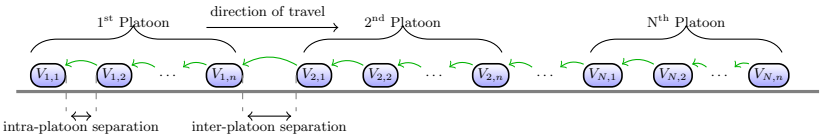


Fig. 2. A stream of n-vehicle N platoons. Green arrows represent the flow of transmitted information.

1.3 Organization

Section 2 explains the vehicular platooning control laws and describes the threat model. Section 3 discusses different optimal attack scenarios and analyze their impacts. Section 4 presents effective attack countermeasures. Experimental results are presented in Section 5. Conclusions are given in Section 6.

2 System Model

The modeling of platoon dynamics and control as well as the attack mechanism are discussed in this section.

2.1 Vehicle and platoon models

We consider N homogeneous platoons, where every vehicle uses the same control law, with n vehicles in each (lead vehicle is indexed as n while the last vehicle is indexed as 1) as shown in Figure 2. Each vehicle is equipped with front and rear range and range-rate sensors, to measure corresponding relative distances and speeds of surrounding vehicles, and implements an upper-level controller, responsible for determining the commanded (desired) acceleration, and a lower-level controller, which uses the desired acceleration to determine throttle and brake commands. The lower-level controller is expected to achieve the desired acceleration with some delay due to its finite bandwidth [27, 24]. We will focus on the upper-level controller since the attacker can easily affect it (e.g., through attacks on sensors). The following model is used to simulate the dynamics of each j^{th} vehicle in the i^{th} platoon

$$\begin{bmatrix} \dot{x}_{i,j}(t) \\ \dot{v}_{i,j}(t) \\ \dot{a}_{i,j}(t) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & \frac{-1}{\tau} \end{bmatrix} \begin{bmatrix} x_{i,j}(t) \\ v_{i,j}(t) \\ a_{i,j}(t) \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\tau} \end{bmatrix} u_{i,j}(t), \tag{1}$$

where x, v a, and u refer to the vehicle's absolute position, velocity, acceleration, and commanded acceleration, respectively, and τ is a time constant used to model the actuator's delay.

In this work, vehicles in a platoon use a bidirectional control technique [34] with two major benefits. First, it is able to guarantee platoon string stability to maintain desirable traffic flow [27, 34]. Second, it does require vehicle-to-vehicle (V2V) transmitted information to generate periodic control commands. We do, however, assume intermittent wireless communication is possible between vehicles for attack detection and to transmit data for the mitigation process (Section

4). These require a data rate far lower than that required to maintain V2V-enabled platoons. For the last vehicle in the i^{th} platoon, we have

$$u_{i,1}(t) = k_p\big(x_{i,2}(t) - x_{i,1}(t) - x_d\big) + k_d\big(v_{i,2}(t) - v_{i,1}(t)\big), \tag{2}$$

where k_p and k_d are the controller's proportional and derivative gains, respectively, and x_d is a constant denoting inter-vehicle desired separation. For the other vehicles in the i^{th} platoon, except the leader, we have

$$\begin{aligned} u_{i,j}(t) = k_p\big\{\big(x_{i,j+1}(t) - x_{i,j}(t) - x_d\big) - \big(x_{i,j}(t) - x_{i,j-1}(t) - x_d\big)\big\} \\ + k_d\big\{\big(v_{i,j+1}(t) - v_{i,j}(t)\big) - \big(v_{i,j}(t) - v_{i,j-1}(t)\big)\big\}, \end{aligned} \tag{3}$$

A different control structure is adopted for the platoons' lead vehicles since we expect that the platoon may encounter other platoons as they travel on the road. Lead vehicles attempt to maintain a desired separation and speed, with respect to a preceding vehicle, by using a control law given by [27]

$$u_{i,n}(t) = k_p\big(x_{i+1,1}(t) - x_{i,n}(t) - h.v_{i,n}(t)\big) + k_d\big(v_{i+1,1}(t) - v_{i,n}(t)\big), \tag{4}$$

where h is a time headway constant. Also, each lead vehicle is equipped with a transitional controller which is engaged in cases it encounters a slowly moving vehicle or a slowly driving platoon on the road. Interested readers are referred to [27] for more details on transitional controllers.

We are interested in studying the effect of control transition. Therefore, we will adopt the Intelligent Driver Model (IDM) [20], which can be used to approximate human driving behavior, to simulate the dynamics of control transitioned vehicle(s). The commanded acceleration of the disbanded platoon vehicles is calculated using

$$\begin{aligned} u_{i,j}(t) &= u_{\max}\big\{1 - \big(v_{i,j}(t)/v_d\big)^4 - \big(s^*(t)/(x_{i,j+1}(t) - x_{i,j}(t))\big)^2\big\}, \\ s^*(t) &= r_0 + v_{i,j}(t)\big\{\ h + (v_{i,j}(t) - v_{i,j+1}(t)/(2\sqrt{u_{\min}u_{\max}})\big\}, \end{aligned} \tag{5}$$

where v_d is the desired velocity, $u_{\min}$, $u_{\max}$ are minimum and maximum acceleration, respectively, and r_0 is the minimum inter-vehicle separation (a vehicle cannot move if the separation is smaller than r_0).

