Undetectable Finite-Time Covert Attack on Constrained Cyber-Physical Systems

Kian Gheitasi Walter Lucia

***Abstract*— In the last decades, several cyber-threats against Cyber-Physical Systems (CPSs) have been reported. Of particular interest are the classes of network attacks capable of affecting the control systems' performance while remaining undetectable. In this paper, under some conditions, we show the existence of a novel class of finite-time undetectable attacks against constrained CPSs. The proposed finite-time attack has the peculiar capability of not producing anomalies after its termination. This is particularly dangerous because it enables a malicious entity to repeatedly or intermittently affect the CPS without raising alarms. Such an attack is here designed by resorting to a set-theoretic approach that leverages robust reachability arguments. Moreover, given the desired attack duration, the set of initial states from which the attack is feasible is characterized. A numerical simulation example involving an industrial continuous-stirred tank reactor system is presented to support the theoretical results.**

I. Introduction

The appellation Cyber-Physical System (CPS) is used to denote engineering systems with a tight coupling between the physical and cyber components. Examples of CPSs can be found in different domains such as transportation systems, water distribution systems, and smart grids [1]. CPSs have the potential to improve traditional engineering systems in terms of efficiency, reliability, and performance. Nevertheless, improved capabilities come along with novel vulnerabilities to cyber-attacks targeting the cyber-infrastructures and communication channels. In this regard, the control community has been very active in studying the security, safety, and privacy issues associated with CPSs, see, e.g. [2]–[6], and references therein.

To design a secure and resilient CPS, it is particularly important to characterize and study such systems' vulnerability to different classes of cyber-attacks. In [7], and [8], an interesting three-dimensional attack classification is proposed to define the attacker's capabilities and stealthiness according to the available resources. In [9], the impact of partial state information on the detectability of deception attacks is studied.

Of particular relevance for this study are the classes of False Data Injection (FDI) attacks capable of affecting the control system performance while remaining stealthy (undetected). Well-known examples of undetectable attacks are zero-dynamics [10], [11], replay [12] and covert attacks [13]. In the classical definition, an attack is said stealthy if it is capable of remaining undetectable (according to the used detection strategy) during its actions. Starting from this definition, different *ad-hoc* active detection schemes have been proposed to reveal such attacks, see e.g. the watermarking solution in [14], the moving target in [15], [16], the blended approach in [6], the sensor coding in [17].

It is interesting to notice that in [18] it has been shown that replay and covert attacks can be straightforwardly detected by simple passive residual based detectors (e.g. a χ^2 detector) in the post-attack phase. From the defender perspective, the latter means that using a standard detection strategy, the system operator can a-posteriori understand that an anomaly has occurred and he/she can take proper countermeasures to avoid future occurrences. On the other hand, from the attacker's point of view, it implies that repetitive or intermittent deception attacks such as replay and covert attacks cannot remain undetectable.

An important question addressed in this paper is the existence of a class of finite-time attacks that are undetectable, with respect to passive anomaly detectors [19], both when the attack is ongoing and afterwards. Such a question is relevant in CPS applications where the attacker is interested to repeatedly or intermittently affect the CPS performance without ever being detected. For example, in a modern water-treatment facility [20], or a power system [21], a malicious entity might be interested in stealing water/energy repeatedly (whenever it is needed), for a finite amount of time, and without ever triggering an anomaly.

A. Contribution

To the best of the author's knowledge, the existence of finite-time stealthy attacks capable of avoiding detection in the post-attack phase has not been studied in the literature. In the preliminary work [18], the existence of such attacks has been investigated in an unconstrained setup. There, it has been proved that the covert attacks proposed in [13] can be appropriately modified to avoid detection in the post-attack phase. In this manuscript, we face a similar design problem but in a more challenging setup (for the attacker) where the plant is subject to bounded but unknown disturbances and state and input constraints. In particular, by resorting to a set-theoretic control framework [22] and robust controllability arguments for constrained systems, we show that, under

This work was supported in part by the Natural Sciences and Engineering Research Council of Canada under Grant RGPIN-2018-06713 and in part by the Fonds Québécois de la Recherche sur la Nature et les Technologies under Grant 2020-NC-268119.

Kian Gheitasi and Walter Lucia are with the Concordia Institute for Information Systems Engineering (CIISE), Concordia University, Montreal, QC, H3G 1M8, CANADA, k_gheita@encs.concordia.ca, walter.lucia@concordia.ca

proper conditions, a finite-time stealthy covert attack exists. Moreover, for a given attack duration and attack objective (e.g. state configuration to reach under attack), we characterize the subspace of states from which the proposed attack is guaranteed to be successful.

This paper is organized as follows: in section II, first, the considered CPS setup (plant, controller, anomaly detector, cyber-attack assets) is presented, then constrained finite-time covert attack design problem is formulated. In section III, The proposed finite-time attack is elaborated, designed and analyzed. Finally, a simulation example is illustrated in section IV to testify the proposed design's effectiveness.

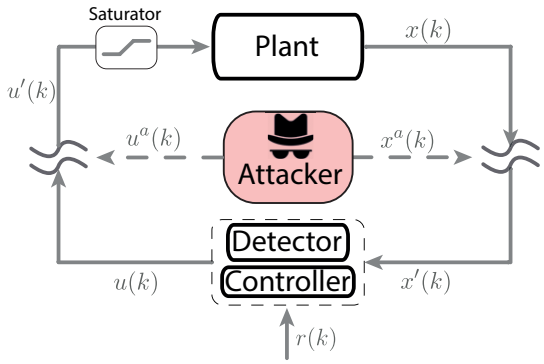


Fig. 1: Networked Control Architecture

II. Considered Setup and Problem Formulation

In this section, the assumed networked control system setup (Fig. 1) and the attack scenario are introduced.

A. Plant dynamics and constraints

Consider the following discrete-time linear system

$$x(k+1) = Ax(k) + Bu'(k) + B_d d(k) \tag{1}$$

where the index $k \in \mathbb{Z}_+ = \{0, 1, ...\}$ denotes discrete-time instants, $x(k) \in \mathbb{R}^n$ the vector of the states, $u'(k) \in \mathbb{R}^m$ the control input vector received by the plant, $d(k) \in \mathbb{R}^d$ a bounded unknown disturbance, and A, B and B_d are the system matrices with appropriate dimensions. The unknown disturbance $d(k)$ is such that

$$d(k) \in \mathcal{D} \subset \mathbb{R}^d, \quad 0_d \in \mathcal{D} \tag{2}$$

with $\mathcal{D}$ a compact set. The actuators' physical limitations impose the following saturation constraint on $u'(k)$

$$u'(k) \in \mathcal{U} \subset \mathbb{R}^m, \quad 0_m \in \mathcal{U} \tag{3}$$

with $\mathcal{U}$ a compact set, while the state are desired to be constrained into the set

$$x(k) \in \mathcal{X} \subset \mathbb{R}^n, \quad 0_n \in \mathcal{X} \tag{4}$$

where $\mathcal{X}$ is a compact set.

Assumption 1: We assume that the plant (1) is stabilizable.

