2018 Annual American Control Conference (ACC)
June 27–29, 2018. Wisconsin Center, Milwaukee, USA

Reachable Set Analysis of Vehicular Platooning in Adversarial Environment

Soodeh Dadras[1], Sara Dadras[1] and Chris Winstead[1]

Abstract— **In this paper, we propose a method based on reachable set theory to investigate adversarial behavior in automated vehicle platoons. Vehicular platoons have been developed to increase highway throughput and safety, and to enhance driving comfort. The resulting deployment of cyber-physical technology in critical infrastructure is increasingly attractive to both hackers and security researchers. To ensure safety and privacy of vehicle occupants, it is essential to identify the vulnerabilities of platoon systems. In this paper, we study the attacker's capabilities under input constraints during two types of attack: motion modification and integral attacks. Using ellipsoidal techniques, we investigate the extent of an attacker's ability to manipulate the control variables and states of a platoon resulting in oscillatory motion or collision. The outcomes of our analysis are demonstrated by an example.**

I. INTRODUCTION

Platooning, also known as Cooperative Adaptive Cruise Control (CACC), is characterized as a group of vehicles with coordinated movement. Platooning has been investigated for around 4 decades [1]. The main objective of platooning is to reduce the inter-vehicle distance significantly compared to what is considered advisable during manual driving. Among the potential benefits are a better use of the road infrastructure by allowing more vehicles to use a given stretch of road, improved energy efficiency by reducing aerodynamic drag, increased highway safety due to reduction of human mistakes, and reduced traffic congestion [2]. Huge body of research involves longitudinal and lateral control of vehicle platoon [3]–[8]. The main concept in platoon control is *string stability*. String stability deals with how errors are propagated through the vehicle string due to disturbances or the reference trajectory of the formation lead. A string-stable control form means that spacing errors between adjacent vehicles do not grow or amplify along the vehicle string [9], [10].

While many features of platooning are active areas of research, e.g. transportation impacts, environmental, mechanical and control concerns [1], [11]–[13], comparatively little work has examined platooning in an adversarial environment and among those, most papers challenge platoon security from communication aspect [14]. A few works that performed security analysis on control in platooning can be grouped into categories of attack design [15]–[19] and mitigation strategies [20]. It has been verified by recent studies that attacks on platooning components may cause physical damages and threaten their normal functions. Research works are mostly seeking the drawbacks in controls and trying to manipulate the vulnerabilities like modification of control law such that attacker can create catastrophic impacts on platoon. This type of impacts included, but are not limited to, collision in high relative velocity to maximize the damage or oscillation to cause passenger discomfort and increase fuel consumption [16], [18], [19]. A scenario wherein a group of malicious vehicles on a highway perform a cooperative attack for creating undesirable wave effects among other vehicles are investigated in [21], [22] . The mathematical analysis to choose the undesirable wave is presented. This investigation helps to understand the effect of drivers behavior on traffic formation. In [16] attacker changes its gains such that system becomes unstable and authors, at the end, briefly introduce the controllability of attacker over platoon. To investigate this idea thoroughly, we study reachability of the platoon in presence of attacker, which can give clear picture of attacker capability in affecting position and velocity of other vehicles in platoon, with its own motion involving acceleration or deceleration. However, the research works mentioned above focus on only designing attacks and disrupting the platoon. The important challenge remaining is to provide guarantees for successful attack. Two intriguing questions in this context are: *(a) Will the attacker be able to carry out the attack successfully? (b) Will the vehicles collide under control constraints?* This problem implies that the attack should be designed with more comprehensive analysis.

This paper is devoted to analysis of reachability properties of vehicular platooning under attack. Reachability analysis determines the set of states that system can possibly visit within finite or infinite time, when started from bounded set of possible input and parameter values. Exact reachable set can be computed for special cases with few states. Except for the simplest of examples, analytic verification of reachable set for continuous and hybrid systems is rarely possible. With the goal of broadening the applicability and automating the process, numerical methods for verifying or validating such properties have been the subject of much study. Several papers in the literature deal with approaches for reachability set computation. Reachable sets and the optimal time to reach a target for a controlled nonlinear system is characterized using Hamilton Jacobi equation with state constraints in [23]. An algorithm which can numerically compute the backward reachable set for a two player, nonlinear differential game with a general target set is proposed in [24]. This algorithm is based on a formulation of reachability in terms of the viscosity solution of a time-dependent Hamilton-Jacobi-Bellman partial differential equation. Hamilton-Jacobi methods to

*This material is based in part upon work supported by the National Science Foundation under Grant No. 1410000.

[1] Soodeh Dadras, Sara Dadras and Chris Winstead are with Electrical and Computer Engineering Department at Utah State University, Logan, UT 84322, USA soodeh.dadras@aggiemail.usu.edu

978-1-5386-5428-6/$31.00 ©2018 AACC

reach-avoid problems with time-varying dynamics, targets, and constraint have applications in game theory and optimal control problems. Hamilton-Jacobi methods for such applications including pursuit-evasion, differential games, and safety certificates for dynamical systems are extended in [25]. Any reachability analysis performed so far on vehicle platoon or any vehicular formation, was for the purpose of collision avoidance [26]–[28] or fuel consumption minimization [29].

Approximation of reachable sets is one major category of numerical methods. Reachable set can be over or under-approximated. Obviously, over-approximated reachable states can contain states which are not practically achievable and minimizing over-approximation results in high computational cost. Hence, under-approximation techniques are more reliable approach.

