2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Leader-follower formations subject to false data injections: a resilient distributed model predictive approach

Domenico Famularo, Giuseppe Franzè, Francesco Tedesco and Antonello Venturino

Abstract— **In this paper, resilience issues for platoons of autonomous agents are addressed when false data injections affect the information exchanged among the neighbors via a communication medium. A distributed model predictive control scheme is used for dealing with the overall regulation task. Conversely, the core of this study relies on the design of an efficient anomaly detector and viable attack countermeasures. In particular, it is formally proven that the proposed device is capable to uncover in finite time malicious actions by simple set-containment set-membership conditions arising from the concept of $k-$ step ahead state predictions convex sets. Moreover, the attack countermeasures have a twofold nature: the first one is conceived by exploiting feasibility arguments of the model predictive philosophy; while the second resilient operation takes inspiration from rejuvenation ideas by leading to safe splitting and/or queuing the initial multi-agent formation.**

I. Introduction

In the last decade, the formation control for multi-agent systems (MASs) has received a particular attention thanks to the increasing number of applications arising in the well-known *Industry 4.0* program [1]. In this context, the use of open and unreliable communication platforms leads to the possibility that data sharing among the MAS agents could be tampered by anonymous and malicious intruders with the undesired consequence that perturbed or even wrong command actions are generated, see the recent survey [2].

Despite framed in a research field of remarkable interest, the characterization of resilience operations for multi-agent systems topologically as leader-follower (LF) configurations is still an open question from several points of view. Most of literature items focus on consensus-like problems [5], [6], [7], [8], while the contributions specifically oriented to deal with reference and/or state trajectory tracking issues are few and often overlook cyber intrusions on the communication links among the involved agents, see e.g., [9], [10] and references therein. Nonetheless, some interesting studies have been recently presented in [11], [12]. The first contribution provides an adaptive distributed architecture, based on Lyapunov approach and H_∞ performance, in charge to comply with formation requirements and FDI attacks mitigation. In [12], the authors propose a resilient control for leader-follower configurations tampered by a set of malicious agents. There, the resilience operations are achieved by the leader action that defines a safe state trajectory to be followed by all the followers.

In this paper, a distributed model predictive control (DMPC) strategy capable to take care of prescribed formation constraints and to on-line adopt control viable countermeasures to mitigate prolonged stealthy false data injections (FDIs) on the transmitted data along the LF chain is developed. The proposed DMPC design takes inspiration from [3] and [4] properly customized to the present context. In fact, the structure of the local controllers is exploited to prove the existence of a new anomaly detector in charge to reveal in finite time FDI occurrences. In particular, the proposed detector exploits feasibility retention arguments to identify anomalies along the state prediction tubes. On the other hand, as the control countermeasures are concerned, two actions can be pursued without compromising the overall feasibility property and by keeping the look towards the satisfaction of the control requirement (i.e., driving the platoon to a prescribed target): use stored and feasible command inputs as soon as the attack is detected; split the platoon in sub-LF configurations. The first step leverages the fact that in attack-free scenarios, each agent stores and updates the computed MPC sequence within a dedicated buffer. Whereas the second countermeasure comes to play when all the feasible stored control moves have been timely used and concerns with the disconnection and re-activation in finite time of the communication link between an agent and its predecessor, see e.g. , [13].

The effectiveness of the proposed approach is evaluated by means of a truck platoon, in which the involved trucks align in a lane on freeways and run as a group.

Notation and preliminaries

Consider a constrained discrete-time linear time-invariant (LTI) system

$$z(t+1) = \Phi z(t) + G w(t),\ t \in \mathbb{Z}_+ := \{0, 1, \ldots\} \tag{1}$$

with $z(t) \in \mathcal{Z}$ and $w(t) \in \mathcal{W}, \forall t \geq 0$. At the generic time instant t, $\hat{z}_k(t)$ and $\hat{w}_k(t)$ denote predicted state and control input at $t+k$, respectively; while $\hat{\mathbf{z}}(\mathbf{t}) := \{\hat{z}_k(t)\}_{k=1}^N$ and $\hat{\mathbf{w}}_{\mathbf{k}}(\mathbf{t}) := \{\hat{w}_k(t)\}_{k=0}^{N-1}$ account for predicted state trajectories and command inputs of length N.

Definition 1: A set $\Xi \subseteq \mathcal{Z}$ is said Positively Invariant (PI) for (1) if $\forall\, z \in \Xi,\ \exists w \in \mathcal{W} : \Phi z + G w \in \Xi$. □

This work was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC), and in part by the research project - ID:PE00000014 “SEcurity and RIghts in the CyberSpace - SERICS” granted by the Italian Ministry of University and Research (MUR), and European Union within the NextGenerationEU program.