Finally, we assume that all vehicles are equipped with a collision-avoidance technique where $u_{\min}$ will be applied when the following condition is true [3, 27]

$$x_{i,j+1}(t) - x_{i,j}(t) \leq r_0 + \big(v_{i,j}^2(t) - v_{i,j+1}^2(t)\big)/2u_{\min}. \tag{6}$$

2.2 Threat model

The aim of the disbanding attack in a multi-platoon scenario is to induce collisions in some platoons, by targeting one or more vehicle(s) in a different platoon, and disrupting traffic flow. This type of attack relies on compromising some aspect of a vehicle's automation system so as to force the vehicle to abandon automated operation, i.e., transition of control, and hence cause the platoon to which

it belongs to disband. The action of disbanding, in turn, will impact upstream platoons. As stated earlier, the level of automation provided by the currently available automation technology is still not highly autonomous. Therefore, it is still expected that human drivers will need to take control of the automated vehicles during certain situations.

One possible attack vector that could be leveraged to compromise a vehicle's automation, and force a transition of control, is to target the vehicle's front and/or rear facing sensors that are relied upon to perceive the relative distance and speed of neighboring vehicles. Existing work has demonstrated that LIDAR, RADAR, camera, and ultra-sonic sensors, which are the most often used sensors in automated vehicles for these purposes, can be jammed or spoofed. In addition, such attacks can be targeted, easy to carryout, accomplished at a distance, and mounted against multiple vehicles at once [9, 25, 33, 35].

To demonstrate the impacts of the disbanding attack in our study, we assume that the attacker has the capability to target the sensors of either one or multiple automated vehicles belonging to one or more platoons. Also, we assume that the mounted attack succeeds in degrading the sensing functionality of the automation system(s) employing the targeted sensor(s). We consider two possible scenarios resulting from the attack. In the case where a sensor of a single vehicle in a platoon is targeted and its automation compromised, the vehicle will utilize V2V communications and alert the other vehicles in that platoon so that they begin to transition their control[1]. In the case of targeting the sensor(s) of all vehicles in a platoon, the automation systems of those vehicles will suffer the disruption of the sensors operation, become unable to handle the current situation, and also begin the process of transition of control. In either case, the automated vehicles are forced to transition their control in an attempt to mitigate the attack and avoid accidents, effectively disbanding the platoon.

Although the process of disbanding a platoon can help with avoiding accidents, the resulting action of braking will cause upstream effects on intact (non-attacked) platoons. Those effects pose a threat to the safety of these platoons, as they cause sudden and excessive velocity changes that could lead to collisions. Disbanding attacks are extremely effective since attack-resilient platooning controllers tend to ignore human intervention in the design process.

3 Human-in-the-loop Attacks

In this section, the disbanding attack is formulated as an optimization problem in order to find optimal attacks. Then, the simulation setup to carry out such an attack is explained.

3.1 Finding optimal disbanding attack

Given the attacker's capabilities and platoon dynamics as described in Section 2, the goal of the attacker is to find which platoon(s) and at what time(s) vehicles'

[1] Disbanding (dissolving) a platoon when one vehicle reverts to manual control has been recommended in actual platooning systems [30].

sensors should be attacked to induce disbanding, such that the velocity deviation of all intact vehicles is maximized, which is a fair indication of throughput and probability of collisions. To assess the impacts of disbanding attacks on platoons, we use the following metrics

- Average velocity error (deviation) describes the non-attacked platoons' slowing down as a result of disbanding another platoon(s). For the j^{th} vehicle in the i^{th} platoon, the average velocity error is defined as

$$E_v = \frac{1}{|T_s|} \sum_{k=1}^{|T_s|} \frac{|v_{i,j}(t_k) - v_d|}{v_d} \cdot 100, \tag{7}$$

  where T_s is the attack window (in seconds), and v_d is desired speed. Since we are considering platoons, equation (7) is modified as follows

$$E_v = \frac{1}{N \cdot n \cdot |T_s|} \sum_{i=1}^{N} \sum_{j=1}^{n} \sum_{k=1}^{|T_s|} \frac{|v_{i,j}(t_k) - v_d|}{v_d} \cdot 100, \tag{8}$$

  by which E_v is calculated for all vehicles $(N \cdot n)$ throughout T_s.
- Collisions: although each vehicle is assumed to be equipped with a collision-avoidance algorithm, crashes between some of the intact vehicles can still occur. Therefore, we will indicate whether the considered attack scenario involves collisions or not.

Let $\boldsymbol{p_d}$ be a vector of indices of platoons to be disbanded, and $\boldsymbol{t_d}$ a vector of times of disbanding. The attacker will solve the following optimization problem

$$\begin{aligned} \underset{\boldsymbol{p_d}, \boldsymbol{t_d}}{\text{maximize}} \quad & E_v = f(\boldsymbol{p_d}, \boldsymbol{t_d}) \\ \text{subject to} \quad & 1 \leq \boldsymbol{p_d} \leq N \\ & 1 \leq \boldsymbol{t_d} \leq T_s \\ & \boldsymbol{p_d}(i_1) \neq \boldsymbol{p_d}(i_2) \text{ for } i_1, i_2 = 1, \ldots, \text{ no. of targeted platoons} \end{aligned} \tag{9}$$

Equation (9) should be interpreted as follows: given a number of targeted platoon(s), the attacker seeks the best values for $\boldsymbol{p_d}$ and $\boldsymbol{t_d}$ such that the highest

Table 1. Parameters used in the simulations.