Currently, the analysis of the vehicle platoon systems cannot tractably provide the exact reachable set if number of vehicles is large. In this paper, under approximated reach set for platoon of vehicles under attack is studied. For the longitudinal control, the Proportional Derivative (PD) control for Bidirectional information flow [30] is used to produce a sequence that minimizes spacing, relative velocity and the cost of traveling from an origin to any destination. The extent of performance disruption of the platoon facing attack is studied using ellipsoidal method and attacker's goal satisfaction are analyzed using homogeneous model for all vehicles. First, reachable states for a single motion change attack, is studied. Then, in the event of integral attack (motion and gain modification), potential impacts are investigated. We demonstrate the platoon states whilst facing two representative attack scenarios and discuss attacker's performance capability in each scenario.

To the best of the authors' knowledge, reach set computation for the attacker has not been investigated in literature. We discuss what the attacker is capable of, based on his position in the platoon and present detailed examination of reachable set for two attack scenarios under input constraints. This study gives us a profound knowledge of what the attacker is really capable of accomplishing, under physical constraints in practical cases.

This paper is organized as follows: In Section (II), we introduce fundamentals of reachable sets; system and threat models are presented in Section (III). The reachable states of platoon during motion modification and integral attacks are demonstrated and discussed in Section (IV). Section (V) concludes the paper.

II. Preliminaries

Reachability analysis computes all possible states a system can attain, and in this sense provides knowledge about the system with a completeness, or coverage, that a finite number of simulation runs can not deliver, due to its inherent complexity.

Reachability analysis is concerned with the computation of the reachable set in a way that can effectively meet some types of requests. These requests include [31]: (a) determination of non-empty intersection of reach set and the target set; (b) finding a feasible initial condition; (c) control that steers the system from this initial condition to the given reachable state in given time.

Several methods exist in literature which propose algorithms to calculate the reachable set of the system like methods based on ellipsoidal representations [32], techniques using support functions [33], and applying Hamilton Jacobi Isac (HJI) equations to differential equations [24]. As the number of the states increases, it becomes harder to calculate the exact reachable set of the system by admissible inputs. Hence, some of the existing methods suggest some approximation algorithms to find the reachable set.

Ellipsoidal method is proposed for calculating reachable set for continuous time linear system under input constraints in [34] and [35]. In [34], authors proposed that they can estimate the reachable tube for the general linear time invariant system described in (1),

$$\dot{x} = Ax + Bu \quad t_0 \leq t \leq T \tag{1}$$

where $x \in R^n$, $u \in R^m$, $A \in R^{n\times n}$ and $B \in R^{n\times m}$ are states, inputs and matrices describing dynamic of the system, respectively.

Definition 2.1: The reachable set $R[x,T] = R(T,t_0,X_0)$ of the system (1) at time T from a set of initial states X_0 and time t_0 is the set of all points x for which there exists a trajectory $x(s,t_0,X_0)$, $x_0 \in X_0$ that transfers the system from (t_0,x_0) to (T,x), $x = x(T)$, while satisfying the associated constraints [36].
Similarly, the reachable tube is the set of all reachable sets over a time interval.

Definition 2.2: The reachable tube is all values (1) can meet during $[t_0,T]$ and is mathematically defined as $Tu(x,T) = \bigcup_{t\in[t_0,T]} R(t,t_0,X_0)$ [36].

Assuming some constraints on the input, our admissible set of inputs is $u(t) \in P(t)$, where $P(t)$ is non-degenerate ellipsoid continuous in t,

$$\begin{aligned} P(t) &= \xi(q(t),Q(t)) \\ &= \{u(t) : (u-q(t)), Q^{-1}(t)(u-q(t)) \leq 1\} \end{aligned} \tag{2}$$

where $q(t) \in R^m$ is the center and positive definite matrix $Q(t) \in R^{m\times m}$ is matrix of ellipsoid.

We can calculate response of the system using

$$x(t) = \exp(A(t-t_0))x_0 + \int_{t_0}^{T} (\exp(A(t-\tau))Bu(\tau)d\tau). \tag{3}$$

Extending (3) to ellipsoidal calculation for reachable set results in

$$\begin{aligned} x(t) \in R[T,t_0,X_0] = \exp(A(t-t_0))\xi(x_0,X_0) + \\ \int_{t_0}^{T} (\exp(A(t-\tau))B\xi(q(\tau),Q(\tau))d\tau). \end{aligned} \tag{4}$$

Above, we briefly point out how to calculate the reachable set using Ellipsoidal toolbox.

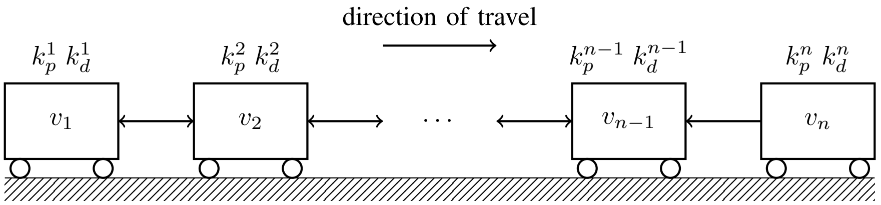

Fig. 1. An n-vehicle platoon employing a bi-directional control law. Arrows represent the flow of information.

III. Problem statement

Our analysis focuses on exploiting longitudinal control laws and input of the vehicles in platoon, which are intended to maintain desired separation and velocity as they follow straight line. Assuming all vehicles are traveling in one dimension, attacker gets the chance to influence other vehicles' motion via manipulating longitudinal control algorithm.