Giuseppe Franzè is with DIMEG, Università della Calabria, Via Pietro Bucci, Cubo 42-C, Rende (CS), 87036, ITALY, giuseppe.franze.@unical.it

Domenico Famularo, Francesco Tedesco and Antonello Venturino are with DIMES, Università della Calabria, Via Pietro Bucci, Cubo 42-C, Rende (CS), 87036, ITALY, {domenico.famularo, franceso.tedesco}.@unical.it, antonello.venturino@dimes.unical.it

979-8-3503-0123-6/23/$31.00 ©2023 IEEE

II. Problem formulation

We will refer to the the class of leader-follower configurations depicted in Fig. 1, whose dynamics is described by the following discrete-time LTI state space model

$$\Sigma^i : \; x^i(t+1) = A_i x^i(t) + B_i u^i(t), \;\; \forall i \in \mathcal{I} := \{1, \ldots, L\}, \tag{2}$$

where $x^i \in \mathbb{R}^n$ is the state, $u^i \in \mathbb{R}^m$ the control input and the following constraints are prescribed:

$$\begin{array}{rl} x^i(t) \in & \mathcal{X}_i := \{x^i \in \mathbb{R}^n : {x^i}^T x^i \leq {\bar{x}^i}{}^2\}, \\ u^i(t) \in & \mathcal{U}_i := \{u^i \in \mathbb{R}^m : {u^i}^T u^i \leq {\bar{u}^i}{}^2\}, \; \forall t \geq 0. \end{array} \tag{3}$$

Let C^i be the local controller associated to each agent Σ^i, and $\Xi_i \subseteq \mathbb{R}^n$ the PI region of the regulated state trajectories under the action of C^i. Then, during the on-line operations the following operating setup is considered:

- data exchange between Σ^i and C^i, $\forall i \in \mathcal{I}$, is not affected by any communication anomalies (induced time delays, false data injections and so on);
- at each time instant t, the agent Σ^i, $i = 1, \ldots, L-1$, transmits to its follower Σ^{i+1} along the LF chain the predicted state trajectory $\hat{\mathbf{x}}^i(t)$, under the action of C^i, and the positively invariant region $\Xi_i(t)$ complying with the current target $\bar{x}^i_t$, hereafter named as the *target set*;
- communication network may be unreliable: the information sent from Σ^i to Σ^{i+1} may be corrupted by malicious intruders as follows:

  - target set:
  $$\hat{\Xi}_i(t) \leftarrow \Xi_i(t) + \Xi_a(t) \tag{4}$$

  - predicted state trajectory:
  $$\hat{\mathbf{z}}^i(t) \leftarrow \hat{\mathbf{x}}^i(t) + \mathbf{x}^a(t) \tag{5}$$

In the sequel, we address the following problem:

Leader-Follower Resilient (LF-R) Problem - *Given the platoon (2)-(3) and a target $x_f \in \mathbb{R}^{L \cdot n}$, design a distributed state-feedback control policy*

$$\begin{array}{rcll} u^1(t) & = & g(x^1(t), x^1_f), & \\ u^i(t) & = & g(x^i(t), x^i_f, \hat{\mathbf{x}}^{i-1}(t)), & \forall i \in \mathcal{I} \setminus \{1\}, \end{array} \tag{6}$$

satisfying constraints (3) and such that, starting from an admissible initial condition $x(0) = [{x^1}^T(0), {x^2}^T(0), \ldots, {x^L}^T(0)]^T$, the team is driven towards $x_f = [{x^1_f}^T(0), {x^2_f}^T(0), \ldots, {x^L_f}^T(0)]^T$ regardless of any admissible occurrence of FDI attacks on the communication network along the leader-follower formation. □

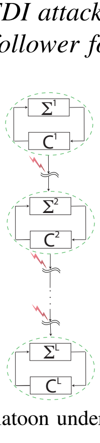

Fig. 1. Platoon under attack

III. The distributed model predictive controller

In this section, a control unit devoted to address the **LF-R** control requirements is outlined by properly customizing the ideas proposed in [15]. Specifically, each agent is equipped with a distributed MPC unit where the leader Σ^1 implements a RHC controller with the prediction horizon length $N_1 = 0$, while each follower Σ^i, $i \in \mathcal{I} \backslash \{1\}$, is regulated by an MPC controller with $N_i = i$. Hence, the following arguments are exploited:

- Dual-mode input parametrization:
  $$\hat{u}^i_k(t) = \left\{ \begin{array}{ll} \hat{u}^i_k(t), & k = 0, \ldots, N_i - 1 \\ K_i(\hat{x}^i_k(t) - \bar{x}^i_t), & k \geq N_i \end{array} \right. \tag{7}$$
  with $K_i \in \mathbb{R}^{m \times n}$ a stabilizing and admissible state feedback law and $\bar{x}^i_t$ an equilibrium condition at the current time instant t;
- Cost function:
  $$J^i(\hat{\mathbf{x}}^i, x^i_f, \hat{\mathbf{u}}^i) := \sum_{k=0}^{N_i - 1} \left[\|\hat{x}^i_k(t) - x^i_f\|^2_{Q_i} + \|\hat{u}^i_k(t)\|^2_{R_i} \right] \tag{8}$$
  where $Q_i > 0$ and $R_i \geq 0$ are symmetric weight matrices.
- Terminal PI region:
  $$\hat{x}^i_{N_i}(t) \in \Xi_i(t) \subset \mathbb{R}^n \tag{9}$$
  The time-varying pair $(\Xi_i(t), K_i(t))$ is computed with respect to $\bar{x}^i_t$.