Parameter	Value	Description
N	[2:10]	number of platoons
n	10	number of vehicles per platoon
k_p	1	controller's proportional gain
k_d	5	controller's derivative gain
x_d	{5,4} m	desired inter-vehicle separation
v_d	31 m/s	nominal velocity
h	1.5 s	time headway
τ	{0.1,0.3,0.5} s	time-lag constant
$v_{\max}$	36 m/s	maximum velocity
$v_{\min}$	0 m/s	minimum velocity
$u_{\max}$	1 m/s^2	maximum acceleration
$u_{\min}$	-5 m/s^2	minimum acceleration
r_0	1 m	minimum inter-vehicle separation
T_s	180 s	simulation time

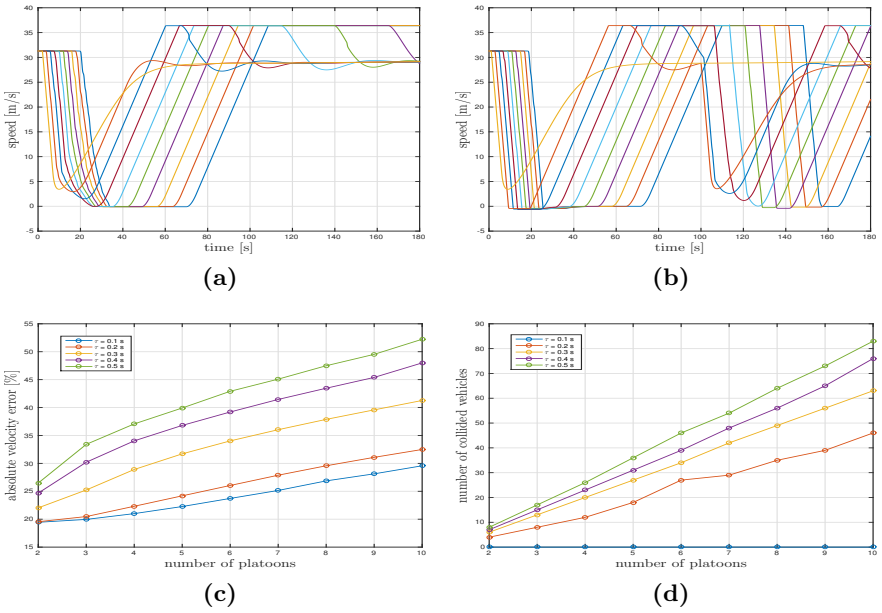


Fig. 3. a) Speed profiles of platoons' rear vehicles (N = 10) when the lead platoon started disbanding at t = 2 s. b) Speed profiles of platoons' rear vehicles (N = 10) when the 9^{th} and 10^{th} platoons started disbanding at t = 2 s and 100 s, respectively. c) Average velocity error for optimal single-platoon disbanding cases. d) Number of collided vehicles for optimal single-platoon disbanding cases.

value for the cost function, E_v, will result. The constraints of the problem ensure that values of $\boldsymbol{p_d}$ and $\boldsymbol{t_d}$ are within bounds and the same platoon cannot be disbanded twice (in case of multi-platoon disbanding). We used the Genetic Algorithm (GA) Toolbox in MATLAB to solve equation (9).

3.2 Simulation setup

For the theoretical results presented in this work, we used MATLAB to simulate a string of platoons, using the control algorithms and dynamics from Section 2.1. Table 1 indicates the setup used in all subsequent simulations. Following previous work, the value of τ was selected to be either 0.1 s [18] or 0.5 s [27]. To generalize the problem, we also simulated values in-between.

To produce realistic simulations, all vehicles' velocities are constrained to be below or equal to a maximum value and all vehicles move only forward (no negative velocities). Also, the acceleration is bounded within minimum and maximum values. Since vehicles' responses to initial separations and velocities may result in some overshoot before reaching the steady-state, all simulations were started at the steady-state so that transient response will not interfere with the attack impacts.

3.3 Results

Two different cases of the disbanding attack are shown in Figure 3a and in Figure 3b (for the disbanding the lead platoon and two foremost platoons, respectively, out of 10). Results are shown in terms of the absolute speed of the last/rear vehicles of intact platoons (legends are removed to reduce visual clutter). We see that disbanding results in not only slowdowns, and hence deviation form a desired speed of 31 m/s, but even complete stops. This behavior is captured by calculating E_v using (8), which is equal to 29.57% for Figure 3a and 43.69% for Figure 3b. For Figures 3c and 3d, the total number of platoons (N) is varied between two and ten (shown on the x-axis), an actuator delay, τ, varied between 0.1–0.5 s, with an increment of 0.1 s, and a time headway (h) equal to 1.5 s.