A. Platoon Model

We use the bi-directional (predecessor-follower) proportional-derivative (PD) controller to demonstrate the impact of a malicious actor on platooning operations. This control law is capable of maintaining a constant separation, d, between vehicles, based solely on local sensing. This is important because it allows us to show that an attacker can affect the platoon solely through malicious movement and need not rely on interfering with inter-vehicle communication. Formally, the dynamics of a platoon with n vehicles employing this control law for the leader are described by the following system of equations,

$$\begin{aligned}
\dot{x}_1 &= v_1,\\
\dot{v}_1 &= k_p^1(x_2 - x_1 - d) + k_d^1(v_2 - v_1),\\
\dot{x}_2 &= v_2,\\
\dot{v}_2 &= k_p^2(x_1 - x_2 + d) + k_p^2(x_3 - x_2 - d),\\
&\quad + k_d^2(v_1 - v_2) + k_d^2(v_3 - v_2),\\
&\vdots\\
\dot{x}_{n-1} &= v_{n-1},\\
\dot{v}_{n-1} &= k_p^{n-1}(x_{n-2} - x_{n-1} + d) + k_p^{n-1}(x_n - x_{n-1} - d),\\
&\quad + k_d^{n-1}(v_{n-2} - v_{n-1}) + k_d^{n-1}(v_n - v_{n-1}),\\
\dot{x}_n &= v_n,\\
\dot{v}_n &= k_p^n x_{n-1} - k_p^n x_n + k_p^n d + k_d^n v_{n-1} - k_d^n v_n + u_l
\end{aligned} \tag{5}$$

where x_i and v_i represent the position and velocity of the i_{th} vehicle, respectively ($\dot{a}$ denotes the first derivative with respect to time of the variable a), and k_p^i and k_d^i represent their proportional and derivative gains, respectively. For normal platooning operations k_p^i and k_d^i are the same for each vehicles (we thus dispense with the superscript unless referring to the gains for a vehicle in a particular position). k_p is traditionally fixed at 1, while k_d varies according to the size of the platoon [16]. Here, u_l represents the control input for the leader (n_{th} vehicle). In the steady-state u_l is generally taken to be equal to zero; however, we note that $k_p^n \neq 0$ and $k_d^n \neq 0$ implies that the followers would be able to influence the leader's movements, unless u_l is set to cancel out the follower movements, which would effectively set $k_p^n = k_d^n = 0$. In any case, from the security perspective it seems inadvisable for followers to be able to influence the leader.

B. Threat Models

We study the behavior of platoon in presence of malicious vehicle and the scope of deviation from its normal performance, traveling at a constant speed with constant spacing. We study two attack scenarios: In the first attack, attacker attempts to take control of all the states and brings them to desired and arbitrary states solely through its motion. This raises a question tabout how probable is it that the attacker will successfully accomplish his goal.. In this attack, attacker choose its gains, as other vehicles in the platoon but it uses its own acceleration/deceleration to influence other vehicles states. The attacker's vehicle is considered to have exactly the same capabilities as the other vehicles in the platoon.

In the second attack scenario, attacker implements an integral attack where attacker takes advantage of motion modification while it modifies its control algorithm. We analyze the attacker capability during integral attack. The attack model would be similar to (6) and the corresponding row to the attacker in A matrix would be modified like [16].

In order to, demonstrate the extent of attacker's capability of controlling platooning operations with being assigned nominal control of the platoon, we assume that the attacker does not act as the leader of the platoon.

The equivalent state-space representation of the linear time-invariant (LTI) system defined by (5) in the presence of an attacker is

$$\begin{aligned}
\dot{\mathbf{X}} &= A\mathbf{X} + B\mathbf{U}\\
\mathbf{Y} &= C\mathbf{X}
\end{aligned} \tag{6}$$

where $X = [x_1,\ v_1,\ x_2,\ v_2,\ \cdots,\ x_n,\ v_n]^\top \in \mathbb{R}^{2n}$ are the states of all the vehicles in the platoon and Y is the output, which in this case is similar to states, $A \in \mathbb{R}^{2n\times 2n}$, $B \in \mathbb{R}^{2n\times 2}$, $C \in \mathbb{R}^{2n\times 2n}$, and $\mathbf{U} = [u_l\, u_a]^\intercal$. C is the identity matrix (because we assume that all the vehicle states are measurable), B has non-zero entries corresponding to the leader and the attacker control, u_l and u_a, respectively, where u_a is the attacker's input in order to achieve the desired states for both attacks.

$$\begin{aligned} z_i &= x_i - x_{i+1} + d \\ y_i &= \dot{x}_i - \dot{x}_{i+1} = v_i - v_{i+1} \end{aligned} \tag{7}$$

The states to be controlled by the attacker are relative position and relative velocity. So, we transform our system of equation, (5) to (8), where attacker is in i_{th} position in the platoon. In case there are n vehicles in the platoon, number of states in absolute coordinate (5) is $2n$ for positions and velocities. On the other hand, using error coordinate (7) and (8), we have $2n-2$ states, z_i and y_i, which are spacing and relative velocity, respectively. Leader of the platoon would be counted as the n_{th} vehicle in platoon, as shown in Fig. 1, and we assume that all vehicles in platoon follow the normal control law in motion modification attack descried in (8).