Since the main aim consists in driving the team towards the target x_f, the condition (9) must be replaced with

$$\hat{x}^i_{N_i}(t) \in \Xi_i(t-1) \cup \Xi_i(t) \tag{10}$$

where $\Xi_i(t)$ is computed such that

$$\bar{x}^i_{t-1} \in \Xi_i(t-1) \cap \Xi_i(t) \tag{11}$$

with $\bar{x}^i_{t-1}$ denoting an equilibrium point selected at the time instant $t-1$.

Within the leader-follower formation, an important requirement consists in ensuring proximity constraints for all the agents within the corresponding PI regions $\Xi_i(t)$, $i = 1, \ldots, L, \forall t \geq 0$. To this end, the PI sets will be computed by resorting to a worst-case approach based on the available information at the previous time instant $t-1$. Notice that at the initial time instant $t = 0$, the pair $(\Xi_1(0), K_1(0))$ is computed by solving the following optimization

$\mathbf{DMPC}^1(t)$:

$$[K_1(t), \Xi_1(t)] = \arg \min_{K_1, \Xi_1} \sum_{k=t}^{\infty} [\|\hat{x}^1_k(t) - x^1_f\|^2_{Q_1} + \|\hat{u}^1_k(t)\|^2_{R_1}] \tag{12}$$

subject to

$$\hat{x}^1_k(t+1) = A_1 \hat{x}^1_k(t) + B_1 \hat{u}^1_k(t), \, \forall k > 0 \tag{13}$$

$$\hat{u}^1_k(t) = K_1 \hat{x}^1_k(t) \in \mathcal{U}_1, \, \forall k > 0 \tag{14}$$

$$\hat{x}^1_k(t) \in \Xi_1 \subseteq \mathcal{X}_1, \, \forall k > 0 \tag{15}$$

$$(A_1 + B_1 K_1)\Xi_1 \subseteq \Xi_1 \subseteq \mathcal{B}\,(x_1(t), \beta_{max}) \tag{16}$$

$$\bar{x}^1_{t-1} \in \Xi_1(t-1) \cap \Xi_1 \tag{17}$$

where $\beta_{max} \in \mathbb{R}_+$ accounts for the maximum displacement of the one-step state evolution starting form the current state condition $x^1(t)$ and $\mathcal{B}\left(x_1(t), \beta_{max}\right)$ is the hyperball of center $x_1(t)$ and radius β_{max}. As a consequence, the leader is driven by

$$\hat{u}_k^1(t) = K_1(t)(x^1(t) - \bar{x}_t^1), \; k \geq 0 \tag{18}$$

where the pair $(\Xi_1(t), K_1(t))$ is updated by shifting $(\Xi_1(t-1), K_1(t-1))$ according to

$$\begin{cases} \Xi_1(t) := \arg\min_{\Xi_1} dist(x_f^1, \Xi_1) \\ \text{subject to } (11) \end{cases} \tag{19}$$

As the followers are concerned, one has that

$$\begin{cases} \Xi_i(t) := \arg\min_{\Xi_i} dist(\Xi_i, \Xi_{i-1}(t-1)), \\ \text{subject to } (11) \text{ and } \Xi \cap (\Xi_{i-1}(t-1) + \mathcal{B}(x^1(t), \epsilon) = \emptyset \end{cases} \tag{20}$$

where $\Xi \cap (\Xi_{i-1}(t-1) + \mathcal{B}(x^1(t), \epsilon)$, with $\epsilon \in \mathbb{R}_+$ a tolerance level, is in charge to guarantee that proximity requirements between the agent Σ^i and its predecessor Σ^{i-1} are always kept.

Hence, given the predecessor predicted state sequence $\hat{x}_k^{i-1}(t)$, each agent Σ^i, determines the augmented predictions $\tilde{x}_k^{i-1}(t)$ compatible with the prediction horizon N_i :

$$\tilde{x}^{i-1}(t) = \begin{cases} \hat{x}_k^{i-1}(t-1), \; k = 1, \ldots, N_{i-1} \\ (A_{i-1} + B_{i-1} K_{i-1})^{t-1+k} (\hat{x}_k^{i-1}(t-1) - \bar{x}_t^{i-1}), \\ k = N_i, \end{cases} \tag{21}$$

and solves the following optimization

DMPC$^i(t)$:

$$\min_{\hat{\mathbf{u}}^i(t)} J^i(\tilde{x}^{i-1}, x_f^i, \hat{\mathbf{u}}^i(t)) \tag{22}$$

subject to

$$\hat{x}_k^i(t+1) = A_i \hat{x}_k^i(t) + B_i \hat{u}_k^i(t) \tag{23}$$

$$\hat{u}_k^i(t) \in \mathcal{U}_i, \; k = 0, 1, \ldots, N_i - 1 \tag{24}$$

$$\hat{x}_k^i(t) \in \mathcal{X}_i, \; k = 0, 1, \ldots, N_i - 1 \tag{25}$$

$$\hat{x}_{N_i}^i(t) \in \Xi_i(t) \tag{26}$$

$$\alpha_{min}^c \leq \|\hat{x}_k^i(t) - \tilde{x}_k^{i-1}(t)\| \leq \alpha_{max}^c, \; k = 0, 1, \ldots, N_i \tag{27}$$

where scalars $\alpha_{max}^c := 2 \cdot \beta_{max}$, $\alpha_{min}^c \in \mathbb{R}^+$ characterize a safe proximity condition between Σ^i and its predecessor Σ^{i-1}.