For each value of N, the solution of (9) indicated that the optimal attack occurred by disbanding the lead platoon at one second (beginning of attack window). Figure 3c shows the optimal (maximum) average velocity error (E_v) for disbanding the lead platoon and for different values of τ. We can see clearly that more severe attack impacts are induced as the total number of platoons increases. Although all vehicle are equipped with an appropriate collision-avoidance algorithm, simulation results indicate that disbanding attacks can also cause accidents between some of the vehicles in the intact platoons, which were not the target of the attack. Figure 3d shows the number of colliding vehicles for each one of the optimal disbanding attack cases displayed in Figure 3c. We can see that collisions occur when actuator delay is greater than 0.1 s, regardless of N, and that the total number of accidents increases as the total number of platoons increases as well.

4 Attack mitigation

We propose two approaches, each of which proactively adjusts the commanded acceleration profiles of intact platoons' vehicles, in an attempt to mitigate attack impacts by lessening the velocity deviations and reducing the number of collisions, if possible. By using the proposed approaches, the automation of intact platoons is maintained and no transition of control will be initiated.

4.1 Optimal mitigation

The mitigation of the disbanding attack is formulated as an optimization problem. Model-Predictive Control (MPC) is used to find an on-line solution using receding horizon [28]. The MPC based formulation is an optimal control technique that has been used successfully in several different applications [5]. It is based on minimizing a cost function (e.g., velocity deviation) in order to achieve a certain goal (e.g., mitigating disbanding attack impacts), while considering performance and physical constraints (e.g., collision-avoidance and speed and acceleration bounds). As such, this optimal approach will be used to compare and evaluate the performance of the heuristic approach suggested in Section 4.2, as this approach requires more computational power and connected infrastructure to perform the calculations required to carryout the mitigation.

Our objective is to compute a control sequence that will command each vehicle behind the disbanded platoon to reduce the deviation in velocity and avoid accidents. More specifically, the controller of an intact vehicle will use current measurements of velocity and acceleration in order to solve

$$\min_{\mathbf{U}} \quad 2\mathbf{M_1U} + \mathbf{U}^T\mathbf{M_2U} \tag{10}$$

$$\text{s.t.} \quad \mathbf{M_3U} \leq \mathbf{M_4}, \tag{11}$$

where $\boldsymbol{U}$ is the resulting control sequence and $\boldsymbol{M_1}$, $\boldsymbol{M_2}$, $\boldsymbol{M_3}$, and $\boldsymbol{M_4}$ are matrices formulated to consider acceleration and physical speed limits, and collision avoidance. The complete formulation is omitted due to space limit.

While this approach would yield an optimal solution for every time instance, it requires global knowledge of the platoon dynamics. Namely, to perform the calculations needed to produce $\boldsymbol{U}$ (control input to command intact vehicles), speed and acceleration measurements of all related vehicles should be available to a centralized controller; i.e., V2I and I2V capabilities are needed to receive current measurements, perform the required calculations, and transmit the resulting acceleration commands back to the corresponding vehicles. It has been shown that such communication structure is feasible [10], but not likely to be deployed in the near term and presents a single-point of failure. For that reason, in the next section we suggest an efficient, decentralized heuristic mitigation approach which requires a less sophisticated communication model and produces nearly equivalent results to the optimal approach.

4.2 Efficient heuristic mitigation

The goal of this approach is to modify the commanded acceleration of a vehicle by comparing the distance it will cover with the distance that will be covered by the preceding vehicle during a predefined time horizon (t_s). Initially, the acceleration commands of both vehicles are calculated according to the platooning control structures given in Section 2.1.

Let us consider a vehicle in an intact platoon $V_{current}$ and a preceding vehicle $V_{preceding}$, where subscripts *current* and *preceding* refer to two adjacent vehicles belonging either to the same platoon or to two different adjacent platoons. Each vehicle's dynamics are described by

$$\begin{aligned} \dot{x}_m(t) &= v_m(t), \\ \dot{v}_m(t) &= u_m(t), \end{aligned} \tag{12}$$

where $m \in \{current, preceding\}$, $t \in [t_s(1) : \Delta t_s : t_s(end)]$, $t_s(1)$ and $t_s(end)$ are the first and last time samples of the time horizon t_s, and Δt_s is the time increment. Under the assumption that u_m is constant for the duration of t_s and using the forward difference approximation [8], the absolute position and velocity can be calculated as follows

$$\begin{aligned} x_m\big(t_s(k+1)\big) &= x_m\big(t_s(k)\big) + \Delta t_s v_m\big(t_s(k)\big), \\ v_m\big(t_s(k+1)\big) &= v_m\big(t_s(k)\big) + \Delta t_s u_m, \end{aligned} \tag{13}$$

Algorithm 1: Heuristic mitigation

Input: $v_m(t_s(1)), u_m(t_s(1))$, for $m \in \{current, preceding\}$ // velocity and commanded acceleration values of current and preceding vehicles.
Output: $u^{new}_{current}$, // new commanded acceleration value for current vehicle.
$u^{new}_{current} \leftarrow u_{current}(t_s(1))$;
compute d_m for the interval of t_s using input data;
if $d_{preceding} < d_{current}$ **then**
  $u^{new}_{current} \leftarrow \frac{d_{preceding} - v_{preceding}\left(t_s(end) - t_s(1)\right)}{0.5\left(t_s^2(end) - t_s^1(1)\right)}$;
  if *current vehicle and preceding one will collide during* t_s **then**
    search for $u^{new}_{current}$ within $\left[a_{min}, u_{preceding}\right)$;

where $k = 1, \ldots, |t_s|$.