$$\begin{aligned}
\dot{z}_1 &= y_1 \\
\dot{y}_1 &= -2k_p z_1 + k_p z_2 - 2k_d y_1 + k_d y_2 \\
\dot{z}_2 &= y_2 \\
\dot{y}_2 &= k_p z_1 - 2k_p z_2 + k_p z_3 \\
&\quad + k_d y_1 - 2k_d y_2 + k_d y_3 \\
&\vdots \\
\dot{z}_{i-1} &= y_{i-1} \\
\dot{y}_{i-1} &= k_p z_{i-2} - 2k_p z_{i-1} + k_p z_i \\
&\quad + k_d y_{i-2} - 2k_d y_{i-1} + k_d y_i - u_a \\
\dot{z}_i &= y_i \\
\dot{i}_2 &= k_p z_{i-1} - 2k_p z_i + k_p z_{i+1} \\
&\quad + k_d y_{i-1} - 2k_d y_i + k_d y_{i+1} + u_a \\
\dot{z}_{i+1} &= y_{i+1} \\
\dot{y}_{i+1} &= k_p z_i - 2k_p z_{i+1} + k_p z_{i+2} \\
&\quad + k_d y_i - 2k_d y_{i+1} + k_d y_{i+2} \\
&\vdots \\
\dot{z}_{n-2} &= y_{n-2} \\
\dot{y}_{n-2} &= k_p z_{n-3} - 2k_p z_{n-2} + k_p z_{n-1} \\
&\quad + k_d y_{n-3} - 2k_d y_{n-2} + k_d y_{n-1} \\
\dot{z}_{n-1} &= y_{n-1} \\
\dot{y}_{n-1} &= k_p z_{n-2} - k_p z_{n-1} + k_d y_{n-2} - k_d y_{n-1} - u_l
\end{aligned} \tag{8}$$

Then, A and B matrices using error coordinate can be formed as (9) and (10). The attacker in the first attack scenario only implements motion modification where the B matrix is modified. Single attacker only tries to control platoon by its own motion in which we can categorize B matrix as a single-column with entries 1 at $2i_{th}$ and -1 at $2i-1_{th}$ rows, where i is the place of the attacker in platoon. If we consider the second vehicle as the attacker, B matrix can be written as:

$$B = \begin{bmatrix} 0 \\ -1 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix} \tag{9}$$

In the integral attack, attacker combines the motion modification in the former attack with its gains modification and applies the changes to its corresponding row of A matrix.

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ -2k_p & -2k_d & k_p & k_d & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ k_p & k_d & -2k_p & -2k_d & k_p & k_d & 0 & \cdots & 0 \\ & & & \ddots & & & & & \\ 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & \cdots & 0 & 0 & 0 & k_p & k_d & -k_p & -k_d \end{bmatrix} \tag{10}$$

The changes to A matrix is described as follows: Allow $A(i,j)$ to represent access to the element at the i_{th} row and j_{th} column of A. When an attacker is present at the first position,

$$\begin{aligned} A(2,1) &= -k_p - \tilde{k_p} \\ A(2,2) &= -k_d - \tilde{k_d} \end{aligned} \tag{11}$$

An attacker in the i_{th} position, $1 < i < n-1$, changes the following elements of (10)

$$\begin{aligned}
A(2(i-1), 2(i-1)-1) &= k_p - \tilde{k_p}, \\
A(2(i-1), 2i-1) &= \tilde{k_p}, \\
A(2i, 2(i-1)-1) &= \tilde{k_p}, \\
A(2i, 2i-1) &= -k_d - \tilde{k_p} \\
A(2(i-1), 2(i-1)) &= k_d - \tilde{k_d}, \\
A(2(i-1), 2i) &= \tilde{k_d}, \\
A(2i, 2(i-1)) &= \tilde{k_d}, \\
A(2i, 2i) &= -k_d - \tilde{k_d}
\end{aligned} \tag{12}$$

When the attacker's position is $i = n-1$,

$$\begin{aligned} A(2(i-1), 2(i-1)-1) &= k_p - \tilde{k_p} \\ A(2(i-1), 2(i-1)) &= k_d - \tilde{k_d} \end{aligned} \tag{13}$$

Where derivative and proportional gains of the attacker shown using $\tilde{k_d}$ and $\tilde{k_p}$.

IV. Reachability Analysis and Simulation Results

In this section, we analyze the attacker's capability to disrupt the stable navigation of the platoon and measure the efficiency of the attack through reachable set. Efficiency of the attack would be measured through attacker's power to cause collisions between vehicles or cause the stop-then-go motion, which causes discomfort to passengers and increase in fuel consumption. We consider a linear model (6) for the platoon where attacker modifies input set while it follows the platoon control law using stable gains or it compromises the platoon via changing entries in A and u_a. In spite of system controllability analysis, which indicates platoon would be able to reach any arbitrary states proposed in [16] for the vehicle platoon, it can be clearly evidenced that attack is not feasible in stable case. This infeasibility stems from the small controllability grammian matrix determinant, which results in a huge control effort. Furthermore, when attacker changes its gains to unstable or marginally stable ones, it can actuate platoon to more diverse desired states. To clarify the difference of the two scenarios described in (6) - (12), the reachable sets of the system in both cases are computed and demonstrated for a small size platoon.

A. Reachability Analysis of the Platoon During Motion Modification Attack

We seek an achievable set of states for vehicles in platoon, such that attacker can steer states of vehicles towards them through its own constrained motion. More specifically, given that platoon already reached its desired constant spacing and velocity before the attack starts, we look for the most severe impact that the attacker can cause when its acceleration and deceleration are bounded the $u_a \in [u_{a_{min}}, u_{a_{max}}]$. This analysis is for the purpose of verifying attacker's capability to compromise the system. As explained, let the initial states and input sets of attacker be the ellipsoids. Initial set $\xi(x_0, X_0)$ for the (7), $x_0 = 0$ and X_0 is a very small deviation around 0 and admissible input set for the single attacker $\xi(q(\tau), Q(\tau))$ is a line stretched between $[u_{a_{min}}, u_{a_{max}}]$.