Notice that the non-convex constraint (27) can be made tractable by using the convexification arguments of [16].

IV. Attack Detection and Resilience Countermeasures

In this section a defense strategy, capable to deal with the possible occurrence of FDI attacks on the communication channel along the LF chain, is presented by resorting to the control architecture of Fig. 2. In order to make the discussion as clear as possible, the main tasks of the proposed resilient approach are separately analyzed.

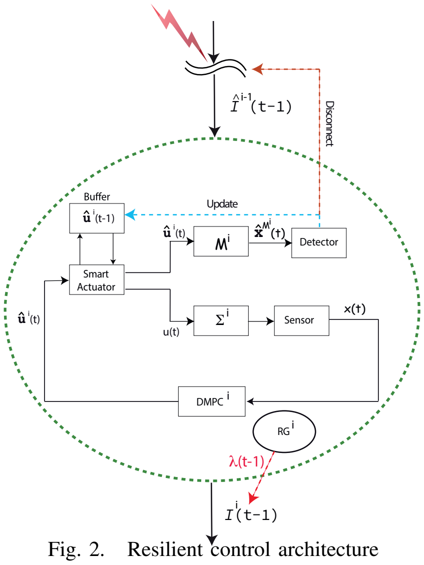

Fig. 2. Resilient control architecture

A. Anomaly detector

According to the problem formulation and DMPC structure, the agent Σ^{i-1} transmits the following information set

$$\mathcal{I}^{i-1}(t) := \{\lambda(t-1)\Xi_{i-1}(t-1), \; \lambda(t-1)\mathbf{z}^{i-1}(t-1), \; \lambda(t-1)K_{i-1}\} \tag{28}$$

where $\lambda \in (0, 1) \subset \mathbb{R}$ is generated by a cryptographically secure pseudo-random number generator unit RG^{i-1}. On the other hand, the agent Σ^i, $i \geq 2$, receives at each t

$$\hat{\mathcal{I}}^i(t) := \{\hat{\Xi}_{i-1}(t-1)/\lambda(t-1), \; \hat{\mathbf{z}}^{i-1}(t-1)/\lambda(t-1), \hat{K}_{i-1}/\lambda(t-1)\} \tag{29}$$

that should be exploited by the local controller for regulation purposes. Notice that the pseudo-random number generators RG^i and RG^{i-1} have the same seed, and are correctly synchronized with each other.

Since the communication medium is unreliable, the data packets in (29) have to be checked in order to verify their integrity. At the current time instant t, the agent Σ^i receives from the predecessor the packet $\hat{\mathcal{I}}^{i-1}(t)$ to be used by the local controller $DMPC^i$ for computing the new sequence $\hat{\mathbf{u}}^i(t)$. The latter is correctly done if the integrity of $\hat{\mathcal{I}}^{i-1}(t)$ is not impaired by malicious actions on the communication channel. Here two set-membership tests are stated and the capability to formally reveal stealthy attacks proven. First, the following condition

$$\hat{\Xi}_{i-1}(t-2) \cap \hat{\Xi}_{i-1}(t-1) \neq \emptyset \tag{30}$$

must be always verified in order to comply with (11). Then, the sequence $\hat{\mathbf{u}}^i(t)$ is checked and, if admissible, exploited at the next time instant $t+1$. To this end, a so-called *twin* model $\mathcal{M}^i$ of the agent Σ^i is defined with the aim to generate the state predictions $\hat{\mathbf{x}}^{\mathcal{M}^i}(t)$ that must fulfill the following inclusions

$$\begin{array}{rl} \hat{x}_0^{\mathcal{M}^i}(t+1) \in & \hat{\mathcal{X}}_i^1(t) \\ \hat{x}_1^{\mathcal{M}^i}(t+1) \in & \hat{\mathcal{X}}_i^2(t) \\ & \vdots \\ \hat{x}_{N_i-2}^{\mathcal{M}^i}(t+1) \in & \hat{\mathcal{X}}_i^{N_i-1}(t) \\ \hat{x}_{N_i-1}^{\mathcal{M}^i}(t+1) \in & \Xi_i(t) \\ \hat{x}_{N_i}^{\mathcal{M}^i}(t+1) \in & \Xi_i(t) \end{array} \tag{31}$$

where

$$\begin{array}{l} \hat{\mathcal{X}}_i^k(t) := \Big\{ x \in \mathcal{X}_i \,|x = A_i x(t) + \sum_{j=0}^{k-1} A_i^{k-i-j} B^i u_j^i(t), \\ \qquad \forall u_j^i(t) \in \mathcal{U}_i, j = 0, \ldots, k-1 \Big\}, \\ \qquad k = 1, \ldots, N_i - 1, \end{array} \tag{32}$$

account for the $k - step$ ahead state predictions polyhedral sets compatible with (3). Then, the following detection logics comes out

$$\mathbf{D}_i(t) := \begin{cases} \text{attack}, & (30) \text{ and/or } (31) \text{ fail} \\ \text{no attack}, & \text{otherwise} \end{cases} \tag{33}$$

Then, the following result holds true.