Definition 1: A set $\Xi \subseteq \mathcal{X}$ is said to be a Robust Control Invariant (RCI) for (1)-(2) [22] if there exists a control law $u(k) := f(x(k))$ complying with (3)-(4) such that

$$\forall x \in \Xi \rightarrow Ax + Bf(x) + B_d d \in \Xi, \forall d \in \mathcal{D} \tag{5}$$

Definition 2: Given two sets $\mathcal{S}_1 \subset \mathbb{R}^{n_s}$ and $\mathcal{S}_2 \subset \mathbb{R}^{n_s}$, their Minkowski/Pontryagin set sum ($\oplus$) and difference ($\ominus$) are [23]:

$$\mathcal{S}_1 \oplus \mathcal{S}_2 := \{s_1 + s_2 | s_1 \in \mathcal{S}_1, s_2 \in \mathcal{S}_2\}$$
$$\mathcal{S}_1 \ominus \mathcal{S}_2 := \{s_1 \in \mathbb{R}^{n_s} | s_1 + s_2 \in \mathcal{S}_1, \forall s_2 \in \mathcal{S}_2\}$$

B. Controller

The networked controller is a tracking state-feedback controller designed to comply with the constraints (3)-(4) despite the disturbance realization (2). By denoting with $x_c(k) \in \mathbb{R}^{n_c}$ the state of the controller, its actions are generically described as

$$u(k) = f(x_c(k), x(k), r(k)) \tag{6}$$

where $r(k)$ is the desired reference signal and $f(\cdot, \cdot, \cdot)$ the control logic. In what follows, we assume that the control logic (6) is given and its Domain of Attraction (DoA) is $\mathcal{X}$.

C. Anomaly detector

A dynamic passive anomaly detector, leveraging the received state measurements $\{x'(k)\}$ and computed control inputs $\{u(k)\}$, is used to reveal anomalies/cyber-attacks, see [19] for a survey paper. Without loss of generality, the anomaly detection rule can be described as

$$\text{anomaly}(k) = \Phi(\{x'(t)\}_{t=0}^{k}, \{u(t)\}_{t=0}^{k-1}, \mathcal{D}) \tag{7}$$

where $\Phi(\cdot, \cdot, \cdot)$ is the binary attack detection logic. Moreover, $\text{anomaly}(k) = 1$ if an attack is detected, 0 otherwise.

D. Cyber-attack assets

The attacker is capable of corrupting the communication channels between the plant and the controller. In particular, the three-dimensional characterization of the attack is [8]:

- The attacker is aware of the plant model (1);
- The attacker can read the control signal $u(k)$ and the state measurement vector $x(k)$.
- The attacker can produce a deception attack to change the control signal ($u(k) \rightarrow u'(k) \in \mathbb{R}^m$) and state measurements ($x(k) \rightarrow x'(k) \in \mathbb{R}^n$) received by the plant and the networked controller, respectively.

Given the available resources, and a desired target state $x_d \in \mathbb{R}^n$, the attacker is able to compute (e.g., by resorting to the method described in [24]) an admissible small RCI target set $\mathcal{X}_d \subset \mathbb{R}^n$, centered in x_d.

E. Problem Formulation

In this paper, the existence and design of finite-time covert attacks, undetectable in the post-attack phase, are investigated. The problem of interest can be formulated as follows:

Undetectable Finite-Time Covert Attack (UFTCA): Consider the networked control system shown in Fig. 1, and the target RCI region $\mathcal{X}_d \subset \mathbb{R}^n$ centered in $x_d \in \mathbb{R}^n$. Design a finite-time deception attack of duration $\bar{T} \in \mathbb{Z}_+$, i.e.

$$\begin{gathered} u'(k) = u(k) + u^a(k), \quad x'(k) = x(k) + x^a(k) \\ \underline{k} \le k \le \bar{k}, \quad \bar{k} - \underline{k} = \bar{T} \end{gathered} \tag{8}$$

with $u^a(k) \in \mathbb{R}^m$ and $x^a(k) \in \mathbb{R}^n$ arbitrarily FDI vectors, such that:

- (O_1) The attack is capable of steering the state trajectory within the target set $\mathcal{X}_d$ for at least one time instant, i.e. $x(k) \in \mathcal{X}_d$, $\forall\, k \in [k_{in}, k_{out}]$, where $k_{in} \geq \underline{k}$, $k_{out} \leq \bar{k}$, and $k_{out} - k_{in} \geq 0$.
- (O_2) Regardless of the used dynamic detector (7), the attack does not trigger any alarm during its actions ($\underline{k} \leq k \leq \bar{k}$) and afterward ($k > \bar{k}$).

III. Finite-time stealthy covert attack

In this section, first the detectability in the post-attack phase of the covert attack, introduced in [13], is discussed. Then, the conditions under which the deception attack fulfills the *UFTCA* objectives are presented and the proposed attack is designed.

A. Basic Covert Attack

Under the presence of FDI attacks on the control signal (i.e. $u^a(k) \neq 0$), the system (1) evolves as:

$$x(k+1) = Ax(k) + B(u(k) + u^a(k)) + B_d d(k) \tag{9}$$

For linearity, it is possible to write

$$x(k) = x^u(k) + x^{u^a}(k) \tag{10}$$

where

$$x^u(k) = A^k x(0) + \sum_{j=0}^{k-1} A^j \left(Bu(k-1-j) + B_d d(k-1-j)\right) \tag{11}$$

$$x^{u^a}(k) = \sum_{j=0}^{k-1} A^j B u^a(k-1-j) \tag{12}$$

Notice that $x^u(k)$ denotes the state evolution of the system due to the initial condition, control input, and disturbance realization, while $x^{u^a}(k)$ is the state evolution of the system due to the presence of the input attack vector $u^a(k)$.

According to the covert attack introduced in [25], an attacker can arbitrarily affect the state trajectory (9) while remaining undetected by (7) if

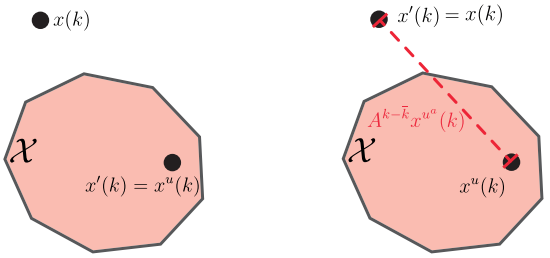
$$u'(k) = u^a(k) + u(k) \in \mathcal{U},\ \forall k \text{ s.t. } \underline{k} \leq k \leq \bar{k} - 1 \tag{13}$$

$$x^a(k) = -x^{u^a}(k),\ \forall k \text{ s.t. } \underline{k} + 1 \leq k \leq \bar{k} \tag{14}$$

***Remark** 1:* The above attack is, by construction, undetectable for $\underline{k} \leq k \leq \bar{k}$ irrespective of Φ used in (7) [13]. Visually, by referring to Fig. 2a, regardless of $u^a(k) \neq 0$, the system state received by the controller is always equal to the expected one, i.e. $x'(k) = x^u(k)$, $\forall\, \underline{k} \leq k \leq \bar{k}$.
On the other hand, when the covert attack is terminated (i.e., $k > \bar{k}$) we have that

$$\begin{aligned} x(k) &= x^u(k) + A^{k-\bar{k}} x^{u^a}(\bar{k}) \\ x'(k) &= x(k), \qquad\qquad k > \bar{k} \end{aligned}$$

Therefore, if $x^{u^a}(\bar{k}) \neq 0_n$, then for some $k > \bar{k}$, $x'(k) \neq x^u(k)$ and such discrepancy can be leveraged by (7) to detect an anomaly (see Fig. 2b). Finally, attack stealthiness in the post-attack phase (i.e., $\forall\, k > \bar{k}$) is guaranteed irrespectively of the detector logic and any disturbance realization if $x^{u^a}(\bar{k}) = 0_n$. □



(a) $\underline{k} \leq k \leq \bar{k}$ (b) $k > \bar{k}$

Fig. 2: State mismatch during and after the attack.