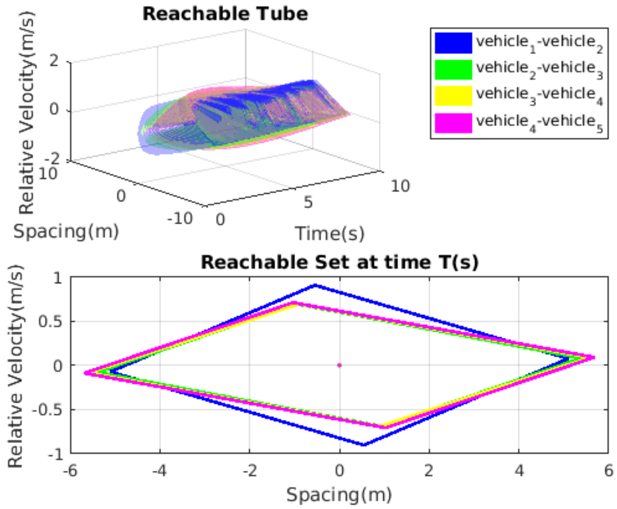

Fig. 2. Platoon reachable set and tube for T(s) duration of motion modification attack, when attacker is in the 1_{st} place.

B. Reachability Analysis of the Platoon During Integral Attack

During integral attack, attacker adds the control law modification attack on top of its erratic acceleration and deceleration to make more impact. The rationale is, changing gain for the attacker causes the platoon system to lose its symmetric structure, and even become more controllable from attacker perspective. In some cases, such control offers the attacker a broader range of impact. Therefore, attacker carries out motion modification attack with same setting described in previous attack while it modifies the A matrix as represented in (11) - (12).

C. Simulation Results

The reachable sets for motion modification and integral attack scenarios are demonstrated for the 5-vehicle platoon model. We computed the reachable sets using Ellipsoid toolbox.

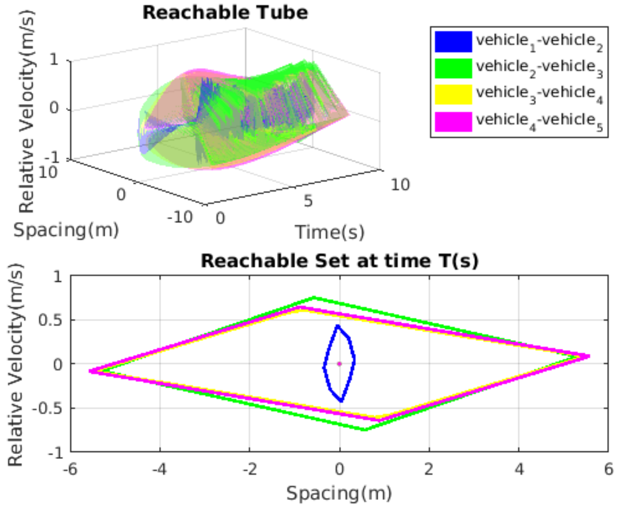

Fig. 3. Platoon reachable set and tube for T(s) duration of motion modification attack, when attacker is in the 2_{nd} place.

First, we show the reach set for the motion modification attack. Attack happens when platoon already reached steady state utilizing stable gains $k_p = 1$ and $k_d = 3.3$. 5-Vehicle platoon model involves 8 states which makes it hard to present the reachable sets graphically. Therefore, we use projection for the purpose of demonstration. In each case we provide the reach tube and reach set for time $T = 10(s)$, where input limits for the attacker is considered to be $[-5, 5]$. Reachable sets and tubes of the platoon for different positions of the attacker using motion modification attack are presented in Figs. 2, 3, ,4 and 5. Reachable relative velocity values are shown versus spacing values in each figure.

The reach set demonstration gives us clear understanding of the extent that attacker, in each position is able to deviate platoon from its normal vehicle following motion and the severity of attack in case of accidents. Our analysis to

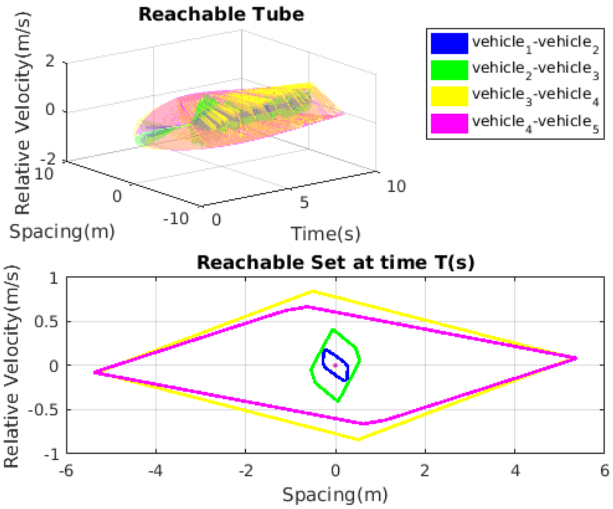

Fig. 4. Platoon reachable set and tube for T(s) duration of motion modification attack, when attacker is in the 3_{rd} place.