Proposition 1: Given the platoon configuration of Figs. 1-2. If at each time instant t, the distributed input sequence $\hat{\mathbf{u}}^i(t)$ is obtained as the solution of the optimization (22)-(27), then persistent FDI attacks (4)-(5) are detected by (33).

B. On-line resilient actions

At each time instant t along the LF chain, the following operating scenarios can occur: 1) *nominal mode*: attacks are not underway; 2) *viable mode*: an anomaly has been detected but a control action can be still applied without compromising constraints fulfillment and closed-loop stability; 3) *attack mode*: feasible command inputs are no longer available.

1) Nominal mode: The stored sequence $\hat{\mathbf{u}}^i(t-1)$ is updated with the currently computed sequence $\hat{\mathbf{u}}^i(t)$, while the plant is driven by $\hat{u}^i((t-1)+1)$.

2) Viable mode: As soon as the attack is detected, the **Smart Actuator** is instructed to apply the feasible stored moves $\hat{u}_k^i((t-1))$, $k = 1, \ldots, N_i - 1$, while the newly computed sequence $\hat{\mathbf{u}}^i(t+r)$, $r \geq 1$, is discarded until the attack is underway.

3) Attack mode: When all the stored commands $\hat{u}_k^i(t-1)$, $k = 1, \ldots, N_i - 1$, have been used, a possible countermeasure to keep the resilience capabilities of the overall formation consists in disconnecting the attacked agent Σ^i and its successors Σ^j, $j \geq i+1$, from the rest of the platoon. This means that two or more platoons (even singletons) could come out. For the sake of clarity, let consider the simplified topological scenario consisting of two configurations, namely LF^1 and LF^2. Hence, the agents belonging to the LF^1 configuration keep the same control horizon lengths $N_i = i-1, i = 1\ldots, L^1$, while for the new platoon LF^2 one has that:

$$N_{L^2} = 0,\ N_i = i - L^2,\ i = L^2 + 1, \ldots, L.$$

As a consequence of such an event, it is assumed that an adequate *re-numbering* procedure is implemented so that the new platoons LF^1 and LF^2 are renamed as follows $\{\Sigma_1^i\}_{i=1}^{L^1}$ and $\{\Sigma_2^i\}_{i=1}^{L^2}$. The admissibility of this countermeasure depends on the feasibility of the distributed model predictive control strategy, that can be preserved by exploiting the robust Bellman equation with constraints [18]., i.e., if at the time instant t there exists a solution to $\mathbf{DMPC}^i(t)$ with $N_i > 0$, then at $t+1$ an admissible solution there exists for the same problem with $N_i - k$, $k > 0$. In fact, let $V_{N_i}(x(t)) = J^i(\bar{x}^{i-1}, x_f^i, \hat{\mathbf{u}}^{i^*}(t))$ be the minimum of the cost at the optimal solution $\hat{\mathbf{u}}^{i^*}(t)$ of $\mathbf{DMPC}^i(t)$. The Bellman optimality principle states that an optimal sequence $\hat{\mathbf{u}}^{i^*}(t)$ is such that: given $x_k^i(t)$ along the optimal system trajectory (by applying the input sub-sequence $\{\hat{u}_0^{i^*}(t), \ldots, \hat{u}_{k-1}^{i^*}(t)\}$, then the subsequent input sequence $\{\hat{u}_{k-1}^{i^*}(t), \ldots, \hat{u}_{N_i-1}^{i^*}(t)\}$ is optimal for the cost-to-go over the horizon $[k,\, N_i]$. Moreover, the *Bellman equation* is:

$$\begin{array}{rl} V_{N_i}(x(t)) = & \min\limits_{\hat{\mathbf{u}}^\mathbf{i}(\mathbf{t})} \Big\{ \sum\limits_{i=0}^{k-1} \left[\|\hat{x}^i(t)\|_{Q_i}^2 + \|\hat{u}^i(t)\|_{R_i}^2 \right] + \\ & V_{N_i-k}(x(t)) \Big\} \end{array} \tag{34}$$

According to the above developments, the following result comes out.

Proposition 2: Given the optimal solution $\hat{\mathbf{u}}^{i^*}(t)$ of the optimization $\mathbf{DMPC}^i(t)$. Then at the next time instant $t+1$, there always exists an admissible solution of $\mathbf{DMPC}^i(t+1)$ with the control horizon equals $N_i - k$.

A further countermeasure arises from the fact that the communication link between two agents can be safely excluded and re-activated in a finite time. This translates into the following operating assumption.

Assumption 1: A guaranteed attack-free communication between two disconnected agents Σ^i and Σ^{i+1} can be reestablished in at most k_o time steps. □

For feasibility reasons that will be soon clarified, LF^1 is added to LF^2 or *viceversa* at the leaf node of the first LF chain. As a consequence, the associated DMPC controllers will be implemented over the horizon of lengths $N_h = N_{L^1} + h$, $h = 1, \ldots, L^2$.

Again, the key question to investigate is how queuing operations preserve the overall feasibility property. To this end, denote with $\mathbf{DMPC}_{LF^1}^i(t)$ and $\mathbf{DMPC}_{LF^2}^i(t)$ the optimizations pertaining to the platoons LF^1 and LF^2, respectively. Then, the following argument is considered: positively invariant regions Ξ_i for LF^1 and LF^2 computed under time-delay scenarios are designed to prove that, if at the time instant t there exists a solution to $\mathbf{DMPC}_{LF^2}^i(t)$ (respectively $\mathbf{DMPC}_{LF^1}^1(t)$) with $N_i \geq 0$, then at the next time instant $t+1$ an admissible solution there exists for the same problem with $N_i + k$, $k > 0$.

Let $\bar{t}$ the time instant when the platoon has been split for the first time, the terminal regions $\Xi_i(t), i = 1, \ldots, L$, $\forall t \geq \bar{t}$, must be computed by assuming that a constant time delay τ occurs on the plant dynamics. This is instrumental to ensure that at each time instant t the computed command $u^i(t), i = 1, \ldots, L$, can be consecutively applied, i.e. $u_k^i(t) = u^i(t), k = 1, \ldots, \tau$. In the present context, the delay is imposed to be equal to the number of followers of the initial platoon

$$\tau := L - 1 \tag{35}$$

and this always allows to provide an admissible sequence when the platoon LF^1 and LF^2 regroup. According to this reasoning, first the positively invariant regions are derived by resorting to the so-called Delay Dependent time-delay scenario [19] and the prescribed constraints (3). To this end, by considering the state-feedback control law

$$u^i(t) = K_i\, x^i(t - \tau) \tag{36}$$

and the regulated plant

$$x^i(t+1) = A_i x^i(t) + B_i\, K_i\, x^i(t - \tau), \tag{37}$$

the delayed system technicalities of [19] allow to show that (36) stabilizes the plant and satisfies the prescribed constraints and the ellipsoidal set

$$\Xi_i := \{x^i \in \mathbb{R}^{n_i}\, | x^{i^T} \left(P^i\right)^{-1} x^i \leq 1\},\;\; P_i = P_i^T \geq 0,$$

is a positively invariant region for the closed-loop state evolutions (37) complying with (3), viz. $\Xi_i \subset \mathcal{X}_i$ and $K_i \Xi_i \subset \mathcal{U}_i$.

Hence, the following result hold true.

Proposition 3: Given the optimal solution $\hat{\mathbf{u}}^{i^*}(t)$ of the optimization $\mathbf{DMPC}^i(t)$ (resp. $\mathbf{DMPC}^1(t)$), computed as prescribed in Sections III-IV. Then at the next time instant $t+1$, there always exists an admissible solution of $\mathbf{DMPC}^i(t{+}1)$ (resp. $\mathbf{DMPC}^1(t{+}1)$) with the control horizon equals $N_i + k,\; k \leq L-1$.

Proposition 4: Let $x^i(0)$ and $x^i_f, i = 1, \ldots, L,$ initial and final conditions be given. Then, the control architecture of Fig. 2 always satisfies the prescribed constraints, complies with the requirements of the **LF-R** *problem and ensures that the regulated state trajectories are asymptotically stable.*

Notice that for the sake of space limitations all proofs have been omitted.

V. Numerical Example

A platoon of $L = 10$ trucks enjoying a car-to-car communication medium is considered [20]. The vehicle dynamics is described by a first order position/velocity approximation

$$\left\{\begin{array}{lcl} \dot{p}_i(t) & = & v_i(t) \\ \dot{v}_i(t) & = & -\frac{c}{m} v_i(t) + \frac{1}{m}\, u_i(t),\; i = 1, \ldots, L, \end{array}\right. \tag{38}$$

with $m = 1000\,[\mathrm{Kg}]$ the vehicle mass, $c = 200\,[\frac{\mathrm{N}}{\mathrm{s\,m}}]$ the friction coefficient and the control input is the engine thrust $u_i(t)$. Starting from the following initial conditions:

$$\left\{\begin{array}{l} p_i(0) = 10 - i + 1\,[\mathrm{m}], \\ v_i(0) = 5\,[\frac{\mathrm{m}}{\mathrm{s}}],\; i = 1, \ldots, 10, \end{array}\right.$$

The target consists in asymptotically approach the velocity set-point fixed to $10\;[\frac{\mathrm{m}}{\mathrm{s}}]$ for each vehicle. The trucks are subject to the following thrust and velocity saturation constraints: $|u_i(t)| \leq \overline{u} = 220\,[\mathrm{N}]$; $|v_i(t)| \leq \overline{v} = 11\,[\frac{\mathrm{m}}{\mathrm{s}}]$. The coordination constraints account for the relative distance between a vehicle and its predecessor: $1\,\mathrm{m} \leq |p_{i-1}(t) - p_i(t)| \leq 21\,[\mathrm{m}]$. The vehicle dynamics has been discretized via Euler Method with $T = 0.1\,[\mathrm{s}]$ and the vehicles are required to synchronize their velocities $v_i(t), i \neq 1$ to the constant leader velocity $10\,[\frac{\mathrm{m}}{\mathrm{s}}]$. As a consequence, the target leader position trajectory (motion law) will be a straight line. In the sequel, the proposed **DMPC** architecture of Fig. 2 will be considered. According to (20), the tolerance level has been set $\epsilon = 0.05\,[\mathrm{m}]$.