Once the vector $x_m(.)$ is obtained, the distance traveled by vehicle V_m during t_s can be calculated as $d_m = x_m\big(t_s(end)\big) - x_m\big(t_s(1)\big)$. Based on the calculated distance traveled by the current vehicle $d_{current}$ and that by the preceding one $d_{preceding}$, we proceed as follows

- If $d_{preceding} < d_{current}$, then $V_{current}$ is covering more distance and it may collide with a preceding vehicle and therefore it has to slow down by modifying its commanded acceleration $u_{current}$. To produce the same traveled distance for $V_{current}$, $u_{current}$ is selected equal to u_{new} which is calculated as

$$u_{new} = \frac{d_{preceding} - v_{current}\big(t_s(end) - t_s(1)\big)}{0.5\big(t_s^2(end) - t_s^2(1)\big)}, \tag{14}$$

  Using the new acceleration command, another important consideration is to ensure that the predicted position vectors of $V_{current}$ and $V_{preceding}$, calculated using (13), will not overlap (collide) during the interval of t_s. If that is the case, then the acceleration needs to be selected from the interval $\big[a_{\min} : \Delta a : u_{new}\big)$ where Δa is a suitable acceleration increment. Namely, $u_{current}$ is set equal to the first value smaller than u_{new} within that interval. If the new value produces no collisions then it is applied. Otherwise, the next value is selected and so on.
- If $d_{preceding} \geq d_{current}$, then the commanded acceleration $u_{current}$, calculated according to the platooning control laws from section 2.1, is maintained.

The steps of this approach are shown in Algorithm 1. Once the disbanding attack is detected for a single platoon, as explained in Section 2.2, the last vehicle of the disbanded platoon will inform the following lead intact vehicle, using the established inter-vehicle communication. The latter vehicle will calculate its acceleration command and modify it, if needed, using this mitigation approach. Furthermore, it will also inform the following vehicle to implement similar steps.

Practically, to implement the suggested approach requires that the following information should be available: commanded acceleration of the current vehicle

(measured locally) and the preceding one (transmitted via the already established communication), and the velocity of the current vehicle (measured locally) and that of the preceding one (estimated form the measurements of velocity and relative velocity). The process described above will be repeated at the next time instant using the newly obtained measurements. $V_{current}$ will reuse the adopted platooning control law once the inter-vehicle distance, with respect to $V_{preceding}$, begins to increase.

Finally, it should be noted that our approach requires a far less sophisticated communication model to connect any two neighboring vehicles, performs a decentralized mitigation, and produces nearly equivalent results to the MPC-based mitigation. Hence, it is not only cheaper to implement the heuristic approach compared to the MPC-based one, the former is also more resilient.

4.3 Results and discussion

Table 2 displays the average velocity error, E_v, collected under different scenarios for the optimal single platoon disbanding attack. Baseline, mit.1, and mit.2 refer to platoons using the control structure from Section 2.1, the heuristic mitigation, and MPC based mitigation, respectively. For all the cases given, the total number of platoons is equal to ten and the inter-vehicle separation, x_d, and actuator delay, τ, are varied, in order to examine various likely scenarios.

We can see (Table 2) that the baseline control does not perform well against the disbanding attack, since all cases involve accidents (except for $x_d = 5$ m and $\tau = 0.1$ s) and an increase in E_v. On the other hand, it is clear that our approach improves the values of E_v for all attack cases.

In addition, collisions are avoided in most attack cases except when τ equals to 0.5 s. Also, the heuristic approach reduces the number of colliding vehicles. For example, the attack case with $x_d = 4$ m resulted in accidents involving 58% and 29% of the total number of vehicles, which is 100, for the baseline and mit.1, respectively. Furthermore, for the attack case with $x_d = 5$ m and $\tau = 0.1$ s, 80% of the intact vehicles experienced stop-and-go behavior at least once because of the use of a collision-avoidance algorithm applying maximum deceleration. However, in our approach, and for all attack cases, all intact vehicles slowed down gradually and did not have to come to a complete stop.

Using mit.2 also helps with improving the values of E_v and avoiding collisions. By comparison, we can see that the values of E_v for both mit.1 and mit.2 are comparable. In fact, it is clear that our approach improves the results, in terms

Table 2. Results for optimal one-platoon disbanding attack

x_d [m]	τ [s]	E_v [%]			Crash		
		baseline	mit.1	mit.2	baseline	mit.1	mit.2
5	0.1	29.570	24.283	23.025	No	No	No
	0.3	41.268	25.556	25.182	Yes	No	No
	0.5	52.235	28.482	28.709	Yes	Yes	Yes
4	0.1	27.995	25.063	22.798	Yes	No	No
	0.3	40.115	26.864	24.823	Yes	No	No
	0.5	52.706	29.079	29.742	Yes	Yes	Yes