determine whether attacker is able to cause any collision between vehicles is based on (7). Collision happens when following vehicle hits or passes predecessor while moving in the same lane. Necessary and sufficient condition for the collision occurrence is presented as (14) ,

$$z_i \geq d. \tag{14}$$

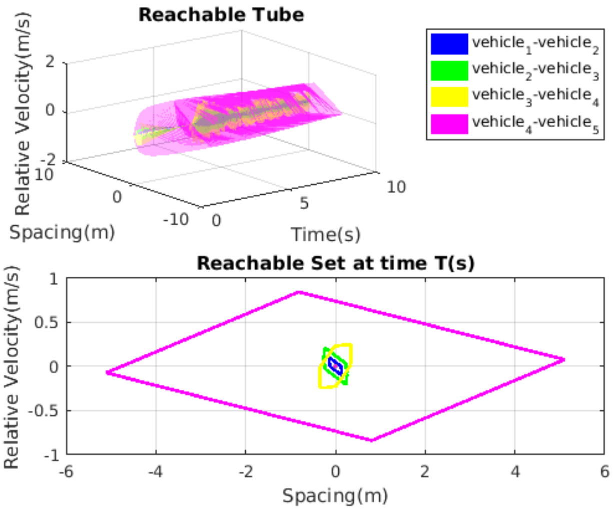

Fig. 5. Platoon reachable set and tube for T(s) duration of motion modification attack, when attacker is in the 4_{th} place.

Comparing desired spacing with the reachable set for the spacing, we would be able to recognize the instances of collision.

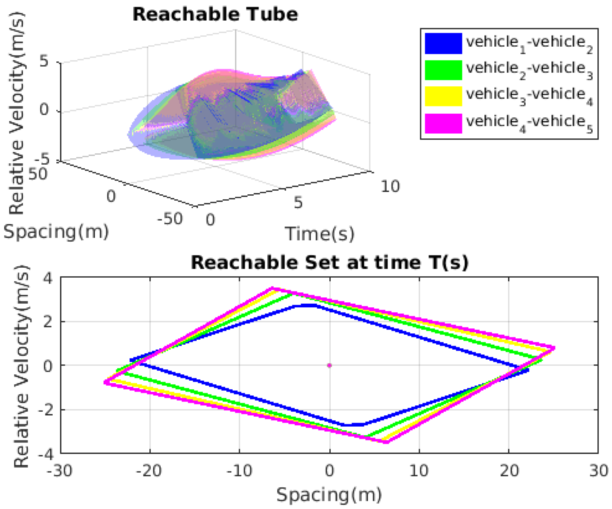

Fig. 6. Platoon reachable set and tube for T(s) duration of integral attack, when attacker is in the 1_{st} place.

For clarification, we assume that $d = 4m$, comparing (14) with Figs. 2 - 5, attacker in all positions is able to cause collisions between vehicles in front, but not the following ones. Observing the relative velocity values for all cases, we note that the collision happens when $v_i = v_{i+1} \pm 0.2$, which barely cause any damage to the vehicles. Higher relative velocity during collisions results in more severe damages. Reachable tubes present a constant pattern after $7(s)$ and reachable set for longer attack duration than 7(s) remain the same.

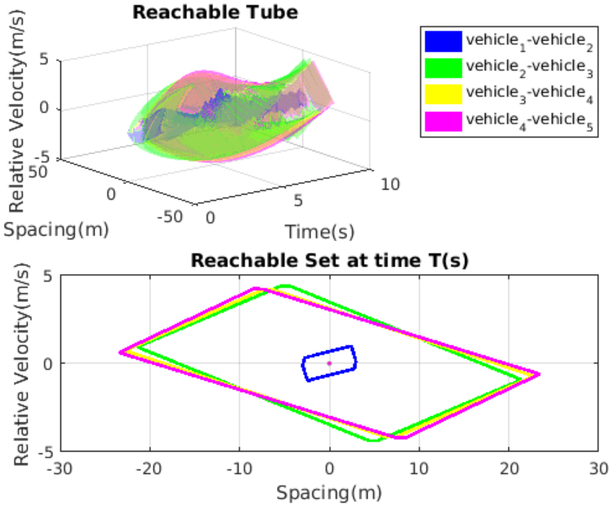

Fig. 7. Platoon reachable set and tube for T(s) duration of integral attack, when attacker is in the 2_{nd} place.

, Attacker randomly selects stable gains $\tilde{k_p} = 0.4$ and $\tilde{k_d} = -0.1$, such that all system eigenvalues remain in left half plane. Attacker uses the same range of input $[-5, 5]$ as motion modification attack to carry out integral attack. Corresponding reach set and tube for attacker in first position

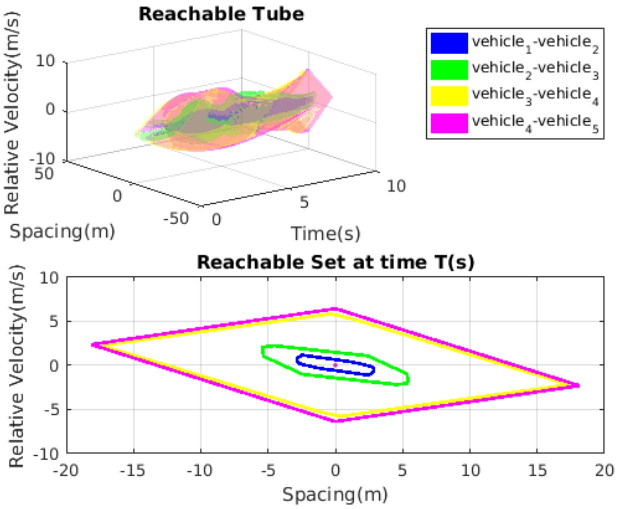

Fig. 8. Platoon reachable set and tube for T(s) duration of integral attack, when attacker is in the 3_{rd} place.