At time instant $t = 5\,s$ the LF topology is disrupted by means of an FDI attack on the communication channel involving the fourth and fifth vehicles.

The predicted state trajectory $\hat{x}^4_k(t)$ is altered and conveyed to the agent 5 that, in order to track the leader, increases first the local thrust signal ($t \in [5, 6.3]$s) to reach the new reference level $11\,[\frac{\mathrm{m}}{\mathrm{s}}]$ (see Fig. 4) (on the prescribed constraint limit), then ($t \in [6.4, 14.9]$s) slows down toward the velocity set-point $1\,[\frac{\mathrm{m}}{\mathrm{s}}]$ so the attack affects obviously all the remaining vehicles. The achieved results are collected in Figs. 3-8. In particular in Figs. 4, 5 velocities and regulated thrusts of the attacked vehicles $\Sigma^i = 5, \ldots, 10$, are reported, whereas in Fig. 3, the counterpart velocity time evolutions of attack-free vehicles.

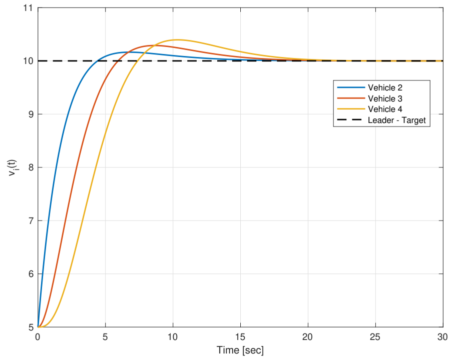

Fig. 3. Leader and $i = 2, 3, 4$ Vehicles (Velocity)

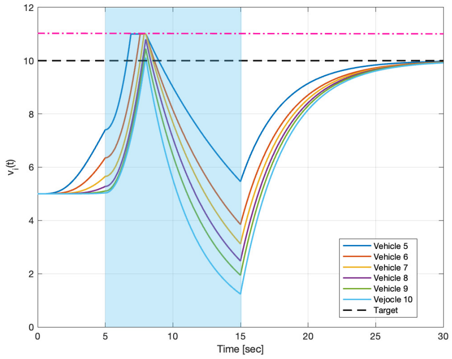

Fig. 4. Vehicles under attack, $i \geq 5$ (Velocity)

In Figs. 6-8, the positions time trend of the vehicle platoon and the relative truck distances are shown. At time $t = 14.4\,s$ the agent 5 detector unit (33) discovers the ongoing attack: as a consequence the feasible stored inputs $\hat{u}^5_k(10)$ are applied for the next 4 steps. At time $t = 14.9\,s$, the signal $\mathbf{D}_5(t)$ in (33) still reveals the `attack` value, the proposed scheme detaches the fifth and following vehicles from the formation for safety concerns and two separated formations are created: $LF^1 := 1, 2, 3, 4$ $LF^2 := 5, 6, 7, 8, 9, 10$ capable to separately accomplish the initial task.

VI. Conclusions

In this paper, resilience operations for constrained multi-agent systems subject to external intrusions are conceived

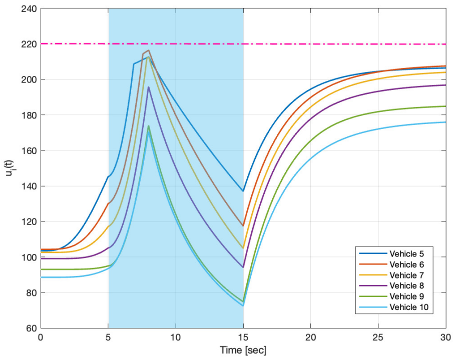

Fig. 5. Vehicles under attack, $i \geq 5$ (Control Input - Thrust)

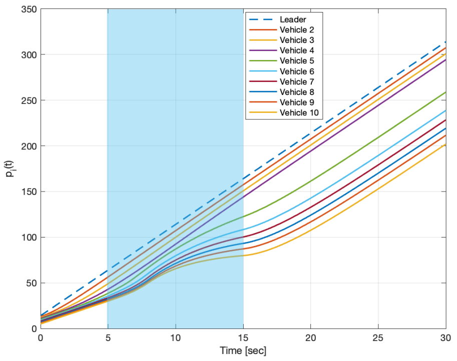

Fig. 6. Platoon position time trend (Σ^5 is under attack)

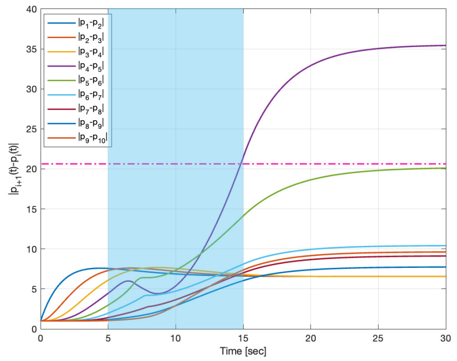

Fig. 7. Relative positions $|p_{i-1}(t) - p_i(t)|$, $i = 2, \ldots, 10$

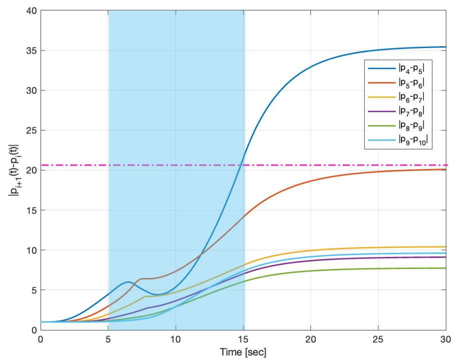

Fig. 8. Relative positions $|p_{i-1}(t) - p_i(t)|$, $i \geq 5$ (Splitted platoon)

by developing a distributed model predictive control architecture. In particular, the detection phase is designed by fully exploiting feasibility arguments proper of the receding horizon control philosophy that are translated into set-containment conditions simple to be on-line checked. Formal proofs on the capability of the proposed distributed detector to reveal the attack concurrence in finite time are provided together with feasibility and closed-loop stability of the DMPC scheme.

References

[1] Y. Lu, "Cyber physical system (CPS)-based industry 4.0: A survey", *J. of Indust. Integr. and Manag.*, Vol. 2, No. 03, 1750014, 2017.

[2] D. Zhang, G. Feng, Y. Shi and D. Srinivasan, "Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances", *IEEE/CAA JAS*,Vol. 8, No. 2, pp. 319-333, 2021.

[3] G. Franzè, W. Lucia, and V. Scordamaglia,"A distributed obstacle avoidance MPC strategy for leader-follower formations", *IFAC Proceedings,* Vol. , No. 3, pp. 2570-2575, 2014.

[4] G. Franzè, W. Lucia, and A. Venturino,"A distributed model predictive control strategy for constrained multi-vehicle systems moving in unknown environments", *IEEE Transactions on Intelligent Vehicles,* Vol. 6, No. 2, pp. 343-352, 2020.

[5] Z. Feng, G. Hu and G. Wen,"Distributed consensus tracking for multi-agent systems under two types of attacks", *International Journal of Robust and Nonlinear Control*, Vol. 26, No. 5, pp. 896-918, 2016.

[6] A. Gusrialdi, Z. Qu, and M. A. Simaan,"Competitive interaction design of cooperative systems against attacks", *IEEE Transactions on Automatic Control*, Vol. 63, No. 9, pp. 3159-3166, 2018.

[7] X. M. Li, Q. Zhou, P. Li, H. Li and R. Lu,"Event-triggered consensus control for multi-agent systems against false data-injection attacks", *IEEE Transactions on Cyb.*, Vol. 50, No. 5, pp. 1856-1866, 2019.

[8] M. Meng, G. Xiao and B. Li,"Adaptive consensus for heterogeneous multi-agent systems under sensor and actuator attacks", *Automatica*, Vol. 122, 109242, 2020.

[9] G. Franzè, F. Tedesco, and D. Famularo,"Resilience against replay attacks: A distributed model predictive control scheme for networked multi-agent systems.", *IEEE/CAA Journal of Automatica Sinica*, Vol. 8, No. 3, pp. 628-640, 2020.

[10] F. Tedesco, D. Famularo and G. Franzè,"A resilient control strategy for networked multi-agent systems subject to covert attacks", *Trans. of the Institute of Measurement and Contr.*, 01423312211021295, 2021.

[11] X. Huang, and J. Dong,"Reliable leader-to-follower formation control of multiagent systems under communication quantization and attacks", *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 50, No. 1, pp. 89-99, 2019.

[12] H. Rezaee, T. Parisini and M. M. Polycarpou,"Resiliency in dynamic leader-follower multiagent systems", *Automatica*, Vol. 125, 109384, 2021.

[13] R. Romagnoli, B.H Krogh, D. de Niz, A. D. Hristozov and B. Sinopoli,"Software Rejuvenation for Safe Operation of Cyber–Physical Systems in the Presence of Run-Time Cyberattacks", *IEEE Trans. on Contr. Sys. Tech.*, DOI: 10.1109/TCST.2023.3236470, 2023.

[14] M. Egerstedt and X. Hu, "Formation constrained multi-agent control", *IEEE Trans. on Rob. and Autom.*, Vol. 17, No. 6 pp., 947-951, 2001.

[15] G. Franzè, W. Lucia and A. Venturino,"A distributed model predictive control strategy for constrained multi-vehicle systems moving in unknown environments", *IEEE Transactions on Intelligent Vehicles*, Vol. 6, No. 12 pp. 343-352, 2021.

[16] A. Casavola, D. Famularo and G. Franzè, "Robust fault detection of uncertain linear systems via quasi-LMIs", *Automatica*, Vol. 44, No. 1, pp. 289-295, 2008.

[17] W. Feller, "An introduction to probability theory and its applications", Vol 2, *John Wiley & Sons*, 2008.

[18] D. Q. Mayne, "Control of constrained dynamic systems", *Eur. J. Control*, Vol. 7, pp. 87-99, 2001.

[19] E. Fridman and U. Shaked, "Delay-dependent H-infinity control of uncertain discrete delay systems", *European Journal of Control* , Vol. 11, pp. 29–37, 2005.

[20] S. Wen and G. Guo, "Control of Leader-Following Vehicle Platoons With Varied Communication Range", *IEEE Trans. on Intel. Vehicles*, Vol. 5, No. 2, pp. 240-250, DOI: 10.1109/TIV.2019.2955899, 2020.