Table 3. Results for optimal two-platoon disbanding attack

x_d [m]	τ [s]	E_v [%]			Crash		
		baseline	mit.1	mit.2	baseline	mit.1	mit.2
5	0.1	38.347	27.056	26.221	Yes	No	No
	0.3	39.839	28.548	29.129	Yes	No	Yes
	0.5	45.004	35.724	38.690	Yes	Yes	Yes
4	0.1	37.069	30.731	29.811	Yes	No	No
	0.3	40.233	33.183	34.868	Yes	Yes	No
	0.5	45.823	38.349	38.914	Yes	Yes	Yes

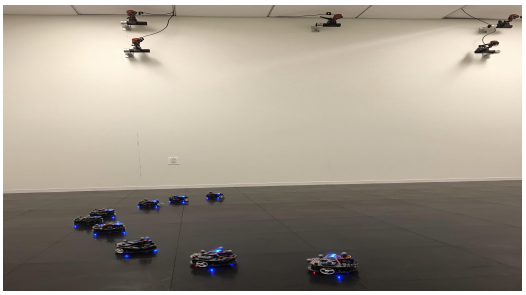


Fig. 4. Experimental environment with small robots and motion capture system

of lowering E_v and no collisions, in some attack cases. Overall, these numbers demonstrate that our heuristic approach produces nearly equivalent results to the optimal MPC approach.

Table 3 shows data for E_v collisions for different cases involving two platoons disbanding, where the total number of platoons is equal to ten. The optimal attack is found to occur by targeting the 10^{th} (lead) and 9^{th} platoons in the formation at times equal to 2s and 100s, respectively, within T_s. We can see that the baseline control produces collisions for all attacks cases. However, with either mit.1 or mit.2, the reduction in velocity is minimized and crashes are avoided completely in some cases. Also, the results for both mitigation approaches are nearly equivalent. Furthermore, by comparison with Table 2, and even with mitigation, the two-platoon disbanding attack results in more crashes, which indicates that it is a more severe attack compared to disbanding a single platoon.

5 Experimental Validation

Our proposed mitigation algorithm was evaluated on a testbed and compared with the baseline algorithm (i.e., a platoon control law with collision avoidance).

5.1 Hardware Setup

Our experimental setup consisted of small robots that represent vehicles in a stream of platoons and a motion capture system for tracking (Figure 4). We implemented the attack and the mitigation algorithm on three 3-vehicle platoons, denoted as per the convention shown in Figure 2. The 3^{rd} (leading) platoon was disbanded and the response of other two platoons was captured.

To each robot is affixed multiple IR markers for tracking by the Optitrack motion capture system. 24 IR cameras, and the Motive software, enable us to capture robot positions. Position data is streamed to a command computer where an interface application utilizing the Robot Operating System (ROS) [26] framework makes the gathered position data for each robot available to our controller application. This application processes the position data and sends appropriate control commands to each robot. The controller application implemented on ROS works in the following manner:

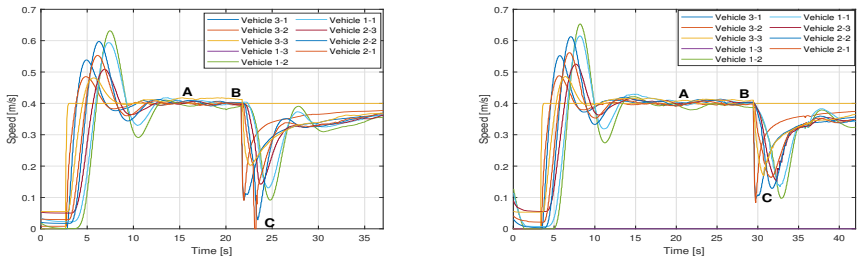
- The raw position data is processed using an Extended Kalman Filter to reduce camera sensor noise and estimate the measured position and velocity.
- The *Pure Pursuit Controller* uses the estimated positions and circular path coordinates from the experimental environment to calculate the angular velocity command for each vehicle.
- The estimated data of all vehicles is used to calculate the relative distance and velocity. This is then fed to the upper-level controller (Section 2.1) and provides desired acceleration values for the robots.
- The mitigation and baseline algorithm then modify the acceleration values from the upper-level controller in case a disbanding attack is detected.
- As the vehicles only act upon instantaneous velocity commands, these acceleration values along with current measured velocities are used to calculate the desired velocities for each vehicle. The desired linear velocities for the vehicles are effected using a PI controller which acts as the lower-level controller (Section 2.1).

Each robot consists of a 32-bit ARM-based mbedNXP LPC1768 microcontroller on the Pololu m3pi platform to which Digi Xbee receivers are interfaced. An Xbee transmitter is also connected to the command computer. These Xbee modules allow us to establish a wireless communication channel over which the angular and linear velocity commands, calculated for each robot using the controller application, are broadcast. The robots receive the broadcast messages and calculate the left and right wheel speeds from the received angular and linear velocities as per the differential drive model.

5.2 Experimental Results

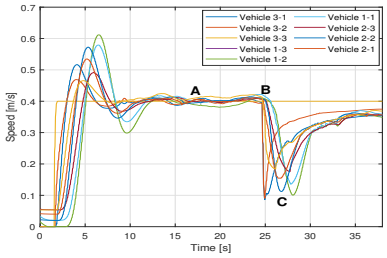
Figure 5 shows individual velocity profiles for the vehicles under consideration (three platoons with three robots in each). Figure 5a indicates the affect on velocities due to disbanding for the baseline control algorithm, given in Section 2.1, where we can see vehicles in the last platoon slow down suddenly (one of them stops) in response to the disbanding of the lead platoon. Figures 5b and 5c give the velocity profiles when the intact robots use the traveled distance mitigation approach, wherein it can be seen that the speed of vehicles in second and third platoon slow down gradually and then begin to accelerate. This mitigation approach was tested with $t_s = 0.5$s and 1s, respectively. The point labeled as A in Figures 5a, 5b, and 5c indicate that the platoons are in a steady state. Point B marks the time when the attack on the lead platoon is emulated, causing all of its vehicles to disband and suddenly decelerate. Deceleration patterns of the vehicles after point B for the baseline controller clearly indicates a sudden drop in velocities for the following platoons, causing some vehicles to come to a complete stop as indicated by point C.

While there are no collisions with the baseline control, sudden deceleration/ acceleration is observed. Such abrupt changes in velocities are not observed when our proposed heuristic mitigation is in place (Figures 5b and 5c, where point C shows that none of the vehicles need to come to a halt). With the mitigation approach, vehicles gradually decelerate and accelerate to recover and maintain



(a) Baseline

(b) Mitigation: $t_s = 0.5$s



(c) Mitigation: $t_s = 1.0$s

Fig. 5. Vehicles' velocities upon disbanding of platoon 3 for baseline control structure and proposed heuristic mitigation algorithm with $t_s = 0.5$s and 1s.

desired spacing and velocities, without collisions. Furthermore, the calculated E_v for the three experiments were 30.02%, 21.82% and 19.73% for Figures 5a, 5b and 5c, respectively. These numbers indicate that with increasing t_s, the change in velocity is smoother and more gradual, yet collisions do not occur. However, with $t_s = 1$ s, the vehicles come to closer proximity, compared the results with $t_s = 0.5$ s. For reference, we have also uploaded short videos of our experiments [1].

6 Conclusion

We presented and studied an attack which targets vehicular platoons and can cause severe deviations in speed, including stop-and-go traffic, and collisions. The attack exploits human-in-the-loop control, whereby a vehicle switches from automated control to human driving at the onset of an attack against the sensing system of a vehicle, causing the platoon to dissolve (or disband). Calculations of key attack factors, such as identifying the platoon to disband and time to disband them, in optimal disbanding scenarios were carried out. Additionally, we proposed mitigation algorithms that reduce sudden velocity changes and also decrease the number of accidents, hence ensuring resilient performance for platoons. Simulations and experimental results corroborate theory, which indicate decreased velocity deviations and thus improved traffic flow. Finally, the proposed heuristic approach was implemented on a hardware testbed, with a

motion capture system and mobile robots representing platoons, and it showed an improved performance, compared to using a baseline control algorithm.

References

1. Mitigation and baseline algorithm experiments. `http://m.youtube.com/channel/UCI-UGJKT7C5E_8bs391LCpA`
2. Truck platooning vision 2025 (2016), `www.eutruckplatooning.com`
3. Amoozadeh, M., Deng, H., Chuah, C.N., Zhang, H.M., Ghosal, D.: Platoon management with cooperative adaptive cruise control enabled by vanet. Vehicular communications **2**(2), 110–123 (2015)
4. Axelsson, J.: Safety in vehicle platooning: A systematic literature review. IEEE Transactions on Intelligent Transportation Systems **18**(5), 1033–1045 (2017)
5. Bemporad, A., Morari, M.: Robust model predictive control: A survey. In: Garulli, A., Tesi, A. (eds.) Robustness in identification and control. Spring, London (1999)
6. Bergenhem, C., Shladover, S., Coelingh, E., Englund, C., Tsugawa, S.: Overview of platooning systems. In: Proceedings of the 19th ITS World Congress, 22-26, Austria (2012)
7. Blanco, M., Atwood, J., M. Vasquez, H., Trimble, T., L. Fitchett, V., Radlbeck, J., Fitch, G., M. Russell, S., A. Green, C., Cullinane, B., Morgan, J.: Human factors evaluation of level 2 and level 3 automated driving concepts (08 2015)
8. Borrelli, F.: Constrained optimal control of linear and hybrid systems, vol. 290. Springer (2003)
9. Chauhan, R., Gerdes, R.M., Heaslip, K.: Attack against an fmcw radar. In: Proceedings of Embedded Security in Cars Conference (2014)
10. Chou, C., Li, C., Chien, W., Lan, K.: A feasibility study on vehicle-to-infrastructure communication: Wifi vs. wimax. In: 2009 Tenth International Conference on Mobile Data Management: Systems, Services and Middleware. pp. 397–398 (2009)
11. Coelingh, E., Solyom, S.: All aboard the robotic road train. IEEE Spectrum **49**, 34–49 (2012)
12. Dadras, S., Gerdes, R.M., Sharma, R.: Vehicular platooning in an adversarial environment. In: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. pp. 167–178. ASIA CCS '15, ACM, USA (2015)
13. DeBruhl, B., Weerakkody, S., Sinopoli, B., Tague, P.: Is your commute driving you crazy?: a study of misbehavior in vehicular platoons. In: WISEC (2015)
14. Dunn, D.D., Mitchell, S.A., Sajjad, I., Gerdes, R.M., Sharma, R., Li, M.: Regular: Attacker-induced traffic flow instability in a stream of semi-automated vehicles. In: 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). pp. 499–510 (2017)
15. Eriksson, A., Stanton, N.A.: Takeover time in highly automated vehicles: Noncritical transitions to and from manual control. Human Factors **59**(4), 689–705 (2017)
16. Gerdes, R.M., Winstead, C., Heaslip, K.: Cps: an efficiency-motivated attack against autonomous vehicular transportation. In: Proceedings of the 29th Annual Computer Security Applications Conference. pp. 99–108. ACM (2013)
17. Gold, C., Dambck, D., Lorenz, L., Bengler, K.: take over! how long does it take to get the driver back into the loop? Proceedings of the Human Factors and Ergonomics Society Annual Meeting **57**(1), 1938–1942 (2013)
18. J. Ploeg, B. Scheepers, E.N.N.v.d.W., Nijmeijer, H.: Design and experimental evaluation of cooperative adaptive cruise control. In: International IEEE Conference on Intelligent Transportation Systems. pp. 260–265 (2011)

19. Jagielski, M., Jones, N., Lin, C.W., Nita-Rotaru, C., Shiraishi, S.: Threat detection for collaborative adaptive cruise control in connected cars. In: Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks. pp. 184–189. WiSec '18, ACM, USA (2018)
20. Kesting, A., Treiber, M., Helbing, D.: Enhanced intelligent driver model to access the impact of driving strategies on traffic capacity. Philosophical Trans. of the Royal Society of London A: Mathematical, Physical and Engineering Sciences **368**(1928), 4585–4605 (2010)
21. Liang, K.Y., Mårtensson, J., Johansson, K.H.: Fuel-saving potentials of platooning evaluated through sparse heavy-duty vehicle position data. 2014 IEEE Intelligent Vehicles Symposium Proceedings pp. 1061–1068 (2014)
22. Merat, N., Jamson, A.: How do drivers behave in a highly automated car? pp. 514–521 (10 2017). https://doi.org/10.17077/drivingassessment.1365
23. Merat, N., Jamson, A.H., Lai, F.C., Daly, M., Carsten, O.M.: Transition to manual: Driver behaviour when resuming control from a highly automated vehicle. Transportation Research Part F: Traffic Psychology and Behaviour **27**, 274 – 282 (2014)
24. Oncu, S., Ploeg, J., van de Wouw, N., Nijmeijer, H.: Cooperative adaptive cruise control: Network-aware analysis of string stability. IEEE Trans. on Intelligent Transportation Systems **15**(4), 1527–1537 (2014)
25. Petit, J., Stottelaar, B., Feiri, M., Kargl, F.: Remote attacks on automated vehicles sensors: Experiments on camera and lidar. Black Hat Europe **11** (2015)
26. Quigley, M., Conley, K., Gerkey, B., Faust, J., Foote, T., Leibs, J., Wheeler, R., Ng, A.Y.: Ros: an open-source robot operating system. In: ICRA workshop on open source software. vol. 3, p. 5. Kobe, Japan (2009)
27. Rajamani, R.: Vehicle Dynamics and Control. Mechanical Engineering Series, Springer (2011)
28. Rawlings, J.B.: Tutorial overview of model predictive control. IEEE Control Systems Magazine **20**(3), 38–52 (2000)
29. Ren, W., Green, D.: Continuous platooning: a new evolutionary operating concept for automated highway systems. In: Proceedings of American Control Conference (ACC). vol. 1, pp. 21–25 (1994)
30. Robinson, T., Chan, E., Coelingh, E.: Operating platoons on public motorways: An introduction to the sartre platooning programme. In: 17th world congress on intelligent transport systems. vol. 1, p. 12 (2010)
31. van der Heijden, R., Lukaseder, T., Kargl, F.: Analyzing attacks on cooperative adaptive cruise control (cacc). In: 2017 IEEE Vehicular Networking Conference (VNC). pp. 45–52 (2017)
32. Vlakveld, W., Verkeersveiligheid, S.W.O., Rijkswaterstaat. Water, V.e.L.: Transition of Control in Highly Automated Vehicles: A Literature Review. SWOV Institute for Road Safety Research (2015)
33. Yan, C., Xu, W., Liu, J.: Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. DEF CON **24** (2016)
34. Yanakiev, D., Kanellakopoulos, I.: A simplified framework for string stability analysis in ahs. In: Proceedings of the 13th IFAC World Congress. pp. 177–182 (1996)
35. Yeh, E., Choi, J., Prelcic, N., Bhat, C., Heath Jr, R.: Security in automotive radar and vehicular networks. Microwave Journal **60**, 148–164 (2017)
36. Zheng, R., Nakano, K., Yamabe, S., Aki, M., Nakamura, H., Suda, Y.: Study on emergency-avoidance braking for the automatic platooning of trucks. IEEE Trans. on Intelligent Transportation Systems **15**(4), 1748–1757 (2014)