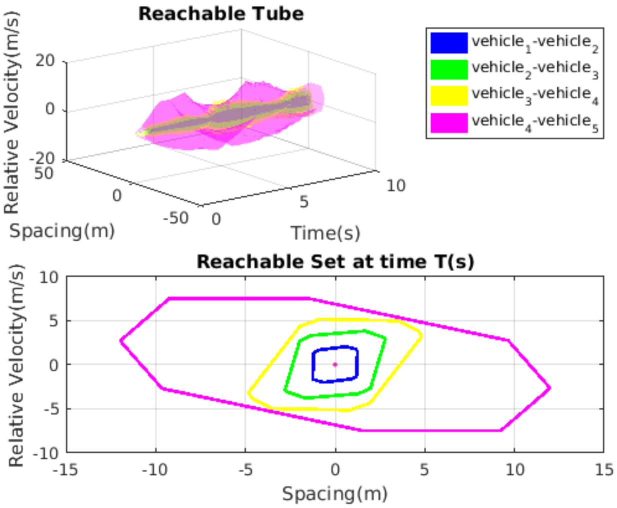

Fig. 9. Platoon reachable set and tube for T(s) duration of integral attack, when attacker is in the 4_{th} place.

are presented in Fig. 6. Comparing the results for the same position of the attacker in two attack scenarios, Fig. 2 and Fig. 6, the attacker has broader range of impact in latter case, where attacker can cause collision in speed of $v_i = v_{i+1} \pm 3$. Attacker reach set grows as position of the attacker moves toward the leader of platoon as shown in Figs. 7 - 9, where attacker collide into leader in speed of $v_i = v_{i+1} \pm 5$. Reachable tube in Fig. 9 represents oscillatory movement which causes passenger discomfort and increases fuel consumption.

D. Discussion and Future work

Reachability analysis is proven useful to learn destructive attacks against vehicular platooning. Through our investigation, we came across several points regarding reach set, which we briefly point out as follows: In attacks involving motion modification, attacker states has the largest reachable set among other members and it grows larger as position of the attacker moves towards leader in integral attack. While moving away from attacker the impact decreases on victims in both direction, and decreasing rate in direction pointing to the first vehicle is greater than the rate towards the leader. Duration of integral attack affects the reach set and in case of utilizing unstable gains, platoon reach set is very large and grows exponentially with time. We are interested to explore the reach set of platoon, when multiple attackers implement any or both attack scenarios on large size platoon. Also, we will propose a control algorithm which drive the system to its reachable states for given time and initial values.

V. Conclusion

In this paper, we have investigated reachability of platoon to determine feasible attacks with destructive impact. Our approach provides new insight to security of control in cyber-physical systems, specifically platooning. Our method proves that the attacker has a very limited capability to disrupt platoon, only utilizing acceleration and deceleration when all vehicles in platoon follow normal control law. Therefore, attacker's attempt would not result in severe damage and present control law has proven to be robust to such attacks. On the other hand, when the attacker combines, the motion modification and control law alteration, it can be shown that this type of attack is more disruptive and can cause collisions between one to all vehicles. Although attacker's motion is bounded, gain changing empowers attacker to create collisions with more physical damages in platoon.

VI. Acknowledgment

This material is based in part upon work supported by the National Science Foundation under Grant No. 1410000.

References

[1] P. Kavathekar and Y. Chen, "Vehicle platooning: A brief survey and categorization," in *ASME 2011 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*. American Society of Mechanical Engineers, 2011, pp. 829–845.

[2] E. van Nunen, R. Kwakkernaat, J. Ploeg, and B. D. Netten, "Cooperative competition for future mobility," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 3, pp. 1018–1025, 2012.

[3] J. Hedrick, "Constant spacing strategies for platooning in automated highway systemsˆ," 1999.

[4] S. Sheikholeslam and C. A. Desoer, "Longitudinal control of a platoon of vehicles," in *American Control Conference, 1990*. IEEE, 1990, pp. 291–296.

[5] S. Dadras, "Path tracking using fractional order extremum seeking controller for autonomous ground vehicle," in *SAE Technical Paper*. SAE International, 03 2017. [Online]. Available: https://doi.org/10.4271/2017-01-0094

[6] S. E. Shladover, C. A. Desoer, J. K. Hedrick, M. Tomizuka, J. Walrand, W.-B. Zhang, D. H. McMahon, H. Peng, S. Sheikholeslam, and N. McKeown, "Automated vehicle control developments in the path program," *IEEE Transactions on vehicular technology*, vol. 40, no. 1, pp. 114–130, 1991.

[7] D. Swaroop, "String stability of interconnected systems: An application to platooning in automated highway systems," *California Partners for Advanced Transit and Highways (PATH)*, 1997.

[8] R. Rajamani, H.-S. Tan, B. K. Law, and W.-B. Zhang, "Demonstration of integrated longitudinal and lateral control for the operation of automated vehicles in platoons," *IEEE Transactions on Control Systems Technology*, vol. 8, no. 4, pp. 695–708, 2000.

[9] E. Shaw and J. K. Hedrick, “String stability analysis for heterogeneous vehicle strings,” in *American Control Conference, 2007. ACC’07.* IEEE, 2007, pp. 3118–3125.

[10] R. Kianfar, P. Falcone, and J. Fredriksson, “A control matching model predictive control approach to string stable vehicle platooning,” *Control Engineering Practice*, vol. 45, pp. 163 – 173, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0967066115300228

[11] T. Litman, “Autonomous vehicle implementation predictions,” 2017.