B. UFTCA design

In this section, we design a finite-time covert attack fulfilling the objectives (O_1)-(O_2) stated in the *UFTCA* problem formulation.

First, the challenges of such a design are highlighted:

1) The attack must determine a control sequence $\{u^a(k)\}_{k=\underline{k}}^{\bar{k}-1}$ where $\exists\, k \in [\underline{k}, \bar{k})$ such that the state trajectory enters the desired RCI region $\mathcal{X}_d$ for at least one time instant. Moreover, the control actions must fulfill the input saturation constraint (3) and be robust against any admissible disturbance realization (2) and controller (6) actions.
2) The attacker, to avoid any possibility of post-attack detection, must make sure that $x^{u^a}(\bar{k}) = 0_n$ (see the analysis in Remark 1). Such an objective must be robust against disturbance realization (2) and controller (6) actions.
3) Given a finite amount of time $\bar{T}$, the attacker must be able to determine (before starting the attack), the set of initial state conditions $\mathcal{X}_a \subseteq \mathcal{X}$, from which the attack is guaranteed to succeed.

Given the constrained and uncertain nature of the above problem, here we provide a solution, based on a robust set-theoretic model predictive control (ST-MPC) paradigm [22], [26], [27]. Please note that other MPC paradigms or constrained control strategies can, in principle, be used instead of ST-MPC. Such a choice is mainly motivated by the fact that ST-MPC will allow to offline define the controller's domain of attraction (union of robust one-step controllable sets) and the worst-case number of steps required to robustly reach the attacker's objectives.

By resorting to a *divide et impera* approach, the UFTCA design problem is divided in two phases (see Fig. 3). In the first phase, a covert attack is designed to ensure that $\forall\, x(k) \in \mathcal{X}$, there exists a sequence of attack actions $\{u^a(k)\}$ such that the state trajectory is driven within $\mathcal{X}_d$. In the second phase, an attack deletion strategy is designed to ensure that $x^{u^a}(\bar{k}) = 0_n$.

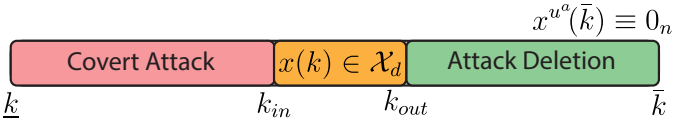


Fig. 3: Finite-time attack: phases and actions.

*1) **Phase I - reaching** $\mathcal{X}_d$:* In this phase, the attack control input $u^a(k)$ is designed to replace $u(k)$ and robustly steer the plant's trajectory into the desired RCI region $\mathcal{X}_d$.

By resorting to the ST-MPC paradigm such a problem can be solved in finite-time as follows:

Offline attack preparation

By considering $\mathcal{X}_d$ as the terminal RCI region (target set) of the attacker, a family of robust one-step controllable sets $\{\mathcal{T}_d^i\}_{i=0}^{N_d}$, $N_d \geq 0$ is computed according to the following recursive definition:

$$\begin{array}{rcl} \mathcal{T}_d^0 & := & \mathcal{X}_d \\ \mathcal{T}_d^i & := & \{x \in \mathbb{R}^n : \exists u^d \in \mathcal{U} \; s.t. \; Ax + Bu^d \in \tilde{\mathcal{T}}_d^{i-1}\}, \; i > 0 \end{array} \tag{15}$$

where $\tilde{\mathcal{T}}_d^i = \mathcal{T}_d^i \ominus B_d\mathcal{D}$, and $u^d \in \mathcal{U}$ is the control input desired by the attacker. Such a recursion is terminated when the union of controllable sets covers the admissible state space region $\mathcal{X}$, i.e.

$$\mathcal{X} \subseteq \bigcup_{i=0}^{N_d} \mathcal{T}_d^i \tag{16}$$

***Remark** 2:* Please note that efficient tools and toolboxes exist to compute exact or approximated robust one-step controllable sets (15) for linear systems, see e.g. [22], [23], [27]–[30] and references therein. □

Attack actions ($\underline{k} \leq k \leq k_{out}$):

By taking advantage of the offline computations, the attacker's actions on the actuation channels reduce to the solution of a simple Quadratic Programming (QP) optimization problem forcing (at each step), the state trajectory to evolve within the family of controllable sets $\{\mathcal{T}_d^i\}_{i=0}^{N_d}$, until the terminal region $\mathcal{T}_d^0 \equiv \mathcal{X}_d$ is reached, i.e.

$$\textit{if } x(k) \in \mathcal{T}_d^i \textit{ compute } u^d(k) \in \mathcal{U} \textit{ s.t. } x(k+1) \in \mathcal{T}_d^{i-1} \tag{17}$$

As a consequence, the following FDI attack is performed to replace $u(k)$ with $u^d(k)$, i.e.,

$$u^a(k) = u^d(k) - u(k) \rightarrow u'(k) = u^d(k) \tag{18}$$

On the other hand, on the measurement channel, to avoid detection, the covert FDI in (14) is used.
The attacker's actions are summarized in the following algorithm:

Algorithm 1: Phase I (covert attack) - attacker's algorithm $\underline{k} < k \leq k_{out}$

Offline: Compute $\{\mathcal{T}_d^i\}_{i=0}^{N_d}$ as in (15)-(16)
Online: Compute $u^a(k), x^a(k)$ as follows:

1: Find the smallest set index $0 \leq i \leq N_d$ containing $x(k)$:

$$i(k) := \min_{0 \leq i \leq N_d} i : \; x(k) \in \mathcal{T}_d^i \tag{19}$$

2: **if** $i(k) == 0$ **then** $\mathcal{T}_d^{next} = \mathcal{T}_d^{i(k)}$
3: **else** $\mathcal{T}_d^{next} = \mathcal{T}_d^{i(k)-1}$
4: **end if**
5: Compute $u^d(k)$ solving the QP problem

$$u^d(k) = \arg\min_{u^d} \|Ax(k) + Bu^d - x_d\|_2^2 \quad s.t. \tag{20}$$

$$Ax(k) + Bu^d \in \tilde{\mathcal{T}}_d^{next}, \; u^d \in \mathcal{U} \tag{21}$$

6: Determine $u^a(k)$ and $x^a(k)$ as in (18) and (14)

Lemma 1: If the Phase I duration is greater or equal than N_d, i.e. $k_{out} - \underline{k} \geq N_d$, then Algorithm 1 ensures that the attack complies with the objective (O_1) regardless of any admissible disturbance realization (2). Moreover, $k_{in} \leq \underline{k} + N_d$, and $x(k) \in \mathcal{X}_d, \forall \, k_{in} \leq k \leq k_{out}$.

Proof - By construction, the QP optimization problem (20) is guaranteed to admit a solution $\forall \, k$ [27]. Moreover, if $x(k) \in \mathcal{T}_d^{i(k)}$ then $Ax(k) + Bu^d \in \tilde{\mathcal{T}}_d^{i(k)-1}$ and $x(k+1) \in \mathcal{T}_d^{i(k)-1}$. As a consequence, regardless of any initial condition $x(\underline{k}) \in \mathcal{X}$, the set-membership index $i(k)$ has a monotonically decreasing behaviour until $i(k) = 0$ is reached. When $i(k) = 0$, then the attacker's control inputs aim to keep $x(k)$ into the RCI set $\mathcal{X}_d$. Therefore, Algorithm 1 ensures that in the worst-case scenario $x(\underline{k} + N_d) \in \mathcal{T}_d^0 = \mathcal{X}_d$, $x(k) \in \mathcal{X}_d$, $\forall k_{in} \leq k \leq k_{out}$, where $k_{in} \leq \underline{k} + N_d$. □

***Remark** 3:* In the worst-case scenario, N_d time steps are needed to fulfill the requirements of Phase I (see Lemma 1). As a consequence, the duration of Phase I should be greater or equal to N_d. □

*2) **Phase II - attack deletion** ($x^{u^a}(\bar{k}) = 0_n$):* In phase II, the attacker, after achieving its primary objective (e.g., $x(k) \in \mathcal{X}_d$), wants to remove any trace of its presence to avoid detection in the post-attack phase. Specifically, as discussed in Remark 1, no passive anomaly detector (7) can discover anomalies in the post-attack phase if $x^{u^a} = 0_n, \forall \, k \geq \bar{k}$. Therefore, the attacker's action $u^a(k)$ for $k_{out} < k \leq \bar{k}$ must be devoted to ensure that the state evolution due to the attacker actions (x^{u^a}) vanishes in a finite number of steps. Different from Phase I, where the attacker's actions aimed to replace $u(k)$ with $u^d(k)$ (see(18)), here the attacker wants to control only x^{u^a}. As a consequence, while removing x^{u^a} the attacker must make sure that the signal $u'(k) = u(k) + u^a(k)$ is admissible, i.e. $u'(k) \in \mathcal{U}$, regardless of the controller input $u(k)$ computed by (6).

Assumption 2: There exists a small convex compact set $\Delta \subset \mathbb{R}^n$, $0_n \in \Delta$, s.t. such that

$$u(k) \oplus \Delta \subseteq \mathcal{U}, \; \forall \, k \tag{22}$$

***Remark** 4:* Note that such an assumption assumes that the control action $u(k)$ computed by (6) are contained into a proper inner set of $\mathcal{U}$. Such an assumption is reasonable in uncertain constrained setups where the controller actions are typically mapped into a smaller input set to ensure constraint satisfaction despite any disturbance realization (2) [31], [32]. Moreover, it is also fulfilled when the state trajectory is in proximity of the equilibrium state [31]. □

In what follows, Assumption 2 is instrumental to ensure that the attack deletion problem has a guaranteed solution in a finite number of steps. Then, in Remark 5, such an assumption is relaxed, and other conditions under which the attack deletion problem can be accomplished are investigated.

Offline attack deletion preparation

Lemma 2: Consider the attacker's desired region $\mathcal{X}_d$, the Phase I attacker's algorithm, and $k_{out} \geq \underline{k} + N_d$. Then, regardless of any admissible disturbance (2) realization

$$x^{u^a}(k_{out}) \in (\mathcal{X}_d \oplus -\mathcal{X}) := \mathcal{X}^{u^a} \tag{23}$$

Proof - According to (10), we have that

$$x^{u^a}(k_{out}) = x(k_{out}) - x^u(k_{out}) \tag{24}$$

Moreover, by noticing that if $k_{out} \geq \underline{k} + N_d$ then $x(k_{out}) \in \mathcal{T}_d^0 \equiv \mathcal{X}_d$ and that $x^u(k_{out}) \in \mathcal{X}$, we have that (23) holds true, concluding the proof. □

By considering $x^{u^a}(\bar{k}) = 0_n$ as the target state and $\mathcal{X}^{u^a}$ as the initial admissible set for $x^{u^a}(k_{out})$, a family of robust one-step controllable sets in the attacker's state space x^{u^a}, namely $\{\mathcal{T}_a^j\}_{j=0}^{N_a}, N_a > 0$, is built considering $u^a(k) \in \Delta$ as the attacker's worst-case input constraint set, i.e.,

$$\begin{aligned} &\mathcal{T}_a^0 := 0_n \\ &\mathcal{T}_a^j := \{x^{u^a} \in \mathbb{R}^n : \exists u^a \in \Delta \; s.t. \; Ax^{u^a} + Bu^a \in \mathcal{T}_a^{j-1}\}, \; j > 0 \end{aligned} \tag{25}$$

Such a recursion is terminated when the admissible set of initial states $x^{u^a}(k_{out})$ is covered, i.e.,

$$\mathcal{X}^{u^a} \subseteq \bigcup_{i=0}^{N_a} \mathcal{T}_a^j \tag{26}$$

Lemma 3: Under Assumption 2, if there exist a family of robust one-step controllable sets $\{\mathcal{T}_a^j\}_{j=0}^{N_a}$, built as in (25) and satisfying (26), then there exists a sequence of control inputs $\{u^a(k)\}_{k=k_{out}+1}^{\bar{k}-1}$ such that $x^{u^a}(\bar{k}) = 0_n$ and $u'(k) = u(k) + u^a(k) \in \mathcal{U}, \forall \, k_{out} < k \leq \bar{k} - 1$

Proof - By construction, recursion (25) ensures that at each time steps there exists $u^a(k) \in \Delta$ such that the one-step evolution $x^{u^a}(k+1)$ belongs to a controllable set whose index is strictly lower than the current one, e.g. if $x^{u^a}(k) \in \mathcal{T}_a^j$, $j > 0 \rightarrow x^{u^a}(k+1) \in \mathcal{T}_a^{j-1}$. Therefore, recursively, we have that $x^{u^a}(\bar{k}) \in \mathcal{T}_a^0 = 0_n$. Moreover, according to Assumption 2, we are guaranteed that $u'(k) \in \mathcal{U}, \forall \, k_{out} < k \leq \bar{k} - 1$. □

Attack deletion ($k_{out} < k \leq \bar{k}$)

Similarly to what is done by the attacker in Phase I, in Phase II, the attacker's actions $u^a(k)$ and $x^a(k)$ are computed according to the following algorithm:

Algorithm 2: Phase II (attack deletion) - attacker's algorithm $k_{out} < k \leq \bar{k}$

Offline: Compute $\{\mathcal{T}_a^j\}_{k=0}^{N_a}$ as in (25)-(26)
Online: Compute $u^a(k), x^a(k)$ as follows:

1: Find the smallest set index $0 \leq j \leq N_d$ containing $x(k)$:

$$j(k) := \min_{0 \leq j \leq N_a} j : x(k) \in \mathcal{T}_a^j \tag{27}$$

2: **if** $j(k) == 0$ **then** $u^a(k) = 0_m$
3: **else**
4: Compute $u^a(k)$ solving the QP problem

$$u^a(k) = \arg\min_{u^a} \|Ax^{u^a}(k) + Bu^a\|_2^2 \quad s.t. \tag{28}$$

$$Ax^{u^a}(k) + Bu^a \in \mathcal{T}_a^{j(k)-1} \tag{29}$$

$$u^a \in \mathcal{U} - u(k) \tag{30}$$

5: **end if**
6: Determine $x^a(k)$ as in (14)

Lemma 4: If the Phase II duration is greater than N_a, i.e. $\bar{k} - k_{out} > N_a$, then Algorithm 2 ensures that the attack is not detectable for $k \geq \bar{k}$, regardless of any admissible disturbance (2) realization.

Proof - First, under Assumption 2, it is guaranteed that $\Delta \subseteq (\mathcal{U} - u(k)), \forall \, u(k)$. Moreover, by following the same reasoning used in Lemma 1, if $\bar{k} - k_{out} > N_a$ then the monotonically decreasing set-membership index $j(k)$ is guaranteed to be zero for $k = \bar{k}$. Therefore, since $\mathcal{T}_a^0 = 0_n$, we have that $\forall \, k \geq \bar{k}$, the contribution of the attack on the state of the system will be zero and detection in the post-attack phase is avoided. □

C. Proposed finite-time attack: feasibility, undetectability and possible extension

In the following propositions, the properties of the finite-time attack developed in subsection III-B are investigated.

Proposition 1: Consider the constrained plant model (1)-(4) and the anomaly detector (7). If, for a given target RCI set $\mathcal{X}_d$, there exist $0 \leq N_d < \infty$ such that (15) satisfies (16), $0 \leq N_a < \infty$ such that (25) complies with (26), and $\Delta \neq \emptyset$ in (22). Then, Algorithm 1 and Algorithm 2 ensure that:

- *the finite-time covert attack (Phase I + Phase II) fulfills the objectives (O1)-(O2), i.e. $\exists k : x(k) \in \mathcal{X}_d$ and the attack is undetectable by (7) for $k > \underline{k}$.*
- *irrespective of any admissible initial plant condition $x(\underline{k}) \in \mathcal{X}$ and bounded disturbance realization $d(k) \in \mathcal{D}$, the minimum attack duration $\bar{T}$ to fulfill (O1)-(O2) is $\bar{T} = N_d + N_a$.*

Proof - By collecting the results in Lemmas 1-4, Algorithm 1 ensures undetectability for $\underline{k} \leq k \leq k_{out}$ and that $x(k) \in \mathcal{X}_d$ for $k_{in} \leq k \leq k_{out}$. Moreover, Algorithm 2 guarantees that the post-attack undetectability condition $x^{u^a}(\bar{k}) = 0_n$ is reached for $k \geq k_{out} + N_a$. Therefore, the minimum finite-time attack duration that ensures fulfilling (O_1)-(O_2) regardless of $x(\underline{k}) \in \mathcal{X}$ is obtained for $k_{out} = k_{in}$ and $\bar{T} = N_d + N_a$. □

Proposition 1 implies that if the attack duration, namely $\bar{T}$, is bigger or equal to $N_a + N_d$, then the proposed finite-time covert-attack is feasible starting from any $x(k) \in \mathcal{X}$. In the next proposition, this is formalized, and it is also shown that for $\bar{T} < N_a + N_d$, the attack might still be feasible starting from a subset of $\mathcal{X}$.

Proposition 2: Given a desired attack duration $\bar{T}$, the set of initial state condition $\mathcal{X}_a \subseteq \mathcal{X}$, $x(\underline{k}) \in \mathcal{X}_a$ such that finite-time attack (Algorithm 1-2) can be successfully completed in $\bar{T}$-steps can be offline determined and it is equal to:

$$\mathcal{X}_a = \left(\bigcup_{i=0}^{\min(\bar{T} - N_a, N_d)} \mathcal{T}_d^i \right) \bigcap \mathcal{X} \tag{31}$$

Proof - First, it is important to underline that regardless of the initial state condition, the attack duration cannot be lower than N_a (number of steps required to cancel out the presence of the attack in Phase II). Therefore, the number of steps available to

the attacker to steer $x(\underline{k})$ into $\mathcal{X}_d$ is $\bar{T}-N_a$. As a consequence, since $\mathcal{X} \subseteq \bigcup_{i=0}^{N_d} \mathcal{T}_d^i$, if $\bar{T} \geq N_d+N_a$, then $\min(\bar{T}-N_a, N_d) = N_d$ and the set of admissible initial condition is equal to entire set of admissible states, i.e. $\mathcal{X}_a = \mathcal{X}$. On the other hand, if $\bar{T} < N_a+N_d$, then $\min(\bar{T}-N_a, N_d) = \bar{T}-N_a$ and $\mathcal{X}_a \subset \mathcal{X}$, see Fig. 4 for an illustration. □

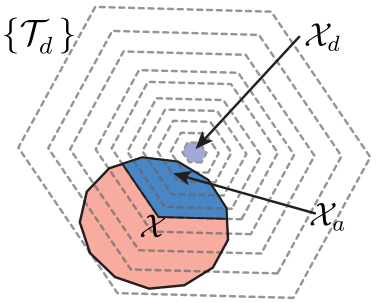


Fig. 4: The state subspace $\mathcal{X}_a \subseteq \mathcal{X}$ (blue region) from which the attack can successfully perform the finite-time attack for $\bar{T} < N_d + N_a$.

***Remark** 5:* The finite-time attack is guaranteed to exist under Assumption 2, i.e. $\Delta \neq \emptyset$, $\forall\, k_{out} < k \leq \bar{k}$. However, it is important to underline that this is only a sufficient condition and that the attack might be feasible otherwise. For the sake of completeness and to open the floor to further research directions, three different situations can be analyzed:

- Consider the case where $\Delta = \emptyset$ and A is Nilpotent with index N, i.e., $A^N = 0_{n\times n}$. In this case, since $x^{u^a}(k) = \sum_{j=0}^{k-1} A^j B^j u^a(k-1-j)$, then, regardless of the initial attack state $x^{u^a}(k_{out})$, $x^{u^a}(k_{out}+N) = 0_n$ if $u^a(k) = 0_m, \forall\, k \geq k_{out}$. Therefore, in Phase II, the attacker does not need to take any actions on the actuation channel to ensure that $x^{u^a}(k)$ converges to zero in N-steps (see (12)). In particular for $k_{out} < k \leq \bar{k}$, $\bar{k} - k_{out} > N$, the attacker can use Algorithm 2 where in Step 4 the optimization problem (28)-(30) is replaced by $u^a(k) = 0_m$.
- Consider the case where $\Delta = \emptyset$ and the matrix A is Schur stable, i.e., its eigenvalues have modulus less than 1. In this case, in Step 4 of Algorithm 2, the attacker can evaluate if the optimization problem (28)-(30) admits a solution for the input constraint $u^a(k) \in \mathcal{U} - u(k)$. If such a problem does not admit a solution then the attacker can apply $u^a(k) = 0_m$, and exploit the contracting nature of A. In such a circumstances, the attack is guaranteed to end when the optimization problem (28) admits a solution for at-most N_a time steps. However, in this case it is not possible to offline determine the number of steps needed to complete Phase II.
- Consider the case where $\Delta = \emptyset$ and the matrix A is unstable. In this case, it is not possible to guarantee that the attack can terminate in a finite-amount of time. Furthermore, x^{u^a} is not guaranteed to remain inside $\bigcup_{j=0}^{N_a}\{\mathcal{T}_a^j\}$ and the recursive feasibility of Algorithm 2 is not ensured. □

***Remark** 6:* The proposed finite-time attack has been designed under the assumption that the entire state vector can be measured. Nevertheless, such an attack can be also designed to deal with a plant model (1) characterized by an output equation $y(k) = Cx(k) + d_y(k)$, where $C \in \mathbb{R}^{p\times n}$, $y(k) \in \mathbb{R}^p$ is the sensor measurement vector, and $d_y(k) \in \mathcal{D}_y \subset \mathbb{R}^p$ is a compact but unknown measurement disturbance set containing the origin. In general, if $C \neq I$, the extension is possible if (i) a state-estimator capable of dealing with bounded process and measurement disturbances can be designed, (ii) the worst-case state-estimation error can be characterized. The first is needed to reconstruct $x(k)$, while the second is important to properly build a family of robust one-step controllable sets (see e.g. (15)) that takes into account the bounded errors introduced by the estimator. Please refer to, e.g., [22, Chapter 11] and reference therein, for exhaustive details on the design of state estimators fulfilling the requirements (i)-(ii). On the other hand, a straightforward extension can be provided if $C = I$ (i.e., the entire state vector can be measured with a bounded error). Note that in this particular case, if $y(k)$ is measured, then $x(k)$ is also known with some uncertainty, i.e., $x(k) \in y(k) \oplus (-\mathcal{D}_y)$. Therefore, such extra uncertainty can be then taken into account in the construction of the robust one-step controllable sets (15) by simply computing $\tilde{\mathcal{T}}_d^i = \mathcal{T}_d^i \ominus (B_d\mathcal{D} \oplus (-A\mathcal{D}_y))$, see [33]. □

IV. Simulation Example

In this section, the industrial Continuous-Stirred Tank Reactor (CSTR) system used in [34] and shown in Fig. 5 has been considered to show in simulation the effectiveness of the proposed constrained finite-time attack.

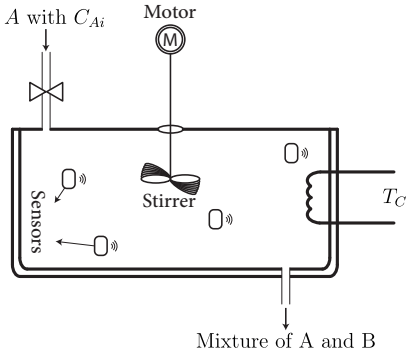


Fig. 5: Continuous-Stirred Tank Reactor (CSTR) system

In this system, the chemical species $\mathcal{A}$ react with the chemical species $\mathcal{B}$ at a specific temperature. The output of the system is a mixture of these two chemicals (see Fig. 5). The state vector of the CSTR system is $x = [C_{\mathcal{A}}, T_r]^T$ where $C_{\mathcal{A}}$ is the concentration of the chemical species $\mathcal{A}$, and T_r is the reaction temperature. On the other hand, $u = [T_C, C_{\mathcal{A}i}]^T$ is the control vector where T_C is the cooling controlled temperature and $C_{\mathcal{A}i}$ is the input concentration of the chemical species $\mathcal{A}$. The linearized discrete-time model of CSTR, for a sampling time $T_s = 1$, is characterized by the following system matrices

[34]:

$$A=\begin{bmatrix} 0.9719 & -0.0013 \\ -0.0340 & 0.8628 \end{bmatrix}, B=\begin{bmatrix} -0.0839 & 0.0232 \\ 0.0761 & 0.4144 \end{bmatrix}$$
$$B_d = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{32}$$

The admissible disturbance set is

$$\mathcal{D} = \{d \in \mathbb{R}^2 : \begin{bmatrix} -0.01 \\ -0.08 \end{bmatrix} \leq d \leq \begin{bmatrix} 0.01 \\ 0.08 \end{bmatrix}\} \tag{33}$$

and the states and inputs are subject to the following constraint sets:

$$\begin{aligned} \mathcal{X} &= \{[C_A, T_r]^T \in \mathbb{R}^2 : -2 \leq C_A \leq 2, -10 \leq T_r \leq 10\} \\ \mathcal{U} &= \{[T_C, C_{Ai}]^T \in \mathbb{R}^2 : -2 \leq T_C \leq 2, -2 \leq C_{Ai} \leq 2\} \end{aligned} \tag{34}$$

The controller (6) is a stabilizing state-feedback controller $u(k) = -K(x - r(k)) + u_{eq}(k)$, with u_{eq} the equilibrium input associated to the desired equilibrium state $x_{eq} = r(k)$, and K (the controller gain) is:

$$K = \begin{bmatrix} -10.903 & 0.560 \\ 1.921 & 1.978 \end{bmatrix} \tag{35}$$

Moreover, the used set Δ is:

$$\Delta = \{[T_C, C_{Ai}]^T \in \mathbb{R}^2 : -0.5 \leq T_C \leq 0.5, -0.5 \leq C_{Ai} \leq 0.5\} \tag{36}$$

The finite-time attack is offline configured as follows. The attacker wants to steer the state of the system in the proximity of the equilibrium pair (x_d, u_d), where $x_d = [-2.5, 0]^T$ and $u_d = [0.74, -0.34]^T$ Please note that the equilibrium state is outside of the admissible safe region $\mathcal{X}$. Moreover, the desired RCI region $\mathcal{X}_d$, centered in x_d, is computed as in [24] (see the blue region in Fig. 7). Then, the attacker builds the families of robust one-step controllable sets $\{\mathcal{T}_d^i\}_{i=0}^{N_d}$ (see Fig. 7) and $\{\mathcal{T}_a^j\}_{j=0}^{N_a}$ (see Fig. 8) as in (15) and (25), respectively. In particular, the terminal conditions (16) and (26) are reached for $N_d = 28$ and $N_a = 47$. As a consequence, the minimum number of steps required to complete the attack for any $x(\underline{k}) \in \mathcal{X}$ is $N_d + N_a = 75$ (see Proposition 1 and Fig. 8). Please note that by exploiting the result in Proposition 2, given a finite duration $\bar{T}$, the attacker is able to offline determine the sets of states $\mathcal{X}_a \subseteq \mathcal{X}$ from where the attack can be successfully completed. In Fig. 8, $\mathcal{X}_a$ is shown for $\bar{T}$ equals to 60, 70 and 75.

In the carried out simulation, the attacker launches for two times the finite-time covert attack described by Algorithm 1 and 2. The details of the attacks, i.e. $\underline{k}$, $k_{in}, k_{out}, \bar{k}$ are shown in Table I. The plant initial condition is $x(0) = 0_2$, and $r(k)$ is shown in Fig. 6.

TABLE I: Finite-time covert attacks timing information

	first attack	second attack
$\underline{k}$	31 s	200 s
k_{in}	53 s	223 s
k_{out}	59 s	234 s
$\bar{k}$	72 s	245 s

Fig. 6 shows the evolution over time for the two components of $r(k)$, $x(k)$ and $x'(k)$. It is possible to notice that during the two attacks $x(k)$ deviates significantly from $r(k)$ causing a constraint violation for $31 \leq k \leq 72$ and $200 \leq k \leq 245$. On the other hand $x'(k)$ (i.e. the signal received by the controller and detector) is unaffected by the presence of the attack. Moreover, the difference between $x'(k)$, and $x(k)$, i.e. the attack's state $x^{u^a}(k)$ becomes exactly zero when each attack is terminated at $k = 72$ and $k = 245$, respectively. As a consequence, the designed attack can be repeatedly executed avoiding detection during the attack and afterwards. To better appreciate the *modus operandi* of the attack, Fig. 7 and Fig. 8 show the state trajectory of the plant $(x(k))$ and attacker $(x^{u^a}(k))$. In Fig. 7, the state trajectory has been divided in four different colors to better highlight the phases of the two attacks. Regardless of the state $x(\underline{k})$, it is possible to notice that the attacker is capable of steering the trajectory in the RCI region $\mathcal{X}_d$. In particular, as shown in Table I, for the first and second attack, the RCI region is reached in 12 and 23 steps, respectively. Moreover, as better shown in Fig. 8, in Phase II, regardless of $x^{u^a}(k_{out}) \in \mathcal{X}_d \oplus (-\mathcal{X})$, the attack termination condition $x^{u^a} = 0_2$ is reached in a finite number of steps. Moreover, the time required for the attacker to completely execute attack 1 and 2 (i.e. $\bar{k} - \underline{k}$) is equal to $41s$ and $45s$, respectively. Such a duration is lower of the worst-case execution time of $75s$ that can be offline predicted by the attacker using (31), see e.g. $\mathcal{X}_a$ in Fig. 7. Finally, in Fig. 9, the control signal $u(k)$, $u'(k)$ and $u^a(k)$ are shown. It is possible to appreciate that the attacker's input vector $u^a(k)$ always ensures that the control signal received by the plant, i.e $u'(k)$, complies with the input constraints.

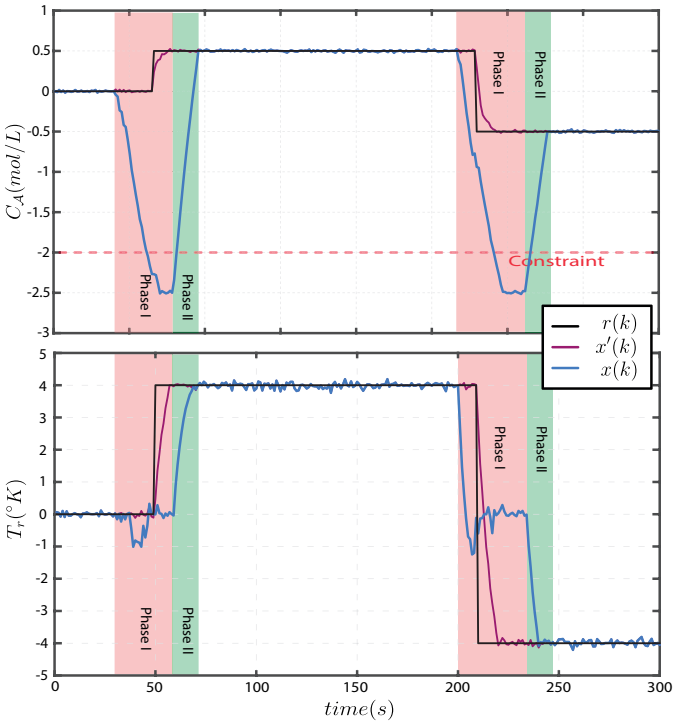


Fig. 6: CSTR Plants states evolution in the presence of the finite-time covert attack

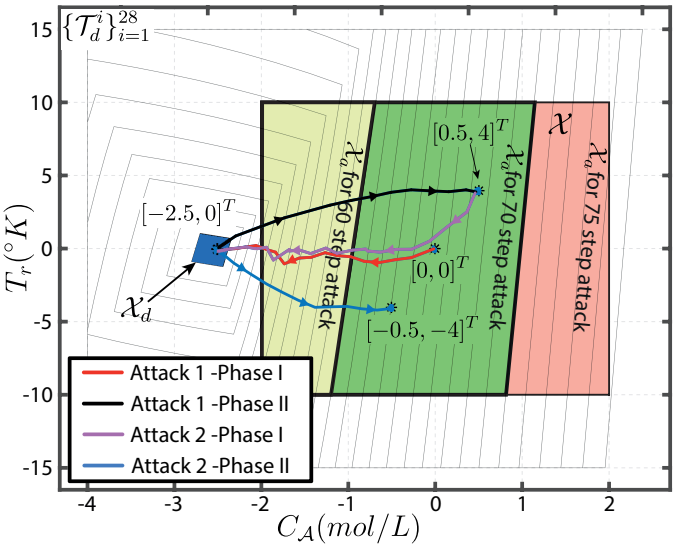


Fig. 7: Plants state trajectory ($x(k)$) and family of robust one-step controllable sets $\{\mathcal{T}_d^i\}_{i=0}^{25}$. The yellow, green and pink regions inside $\mathcal{X}$ depict the set of initial states $x(\underline{k}) \in \mathcal{X}_a \subseteq \mathcal{X}$ for which the constrained finite-time attack can be completed if $\bar{T} = 60$ (yellow region), $\bar{T} = 70$ (yellow + green regions) and $\bar{T} = 75$ (yellow + green + pink regions).

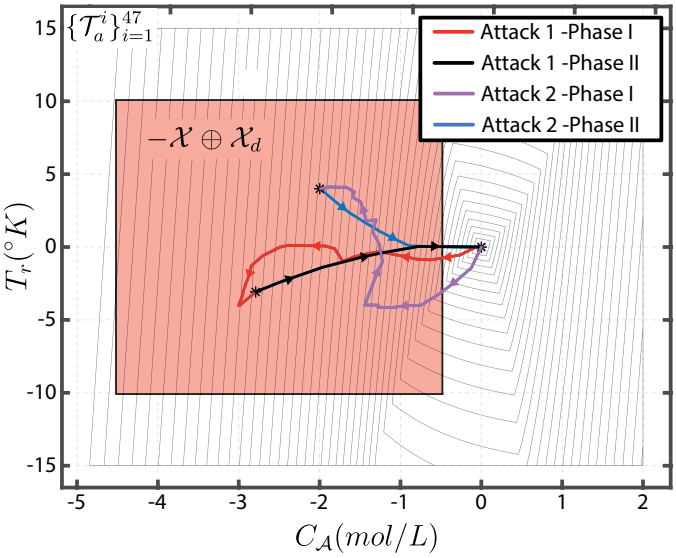


Fig. 8: Attacker's state trajectory (x^{u^a}) and family of robust one-step controllable sets $\{\mathcal{T}_a^i\}_{i=0}^{47}$.

V. Conclusion

In this paper, we have shown the existence of finite-time attacks against constrained CPS. The proposed finite-time covert attack has been designed by jointly combining robust controllability arguments and a set-theoretic-based receding horizon control paradigm. It has been formally proved that the designed attack is stealthy regardless of any anomaly detector deployed on the controller side of the networked CPS. Furthermore, under proper feasibility conditions, it has been proved that such an attack terminates in a finite number of steps and that the worst-case execution time, as well as the set of admissible initial states, can be offline determined.

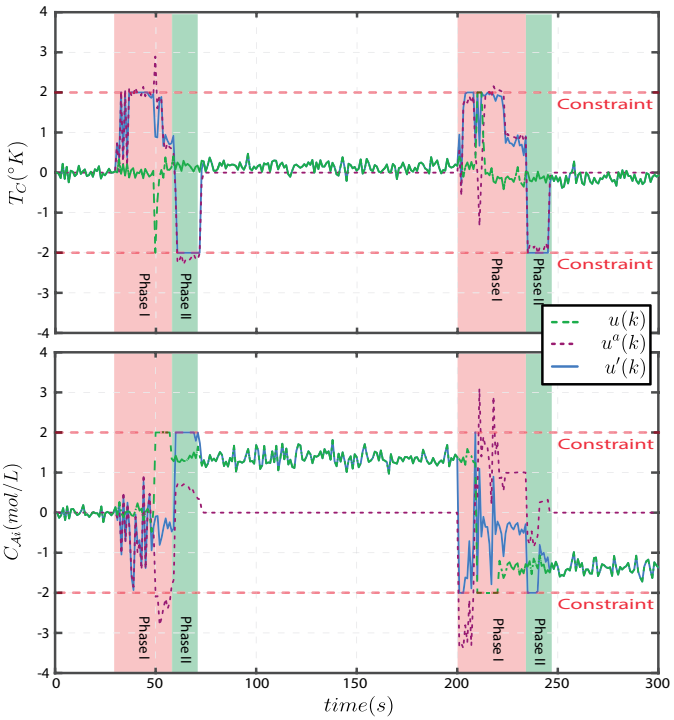


Fig. 9: Control signals $u(k)$, $u^a(k)$ and $u'(k)$.

References

[1] S. K. Khaitan and J. D. McCalley, "Design techniques and applications of cyberphysical systems: A survey," *IEEE Systems Journal*, vol. 9, no. 2, pp. 350–365, 2014.

[2] A. Barboni, H. Rezaee, F. Boem, and T. Parisini, "Detection of covert cyber-attacks in interconnected systems: a distributed model-based approach," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3728–3741, 2020.

[3] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 2018.

[4] L. Niu, Z. Li, and A. Clark, "Lqg reference tracking with safety and reachability guarantees under false data injection attacks," in *American Control Conference (ACC)*. IEEE, 2019, pp. 2950–2957.

[5] V. Dolk, P. Tesi, C. De Persis, and W. Heemels, "Event-triggered control systems under denial-of-service attacks," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 93–105, 2016.

[6] M. Ghaderi, K. Gheitasi, and W. Lucia, "A blended active detection strategy for false data injection attacks in cyber-physical systems," *IEEE Transactions on Control of Network Systems*, vol. 8, no. 1, pp. 168–176, 2020.

[7] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proceedings of the 1st international conference on High Confidence Networked Systems*, 2012, pp. 55–64.

[8] 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.

[9] Y. Chen, S. Kar, and J. M. Moura, "Dynamic attack detection in cyber-physical systems with side initial state information," *IEEE Trans. on Automatic Control*, vol. 62, no. 9, pp. 4618–4624, 2016.

[10] G. Park, C. Lee, H. Shim, Y. Eun, and K. H. Johansson, "Stealthy adversaries against uncertain cyber-physical systems: Threat of robust zero-dynamics attack," *IEEE Transactions on Automatic Control*, vol. 64, no. 12, pp. 4907–4919, 2019.

[11] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Revealing stealthy attacks in control systems," in *50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, 2012, pp. 1806–1813.

[12] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Allerton conference on communication, control, and computing*. IEEE, 2009, pp. 911–918.
[13] R. S. Smith, "Covert misappropriation of networked control systems: Presenting a feedback structure," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 82–92, 2015.
[14] Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 93–109, 2015.
[15] S. Weerakkody and B. Sinopoli, "Detecting integrity attacks on control systems using a moving target approach," in *IEEE Conference on Decision and Control (CDC)*. IEEE, 2015, pp. 5820–5826.
[16] P. Griffioen, S. Weerakkody, and B. Sinopoli, "A moving target defense for securing cyber-physical systems," *IEEE Transactions on Automatic Control*, pp. 1–1, 2020.
[17] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding schemes for securing cyber-physical systems against stealthy data injection attacks," *IEEE Transaction on Control of Network Systems*, vol. 4, no. 1, pp. 106–117, 2016.
[18] K. Gheitasi and W. Lucia, "A finite-time stealthy covert attack against cyber-physical systems," in *7th International Conference on Control, Decision and Information Technologies (CoDIT)*, vol. 1. IEEE, 2020, pp. 347–352.
[19] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell, "A survey of physics-based attack detection in cyber-physical systems," *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, pp. 1–36, 2018.
[20] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water scada systemspart i: Analysis and experimentation of stealthy deception attacks," *IEEE Transaction on Control Systems Technology*, vol. 21, no. 5, pp. 1963–1970, 2012.
[21] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.
[22] F. Blanchini and S. Miani, *Set-theoretic methods in control*. Springer, 2008.
[23] F. Borrelli, A. Bemporad, and M. Morari, *Predictive control for linear and hybrid systems*. Cambridge University Press, 2017.
[24] S. V. Rakovic, E. C. Kerrigan, K. I. Kouramas, and D. Q. Mayne, "Invariant approximations of the minimal robust positively invariant set," *IEEE Transactions on automatic control*, vol. 50, no. 3, pp. 406–410, 2005.
[25] R. S. Smith, "A decoupled feedback structure for covertly appropriating networked control systems," *IFAC Proceedings Volumes*, vol. 44, no. 1, pp. 90–95, 2011.
[26] W. Lucia, D. Famularo, and G. Franze, "A set-theoretic reconfiguration feedback control scheme against simultaneous stuck actuators," *IEEE Transactions on Automatic Control*, vol. 63, no. 8, pp. 2558–2565, 2017.
[27] D. Angeli, A. Casavola, G. Franzè, and E. Mosca, "An ellipsoidal off-line mpc scheme for uncertain polytopic discrete-time systems," *Automatica*, vol. 44, no. 12, pp. 3113–3119, 2008.
[28] J. K. Scott, D. M. Raimondo, G. R. Marseglia, and R. D. Braatz, "Constrained zonotopes: A new tool for set-based estimation and fault detection," *Automatica*, vol. 69, pp. 126–136, 2016.
[29] M. Herceg, M. Kvasnica, C. N. Jones, and M. Morari, "Multi-parametric toolbox 3.0," in *2013 European control conference (ECC)*. IEEE, 2013, pp. 502–510.
[30] A. Kurzhanskiĭ and I. Vályi, *Ellipsoidal calculus for estimation and control*. Nelson Thornes, 1997.
[31] A. H. Glattfelder and W. Schaufelberger, *Control systems with input and output constraints*. Springer Science & Business Media, 2003.
[32] T. Nguyen and F. Jabbari, "Disturbance attenuation for systems with input saturation: an lmi approach," *IEEE Transactions on Automatic Control*, vol. 44, no. 4, pp. 852–857, 1999.
[33] G. Franze, W. Lucia, and F. Tedesco, "Resilient model predictive control for constrained cyber-physical systems subject to severe attacks on the communication channels," *IEEE Transactions on Automatic Control*, 2021.
[34] H. Gao, T. Chen, and L. Wang, "Robust fault detection with missing measurements," *International Journal of Control*, vol. 81, no. 5, pp. 804–819, 2008.

Kian Gheitasi received the B.Sc. degree in Electrical Engineering (2014) from the University of Tabriz, Iran, and the M.Sc. degree in Aerospace Engineering (2016) from the University of Tehran, Iran. He is currently a Ph.D. student of Information and Systems Engineering at Concordia University, Canada. His research interests include control theory and applications, and the security of cyber-physical systems.

Walter Lucia is currently an Associate Professor at the Concordia Institute for Information Systems Engineering, Concordia University, Canada. He received the M.Sc. degree in Automation Engineering (2011) and the Ph.D. degree in Systems and Computer Engineering (2015) from the University of Calabria, Italy. Before joining Concordia University, he was visiting research scholar in the ECE Department at Northeastern University (USA) and visiting postdoctoral researcher in the ECE Department at Carnegie Mellon University (USA). Dr. Lucia is currently an Associate Editor for the Control System Society - Conference Editorial Board, IEEE Systems Journal and Springer Journal of Control, Automation and Electrical Systems. