Attack Resilient Heterogeneous Vehicle Platooning Using Secure Distributed Nonlinear Model Predictive Control

Mohammad Hossein Basiri, Nasser L. Azad, and Sebastian Fischmeister

Abstract— **Recently, vehicle platoons have offered significant enhancements in traffic management, energy consumption and safety in intelligent transportation systems. Despite the benefits brought by the platoons, they potentially suffer from insecure networks which provide the connectivity among the vehicles participating in the platoon. This paper deals with the secure control of vehicle platoons under the risk of a common cyber attack, namely Denial of Service (DoS) attack. A DoS intruder can endanger the security of platoon by jamming the communication network among the vehicles which is responsible to transmit inter-vehicular data throughout the platoon. This can potentially result in huge performance degradation or even hazardous collisions. We propose a secure distributed nonlinear model predictive control algorithm consisting of i) detection and ii) mitigation phases. The algorithm is capable of handling DoS attack performed on a platoon equipped by different communication topologies and at the same time it guarantees the desired formation control performance. Stability analysis of the attacked platoon running the given algorithm is also presented. Simulation results on a sample heterogeneous attacked platoon exploiting two-predecessor follower communication environment demonstrates the effectiveness of the method.**

I. Introduction

In recent years, vehicle platooning has attracted researchers' attention due to its capability to enhance road throughput, fuel economy, and driving comfort by exploiting wireless data communications. Basically, the vehicles participating in a platoon are able to exchange inter-vehicular data with each other, which in essence, results in improved achievement of the control objectives benefiting from the received data from the ego-vehicle's neighbors [1]. Data transfer among a platoon is mainly managed by Dedicated Short Range Communications (DSRC) in Vehicular Adhoc Networks (VANET) that has been utilized for safety guarantees and reliable data exchange [2]. During years, different controllers have been introduced to take advantage of this connectivity among the vehicles to improve driving experience [3]–[5]. Cooperative Adaptive Cruise Control (CACC) [6], model predictive control [3], and decentralized overlapping control [7], are some instances reported in the literature to achieve specific driving control objectives.

Having been looked at vehicle platoons from a different perspective, they basically lie under a broad class of newly emerged systems, called Cyber Physical Systems (CPS). CPS form large scale widespread systems which provide the ground to bind communication, computation, and control. In these systems, the interconnection of the cyber layer and the physical layer increases the risk of destructive cyber attacks on different parts of the system [8]. Bias injection attack, zero dynamics attack, covert attack, message tampering, and man-in-the-middle attack are several paradigms that can lead to network or system failures. There has been a considerable amount of research on CPS security to address the susceptibility of those systems against cyber attacks [9]–[11].

This should also be noted that although some techniques introduced in the fault-tolerant control are applicable to security problems, most of them have been shown to fail to mitigate the effects of an attack [12]. This is due to the fact that an attacker is intrinsically an intelligent agent who might have some *a priori* knowledge about the system dynamics and the controller contrary to a random fault. Furthermore, an intelligent adversary might target specific components of a system based on his own criteria, such as optimizing the amount of consumed energy or the intended level of devastation. In this respect, various system-theoretic, graph-theoretic, and game-theoretic approaches [13]–[16] have been proposed in the last decade to address security issues of general control systems.

Hence, referring back to vehicle platoons as a class of CPS, aside from the advantages raised by the wireless connectivity in a platoon, connected vehicles can be highly vulnerable to cyber attacks [17]–[19]. Various types of intrusions imposed by either insider or outsider adversary on connected vehicles such as GPS spoofing, DoS, masquerading, insider/outsider eavesdropping have been investigated in literature [20]. Each of these attacks can degrade system performance by violating one or more of the data integrity, data availability, and data confidentiality. A detailed and formal attack classification in a three-dimensions attack space is presented in [21].

Adversarial attackers can even access the control of the vehicles remotely, hence, largely endanger the safety of the platoon. For instance, false data injected by a replay intruder, which seems admissible to the system and the controller, might cause violation of the safe desired gap among consecutive vehicles and result in severe accidents [17]. As another example, in GPS spoofing, legitimate GPS signals are interfered with by the attacker who transmits inaccurate coordinates. This will fool the controller of an ego-vehicle; thus, incorrect torque input is applied to the wheels, which might cause collisions. Insecure vehicle platooning can also

M. H. Basiri, and S. Fischmeister are with the Department of Electrical and Computer Engineering, University of Waterloo, ON, Canada, E-mail: {mh.basiri, sfischme}@uwaterloo.ca.

N. L. Azad is with the Department of Systems Design Engineering, University of Waterloo, ON, Canada, E-mail: nlashgar@uwaterloo.ca.

be a consequence of individual unreliable cars participating in the string of vehicles. As a practical means for the attacker, he might access remotely to the CAN bus of the car through unauthorized infotainment facility, thereby take the full control of acceleration or braking operations [22].

Consequently, it is of significant importance to ensuring the safety and security of a platoon despite the existence of such attacks to guarantee the desired driving performance. In this paper, we focus on the malicious DoS attack, which aims to devastate the communication link among the vehicles. In fact, a DoS attacker uses the disruption resources to violate data integrity or availability, hence, causes a blockage or at least suffering delays in data transfer in the network by making the beacon nodes unnecessarily busy. Researchers have devoted efforts to address the DoS attack in networked control systems and platoons; however, they mostly limit the study to linear models along with a linear controller applied to homogeneous platoons and assume perfect communication links [3], [23]–[25].

We consider a general heterogeneous platoon under DoS attack with nonlinear vehicle dynamics in our analyses. It is shown that our proposed algorithm mitigates the effect of the attack while the desired platoon formation is maintained. The stability of the attacked platoon exploiting the introduced technique is also investigated. Besides, our proposed method can handle different communication topologies, which are some other missing contributions in the literature.

The remainder of this paper is organized as follows. Sec. II defines the problem statement, including the control objectives and the attack model. Sec. III details the main results and describes the proposed algorithm. Stability analysis of the attacked platoon employing the proposed method is presented in the section. Simulation results on a sample heterogeneous attacked platoon demonstrating the fruitfulness of the method are given in Sec. IV. Finally, Sec. V concludes the paper and gives some open avenues to continue this work.

II. Problem Statement

A. System Model

We consider a heterogeneous platoon consisting of n follower vehicles each of which modeled with the following discrete-time nonlinear dynamics model [3]

$$\begin{cases} p_i(t+1) = p_i(t) + v_i(t)\Delta t, \\ v_i(t+1) = v_i(t) + \dfrac{\Delta t}{M_i}\left(\eta_{T,i}\dfrac{T_i(t)}{R_{w,i}} - C_{A,i}v_i^2(t) - M_i g f_{r,i}\right) \\ T_i(t+1) = T_i(t) - \dfrac{1}{\tau_i}T_i(t)\Delta t + \dfrac{1}{\tau_i}u_i\Delta t, \quad i = 1,2,\dots,n \end{cases} \tag{1}$$

where Δt is the sampling time, $p_i(t)$ and $v_i(t)$ are the position and velocity of vehicle i, respectively. M_i denotes the mass, $C_{A,i}$ is the coefficient of aerodynamic drag, $f_{r,i}$ is the coefficient of rolling resistance, g is the gravity constant, $T_i(t)$ is the actual driving/braking torque applied to the drivetrain, $R_{w,i}$ is the tire radius, τ_i is the inertial lag of vehicle powertrain, $\eta_{T,i}$ is the mechanical efficiency of the driveline, and $u_i(t)$ is the desired driving/braking torque which represents the control input.

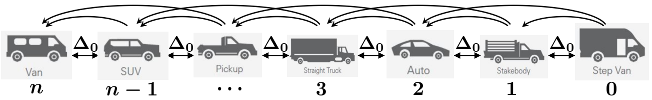


Fig. 1: TPF heterogeneous platoon consisted of n followers

The states and outputs of each vehicle are represented by $x_i(t) = [p_i(t), v_i(t), T_i(t)]^\intercal$, and $y_i(t) = [p_i(t), v_i(t)]^\intercal$, respectively. Collecting the nonlinear terms of the dynamics (1) creates a more compact form

$$\begin{cases} x_i(t+1) = \phi_i\left(x_i(t)\right) + \psi_i u_i(t) \\ \quad y_i(t) = \gamma x_i(t). \end{cases} \tag{2}$$

where $\psi_i = [0, 0, (1/\tau_i)\Delta t]^\intercal$, $\gamma = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$, and

$$\phi_i = \begin{bmatrix} p_i(t) + v_i(t)\Delta t \\ v_i(t) + \dfrac{\Delta t}{M_i}\left(\eta_{T,i}\dfrac{T_i(t)}{R_{w,i}} - C_{A,i}v_i^2(t) - M_i g f_{r,i}\right) \\ T_i(t) - (1/\tau_i)T_i(t)\Delta t \end{bmatrix}$$

Stacking the states, outputs, and the control input signals of all vehicles into vectors yields the platoon dynamics as follows

$$\begin{cases} X(t+1) = \mathbf{\Phi}(X(t)) + \mathbf{\Psi}U(t), \\ Y(t+1) = \mathbf{\Theta}\cdot X(t+1), \end{cases} \tag{3}$$

where $X(t) = [x_1(t)^\intercal, x_2(t)^\intercal, \dots, x_n(t)^\intercal]^\intercal \in \mathbb{R}^{3n\times 1}$, $Y(t) = [y_1(t)^\intercal, y_2(t)^\intercal, \dots, y_n(t)^\intercal]^\intercal \in \mathbb{R}^{2n\times 1}$, $U(t) = [u_1(t), u_2(t), \dots, u_n(t)]^\intercal \in \mathbb{R}^{n\times 1}$. Besides, $\mathbf{\Phi} = [\phi_1^\intercal, \phi_2^\intercal, \dots, \phi_n^\intercal]^\intercal \in \mathbb{R}^{3n\times 1}$, $\mathbf{\Psi} = \mathrm{diag}\{\psi_1, \psi_2, \dots, \psi_n\} \in \mathbb{R}^{3n\times n}$, and $\mathbf{\Theta} = I_N \otimes \gamma \in \mathbb{R}^{2n\times 3n}$.

We model the communication links among the vehicles in the platoon by a graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ where $\mathcal{V}$ and $\mathcal{E}$ denote the set of nodes (vehicles) and the edges (modeling the links between the vehicles), respectively [26]. Followed by this definition, the adjacency, in-degree, and pinning matrices are defined as

$$\mathcal{A} = [a_{ij}] = \begin{cases} a_{ij} = 1, & \text{if } \{j,i\} \in \mathcal{E} \\ a_{ij} = 0, & \text{if } \{j,i\} \notin \mathcal{E} \end{cases} \tag{4}$$

$$\mathcal{D} = \mathrm{diag}\{\mathrm{deg}_1, \mathrm{deg}_2, \dots, \mathrm{deg}_n\} \tag{5}$$

$$\mathcal{P} = \mathrm{diag}\{p_1, p_2, \dots, p_n\} \tag{6}$$

where $\mathrm{deg}_i = \Sigma_{j=1}^n a_{ij}$, and $p_i = 1$ if the leader vehicle can send data to vehicle i and $p_i = 0$ otherwise. Furthermore, we define the neighbor set of vehicle i as $\mathcal{N}_i = \{j \mid a_{ij} = 1, j = 1, 2, \dots, n\}$ which are the vehicles that can send data to vehicle i. Besides, we define the set $\mathcal{O}_i = \{j \mid a_{ji} = 1, j = 1, 2, \dots, n\}$ which are the vehicles that can receive data from vehicle i. If vehicle i can also receive data from the leader, then $\mathcal{I}_i = \mathcal{N}_i \cup \{0\}$, otherwise $\mathcal{I}_i = \mathcal{N}_i$. In this paper, for convenience, we consider a heterogeneous platoon equipped by Two-Predecessor Follower (TPF) communication topology as an example shown in Fig. 1; however, it is easy to adapt our algorithm for other communication topologies.

B. Platoon Control Objectives

The platoon control objective is for the followers to track the reference speed profile generated by the leader while maintaining a constant distance between any two consecutive vehicles, i.e.

$$\begin{cases} \lim\limits_{t\to\infty} \|v_i(t) - v_0(t)\| = 0, \\ \lim\limits_{t\to\infty} \|p_{i-1}(t) - p_i(t) - \Delta_{i-1,i}\| = 0, \end{cases} \quad i = 1, 2, \ldots, n, \tag{7}$$

where $\Delta_{i-1,i} = \Delta_0$ is the desired constant space between consecutive vehicles $i-1$ and i.

C. Attack Description

We focus on a widely spread cyber attack, called the DoS attack. Basically, a DoS attacker jeopardizes the security of the system through jamming the network by flooding it with fake requests so that the shared network becomes overwhelmed by these demands, hence, is too busy to process the legitimate requests sent by the authorized users [27], [28]. This inherently causes packet loss or at least suffering delays in data transfers. In our application, we assume that the DoS attacker is able to block the communication link among two nonconsecutive neighboring vehicles which results in missing inter-vehicular data received by the follower vehicle. In essence, if the communication link among vehicle i and $i-2$ is attacked during $t \in [t_0, t_1]$, the vehicle i is only able to receive the valid data up to $t = t_0$ and has the exact same data until the attack is over, i.e., vehicle i will restart to receive updated data from vehicle $i-2$ at $t > t_1$. In the rest of the paper, we denote $\tau_a = t_1 - t_0$ as the attack period for notational convenience.

Assumption 1: As a standard assumption and from a practical point of view, we assume that the attacker has a limited amount of energy resources that prevents him from jamming the network ceaselessly [16], [29], [30]. □

Remark 1: It is remarkable that the DoS attacker never attacks a link among consecutive vehicles. This is due to fact that in our algorithm the positions and velocities are transmitted which can be reliably measured by on-board sensors mounted on an ego-vehicle such as GPS and radar. Hence, once a follower detects that those quantities are no longer updated, it can switch to its redundant sensors to have real time data. □

III. Main Results

A. Secure–DNMPC for Vehicle Platooning

To combat the DoS attacker described in the previous section, we exploit a modified version of the Distributed Nonlinear Model Predictive Control (DNMPC) approach proposed in [3], called Secure–DNMPC which aims at mitigating the effects of the attack while achieving the desired control objectives. The algorithm is basically composed of two main phases, namely i) the detection and ii) the mitigation phase. In the first phase, we attempt to detect if a DoS attack is underway. If an attack is detected such that the communication link connecting the ego-vehicle with its immediate preceding or following vehicle is endangered, then the algorithm commands the victim vehicle to ignore the data received through the V2V link (until the attack is over) and switch to its on-board sensors followed by the implementation of the Secure–DNMPC. Otherwise, if the blocked link corresponds to the farther neighbors of the ego-vehicle, the victim vehicle makes use of the most recent updated data prior to the attack commence and the mitigation phase starts by performing Secure–DNMPC. Inherently, in the second phase, each vehicle solves a local optimal control problem given as follows to generate its own optimal control input signal which then needs to be exchanged with its neighbors.

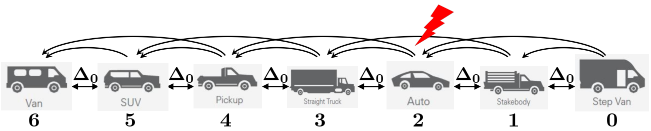


Fig. 2: TPF heterogeneous platoon imposed by a DoS attacker on the communication link between vehicle 1 and 3

Problem 1 (Local NMPC): Each vehicle i has to solve a local NMPC problem at each time instant t to get its own optimal control input and exchange it with its neighbors as follows

Local NMPC: Vehicle $i = 1, 2, \ldots, n$, has to solve the following optimization problem with prediction horizon N_p at each time instant t

$$\begin{aligned} &\min_{u_i^p(0|t-\tau_a),\ldots,u_i^p(N_p-1|t-\tau_a)} J_i(y_i^p, u_i^p, y_i^a, y_{-i}^a) \\ &\quad = \Sigma_{k=0}^{N_p-1} \Big(\big\| y_i^p(k|t-\tau_a) - y_{\text{des},i}^a(k|t-\tau_a) \big\|_{Q_i} \\ &\quad + \| u_i^p(k|t-\tau_a) - h_i(v_i^p(k|t-\tau_a)) \|_{R_i} \\ &\quad + \| y_i^p(k|t-\tau_a) - y_i^a(k|t-\tau_a) \|_{F_i} \\ &\quad + \Sigma_{j\in\mathcal{N}_i} \Big\| y_i^p(k|t-\tau_a) - y_j^a(k|t-\tau_a) - \tilde{\Delta}_{i,j} \Big\|_{G_i} \Big) \end{aligned}$$

Subject to:

$$\begin{aligned} x_i^p(k+1|t-\tau_a) &= \phi(x_i^p(k|t-\tau_a)) + \psi u_i^p(k|t-\tau_a) \\ y_i^p(k|t-\tau_a) &= \gamma x_i^p(k|t-\tau_a) \\ x_i^p(0|t-\tau_a) &= x_i(t-\tau_a) \\ u_i^p(k|t-\tau_a) &\in \mathfrak{U}_i \\ y_i^p(N_p|t-\tau_a) &= \frac{1}{|\mathcal{I}_i|} \Sigma_{j\in\mathcal{I}_i} \left(y_{-j}^a(N_p|t-\tau_a) + \tilde{\Delta}_{i,j} \right) \\ T_i^p(N_p|t-\tau_a) &= h_i(v_i^p(N_p|t-\tau_a)) \end{aligned}$$

where $y_{\text{des},i}(t) = \gamma x_{\text{des},i}(t)$, $x_{\text{des},i}(t) = [p_0(t) - i\Delta_0, v_0, h_i(v_0)]^\mathsf{T}$, $h_i(v_0) = \frac{R_{w,i}}{\eta_{T,i}} \times \left(C_{A,i} v_0^2 + M_i g f_{r,i} \right)$, $\mathfrak{U}_i = \{u_i \mid u_i \in [\underline{u}_i, \bar{u}_i]\}$ defines the feasible bounds on the control input, $\tilde{\Delta}_{i,j} = [\Delta_{i,j}, 0]^\mathsf{T}$ denotes the desired spacing between the vehicles i and j, and Q_i, R_i, F_i, and G_i are the NMPC tuning weight matrices. $y_i^a(t)$ represents

Algorithm 1 Secure–DNMPC for Vehicle Platooning under DoS Attack

```
1:  Initialization:
    Assumed values for vehicle $i$ are set at time $t = 0$,
        $u_i^a(k|0) = h_i(v_i(0)), y_i^a(k|0) = y_i^p(k|0), \quad k = 0, 1, \ldots, N_p - 1$
2:  while $t \leq t_{\text{final}}$ do
3:    if $p_{-j}^a(t) = p_{-j}^a(t-1), j \in \mathcal{N}_i$ then          ▷ Check to see if a DoS is underway
4:      if $j = i - 1$ or $j = i + 1$ then                               ▷ Check to see if the attacked link
5:                                                       corresponds to a predecessor or a follower
6:        Disable communication link, switch to on-board sensors & Go to: 8
7:      else
8:        for Each vehicle $i$ do                                           ▷ Implement Secure–DNMPC
9:          Solve Problem 1 at time $t > 0$ and yield $u_i^*(k|t-\tau_a), \quad k = 0, 1, \ldots, N_p - 1$
10:         Compute: $\begin{cases} x_i^*(k+1|t-\tau_a) = \phi_i(x_i^*(k|t-\tau_a)) + \psi_i u_i^*(k|t-\tau_a), \\ \quad x_i^*(0|t-\tau_a) = x_i(t-\tau_a), \quad k = 0, 1, \ldots, N_p - 1 \end{cases}$
11:         Compute: $u_i^a(k|t-\tau_a+1) = \begin{cases} u_i^*(k+1|t-\tau_a), & k = 0, 1, \ldots, N_p - 2 \\ h_i\left(v_i^*(N_p|t-\tau_a)\right), & k = N_p - 1 \end{cases}$
12:         Compute: $\begin{cases} x_i^a(k+1|t-\tau_a+1) = \phi_i\left(x_i^a(k|t-\tau_a+1)\right) + \psi_i u_i^a(k|t-\tau_a+1) \\ \quad x_i^a(0|t-\tau_a+1) = x_i^*(1|t-\tau_a), \quad k = 0, 1, \ldots, N_p - 1 \end{cases}$
13:         Compute: $y_i^a(k|t-\tau_a+1) = \gamma x_i^a(k|t-\tau_a+1), \quad k = 0, 1, \ldots, N_p - 1$
14:         Send $y_i^a(k|t-\tau_a+1)$ to the vehicles lie in the set $\mathcal{O}_i$, and receive $y_{-j}^a(k|t-\tau_a+1)$ from neighboring
    vehicles $j \in \mathcal{N}_i$ and compute $y_{\text{des},i}(k|t-\tau_a+1)$
15:         Exert the first element of the optimal control signal $u_i(t-\tau_a) = u_i^*(0|t-\tau_a)$
16:       end for
17:     end if
18:   end if
19: end while
```

the data sent by the vehicle i to the set $\mathcal{O}_i$ while y_{-j}^a denotes the data received by the vehicle i from its neighbors $j \in \mathcal{N}_i$. The penultimate constraint referred to as the terminal averaging constraint is to enforce the vehicle i to have the same output as the average of assumed outputs in $\mathcal{I}_i$. The last terminal constraint is to enforce vehicle i to drive with a constant speed at the end of the prediction horizon. These two constraints are necessary for the stability of the DMPC algorithm [3]. Superscript a, p, and $*$ are to distinguish between assumed, predicted and optimal quantities, respectively. The assumed quantities are the ones transmitted by the vehicles in the platoon. □

The proposed approach is described in detail in Algorithm 1.

B. Stability Analysis of Secure–DNMPC

In this section we analyze the stability of the Secure–DNMPC algorithm which incorporates the time delay τ_a imposed by the DoS attacker. Prior to stability analysis, we first introduce the following Lemmas.

Lemma 1 ([31]): The eigenvalues of Kronecker product of two matrices $A \in \mathbb{R}^{n \times n}$ and $B \in \mathbb{R}^{m \times m}$ are

$$\lambda_i \mu_j, \quad i = 1, 2, \ldots, n, \quad j = 1, 2, \ldots, m,$$

where λ_i and μ_j are the eigenvalues of A and B, respectively. □

Lemma 2 ([3]): For any platoon wherein all the vehicles can receive data (directly/indirectly) from the leader vehicle, the eigenvalues of $(\mathcal{D} + \mathcal{P})^{-1} \mathcal{A}$ lie within the unit circle disk, i.e.

$$\left| \lambda_i \left\{ (\mathcal{D} + \mathcal{P})^{-1} \mathcal{A} \right\} \right| < 1. \tag{8}$$

□

Now, we can prove the stability of the Secure–DNMPC algorithm.

Theorem 1: If a platoon which is under a DoS attack satisfies the condition in Lemma 2, then the terminal output of the system controlled by the Secure–DNMPC proposed in Algorithm 1 asymptotically converges to the desired state, i.e.

$$\lim_{t \to \infty} |y_i^p(N_p|t-\tau_a) - y_{\text{des},i}(N_p|t-\tau_a)| = 0. \tag{9}$$

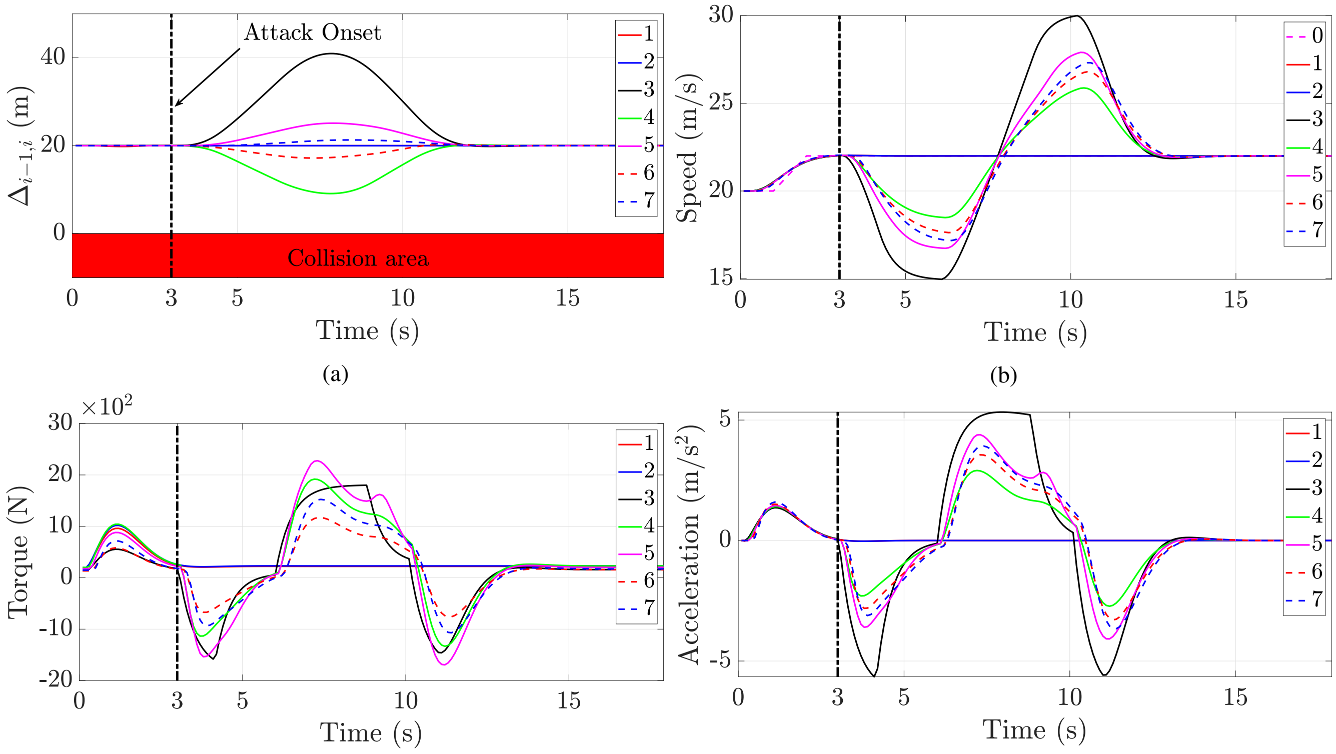
□

Proof: First of all, we state that a suitable Lyapunov candidate to prove the asymptotic stability is the sum of all local cost functions introduced in the local NMPC problem as suggested by [32]

$$\begin{aligned} J_\Sigma^*(t-\tau_a) = \Sigma_{i=1}^n J_i^* \big(& y_i^*(:|t-\tau_a), u_i^*(:|t-\tau_a), \\ & y_i^a(:|t-\tau_a), y_{-i}^a(:|t-\tau_a) \big). \end{aligned}$$

Inspired by a similar idea used in [3], we define the tracking error output vector

$$\tilde{y}_i^p(N_p|t-\tau_a) = y_i^p(N_p|t-\tau_a) - y_{\text{des},i}(N_p|t-\tau_a) \tag{10}$$



(a)

(b)

(c)

(d)

Fig. 3: (a) Consecutive spacing, (b) speed, (c) torque, and (d) acceleration of the TPF heterogeneous DoS attacked platoon

As we assumed that the followers have zero acceleration at the end of the horizon, using the update control law defined in line 11 of the Algorithm 1 we get

$$y_i^a(N_p|t-\tau_a+1) = y_i^p(N_p|t-\tau_a)+Ey_i^p(N_p|t-\tau_a)\Delta t, \tag{11}$$

where $E = \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$. Combining (11) with the terminal averaging constraint together with considering the defined tracking error vector in (10) yields

$$\tilde{y}_i^p(N_p|t-\tau_a+1) = \frac{1}{|\mathcal{I}_i|}\Sigma_{j\in\mathcal{I}_i}(I_2+E\Delta t)\tilde{y}_j^p(N_p|t-\tau_a). \tag{12}$$

This can be rewritten in a matrix format

$$\tilde{Y}^p(N_p|t-\tau_a+1) = \big((\mathcal{D}+\mathcal{P})^{-1}\mathcal{A}\big)\otimes(I_2+E\Delta t)\tilde{Y}^p(N_p|t-\tau_a) \tag{13}$$

where $\tilde{Y}^p(N_p|t-\tau_a) = [\tilde{y}_j^p(N_p|t-\tau_a),\ldots,\tilde{y}_j^p(N_p|t-\tau_a)]^\intercal \in \mathbb{R}^{2n\times 1}$. Based on Lemma 2 the eigenvalues of $(\mathcal{D}+\mathcal{P})^{-1}\mathcal{A}$ lie within the unit circle disk. Besides, one can easily check that the eigenvalues of $I_2+E\Delta t$ are all equal to one. Hence, according to Lemma 1, the eigenvalues of $\big((\mathcal{D}+\mathcal{P})^{-1}\mathcal{A}\big)\otimes(I_2+E\Delta t)$ lie within the unit circle disk. This together with (13) completes the proof. ■

IV. Simulation Results

A heterogeneous platoon consisted of seven different vehicles is considered where they can exchange inter-vehicular data among each other through the TPF communication topology. It is assumed that the communication link among the vehicle 1 and 3 is subject to a DoS attack. Hence, vehicle 3 will not be able to receive the real time data including the position and velocity of vehicle 1 while the attack is performing (see Fig. 2). It is notable that to tackle a practical scenario, based on Assumption 1 the external intruder is able to cause communication degradation among the vehicles for a finite time period. In the simulations the DoS attacker starts jamming the communication link from vehicle 1 to 3 for $\tau_a = 3$ seconds in the time interval $t \in [3, 6]$. Seven different vehicles with practical parameters form the platoon wherein the leader vehicle starts driving at $v_0(0) = 20m/s$ for one second, then it accelerates to reach $v_0(2) = 22m/s$ and continues with this velocity until the end of the simulation. The prediction horizon and desired spacing among consecutive vehicles have been chosen as $N_p = 20$, and $\Delta_0 = 20$ meters, respectively. We have extended the code in [33] for our security analysis. From Fig. 3a one can see that despite the blockage of data transfer link from vehicle 1 to 3, there is no collision occurred in the platoon and the safety has been ensured. Besides, Fig. 3b demonstrates that Secure–DNMPC algorithm effectively mitigates the DoS attack and the followers begin to keep tracking the leader's speed profile shortly after the attack is over. Convergence of torque and acceleration are also shown in Fig. 3c, and 3d. We highlight that the proposed algorithm has been also successfully tested on different platoon formations such as Two-Predecessor Leader Follower (TPLF), with different spacing policies such as Constant Time Headway (CTH) policy, and also on Federal Test Procedure (FTP) drive cycle to emulate urban driving.

Remark 2: To select an appropriate value for the prediction horizon, one has to notice as τ_a increases, N_p needs to be decreased in order to let the vehicles have enough time to exchange and update their data prior to the attack occurrence. On the other hand, too small values for N_p results in frequent rapid oscillations in the control input which makes the controller unimplementable in practice. □

V. Conclusion and Future Works

Having focused on a general heterogeneous platoon formation under the risk of DoS attack, we proposed a secure control algorithm which enables the platoon to detect and mitigate the devastation imposed by the intruder. The algorithm guarantees the desired platoon performance in terms of its control objectives together with its safety. Besides, the proposed method tackles the attacker regardless of the employed communication topology among the vehicles. Simulations performed on a TPF heterogeneous platoon with practical vehicle dynamics parameters indicate the efficacy of the proposed technique. Dealing with other cyber attacks along with achieving additional performance objectives such as driving comfort and ecological driving are left as our future studies.

Acknowledgment

The authors would like to thank Dr. Yang Zheng (SEAS and CGBC at Harvard University, Cambridge, MA, USA) for the fruitful discussions during this work. Also, the authors would like to thank the support from NSERC of Canada.

References

[1] D. Swaroop, J. K. Hedrick, and S. B. Choi, "Direct adaptive longitudinal control of vehicle platoons," *IEEE Transactions on Vehicular Technology*, vol. 50, no. 1, pp. 150–161, 2001.

[2] J. Guo and N. Balon, "Vehicular ad hoc networks and dedicated short-range communication," *University of Michigan*, 2006.

[3] Y. Zheng, S. E. Li, K. Li, F. Borrelli, and J. K. Hedrick, "Distributed model predictive control for heterogeneous vehicle platoons under unidirectional topologies," *IEEE Transactions on Control Systems Technology*, vol. 25, no. 3, pp. 899–910, 2017.

[4] E. van Nunen, J. Reinders, E. Semsar-Kazerooni, and N. Van De Wouw, "String stable model predictive cooperative adaptive cruise control for heterogeneous platoons," *IEEE Transactions on Intelligent Vehicles*, vol. 4, no. 2, pp. 186–196, 2019.

[5] F. Acciani, P. Frasca, G. Heijenk, and A. Stoorvogel, "Stochastic string stability of vehicle platoons via cooperative adaptive cruise control with lossy communication," *arXiv preprint arXiv:1905.04779*, 2019.

[6] V. Milanés, S. E. Shladover, J. Spring, C. Nowakowski, H. Kawazoe, and M. Nakamura, "Cooperative adaptive cruise control in real traffic situations," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 1, pp. 296–305, 2013.

[7] S. S. Stankovic, M. J. Stanojevic, and D. D. Siljak, "Decentralized overlapping control of a platoon of vehicles," *IEEE Transactions on Control Systems Technology*, vol. 8, no. 5, pp. 816–832, 2000.

[8] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems securitya survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

[9] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry *et al.*, "Challenges for securing cyber physical systems," in *Workshop on future directions in cyber-physical systems security*, vol. 5, no. 1, 2009.

[10] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[11] M. H. Basiri, J. G. Thistle, J. W. Simpson-Porco, and S. Fischmeister, "Kalman filter based secure state estimation and individual attacked sensor detection in cyber-physical systems," in *2019 American Control Conference (ACC)*. IEEE, 2019, pp. 3841–3848.

[12] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *2008 The 28th International Conference on Distributed Computing Systems Workshops*. IEEE, 2008, pp. 495–500.

[13] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE transactions on automatic control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[14] Y.-C. Liu, G. Bianchin, and F. Pasqualetti, "Secure trajectory planning against undetectable spoofing attacks," *Automatica*, vol. 112, p. 108655, 2020.

[15] S. Weerakkody, X. Liu, S. H. Son, and B. Sinopoli, "A graph-theoretic characterization of perfect attackability for secure design of distributed control systems," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 60–70, 2016.

[16] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Transactions on Automatic Control*, vol. 60, no. 10, pp. 2831–2836, 2015.

[17] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 126–132, 2015.

[18] P. Koopman and M. Wagner, "Autonomous vehicle safety: An interdisciplinary challenge," *IEEE Intelligent Transportation Systems Magazine*, vol. 9, no. 1, pp. 90–96, 2017.

[19] M. H. Basiri, M. Pirani, N. L. Azad, and S. Fischmeister, "Security of vehicle platooning: A game-theoretic approach," *IEEE Access*, vol. 7, no. 1, pp. 185 565–185 579, 2019.

[20] C. Laurendeau and M. Barbeau, "Threats to security in dsrc/wave," in *International Conference on Ad-Hoc Networks and Wireless*. Springer, 2006, pp. 266–279.

[21] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[22] P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the in-vehicle network in the connected car," in *2011 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2011, pp. 528–533.

[23] M. Long, C.-H. Wu, and J. Y. Hung, "Denial of service attacks on network-based control systems: impact and mitigation," *IEEE Transactions on Industrial Informatics*, vol. 1, no. 2, pp. 85–96, 2005.

[24] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-time detection of denial-of-service attacks in ieee 802.11 p vehicular networks," *IEEE Communications letters*, vol. 18, no. 1, pp. 110–113, 2013.

[25] Z. A. Biron, S. Dey, and P. Pisu, "Resilient control strategy under denial of service in connected vehicles," in *2017 American Control Conference (ACC)*. IEEE, 2017, pp. 4971–4976.

[26] F. L. Lewis, H. Zhang, K. Hengster-Movric, and A. Das, *Cooperative control of multi-agent systems: optimal and adaptive design approaches*. Springer Science & Business Media, 2013.

[27] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Başar, "Resilient control of cyber-physical systems against denial-of-service attacks," in *2013 6th International Symposium on Resilient Control Systems (ISRCS)*. IEEE, 2013, pp. 54–59.

[28] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2009, pp. 31–45.

[29] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 3023–3028, 2015.

[30] Q. Sun, K. Zhang, and Y. Shi, "Resilient model predictive control of cyber-physical systems under dos attacks," *IEEE Transactions on Industrial Informatics*, 2019.

[31] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge university press, 2012.

[32] T. Keviczky, F. Borrelli, and G. J. Balas, "Decentralized receding horizon control for large scale dynamically decoupled systems," *Automatica*, vol. 42, no. 12, pp. 2105–2115, 2006.

[33] Y. Zheng, *DMPC for platoons*, 2019, [Online]. Available: https://github.com/zhengy09/DMPC_for_platoons.