[12] D. J. Verburg, A. C. M. van der Knaap, and J. Ploeg, “Vehil: developing and testing intelligent vehicles,” in *Intelligent Vehicle Symposium, 2002. IEEE*, vol. 2, June 2002, pp. 537–544 vol.2.

[13] K. J. Malakorn and B. Park, “Assessment of mobility, energy, and environment impacts of intellidrive-based cooperative adaptive cruise control and intelligent traffic signal control,” in *Sustainable Systems and Technology (ISSST), 2010 IEEE International Symposium on*. IEEE, 2010, pp. 1–6.

[14] M. Kaur, J. Martin, and H. Hu, “Comprehensive view of security practices in vehicular networks,” in *Connected Vehicles and Expo (ICCVE), 2016 International Conference on*. IEEE, 2016, pp. 19–26.

[15] S. Dadras and C. Winstead, “Collaborative attacks on vehicular platooning,” 2018.

[16] 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*, ser. ASIA CCS ’15. New York, NY, USA: ACM, 2015, pp. 167–178. [Online]. Available: http://doi.acm.org/10.1145/2714576.2714619

[17] S. Dadras and C. Winstead, “Insider vs. outsider threats to autonomous vehicle platooning,” 2018.

[18] B. DeBruhl, S. Weerakkody, B. Sinopoli, and P. Tague, “Is your commute driving you crazy?: a study of misbehavior in vehicular platoons,” in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2015, p. 22.

[19] S. Dadras and C. Winstead, “Cybersecurity of autonomous vehicle platooning,” 2017.

[20] S. Dadras, S. Dadras, and C. Winstead, “Identification of the attacker in cyber-physical systems with an application to vehicular platooning in adversarial environment,” in *2018 American Control Conference (ACC)*, June 2018.

[21] M. Ghanavati, A. Chakravarthy, and P. Menon, “Pde-based analysis of automotive cyber-attacks on highways,” in *2017 American Control Conference (ACC)*, May 2017, pp. 1833–1838.

[22] M. Ghanavati, A. Chakravarthy, and P. P. Menon, “Analysis of automotive cyber-attacks on highways using partial differential equation models,” *IEEE Transactions on Control of Network Systems*, vol. PP, no. 99, pp. 1–1, 2017.

[23] O. Bokanowski, N. Forcadel, and H. Zidani, “Reachability and minimal times for state constrained nonlinear problems without any controllability assumption,” *SIAM Journal on Control and Optimization*, vol. 48, no. 7, pp. 4292–4316, 2010.

[24] I. M. Mitchell, A. M. Bayen, and C. J. Tomlin, “A time-dependent hamilton-jacobi formulation of reachable sets for continuous dynamic games,” *IEEE Transactions on automatic control*, vol. 50, no. 7, pp. 947–957, 2005.

[25] J. F. Fisac, M. Chen, C. J. Tomlin, and S. S. Sastry, “Reach-avoid problems with time-varying dynamics, targets and constraints,” in *Proceedings of the 18th International Conference on Hybrid Systems: Computation and Control*. ACM, 2015, pp. 11–20.

[26] M. Chen, Q. Hu, C. Mackin, J. F. Fisac, and C. J. Tomlin, “Safe platooning of unmanned aerial vehicles via reachability,” in *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*. IEEE, 2015, pp. 4695–4701.

[27] M. Chen, Q. Hu, J. F. Fisac, K. Akametalu, C. Mackin, and C. J. Tomlin, “Reachability-based safety and goal satisfaction of unmanned aerial platoons on air highways,” *Journal of Guidance, Control, and Dynamics*, 2017.

[28] C. Dabadie, S. Kaynama, and C. J. Tomlin, “A practical reachability-based collision avoidance algorithm for sampled-data systems: Application to ground robots,” in *Intelligent Robots and Systems (IROS 2014), 2014 IEEE/RSJ International Conference on*. IEEE, 2014, pp. 4161–4168.

[29] J. Ding, J. Sprinkle, S. S. Sastry, and C. J. Tomlin, “Reachability calculations for automated aerial refueling,” in *Decision and Control, 2008. CDC 2008. 47th IEEE Conference on*. IEEE, 2008, pp. 3706–3712.

[30] D. Yanakiev and I. Kanellakopoulos, “A simplified framework for string stability analysis in ahs,” in *IN PROCEEDINGS OF THE 13TH IFAC WORLD CONGRESS*, 1996, pp. 177–182.

[31] R. Gagarinov and A. Kurzhanski, “Ellipsoidal toolbox,” 2014.

[32] A. Kurzhanskii and I. Valyi, *Ellipsoidal calculus for estimation and control*. Nelson Thornes, 1997.

[33] C. L. Guernic and A. Girard, “Reachability analysis of linear systems using support functions,” *Nonlinear Analysis: Hybrid Systems*, vol. 4, no. 2, pp. 250 – 262, 2010, {IFAC} World Congress 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1751570X09000387

[34] A. B. Kurzhanski and P. Varaiya, “On ellipsoidal techniques for reachability analysis. part i: external approximations,” *Optimization methods and software*, vol. 17, no. 2, pp. 177–206, 2002.

[35] F. L. Chernousko, *State estimation for dynamic systems*. CRC Press, 1993.

[36] Y. Zhou and J. S. Baras, “Reachable set approach to collision avoidance for uavs,” in *2015 54th IEEE Conference on Decision and Control (CDC)*, Dec 2015, pp. 5947–5952.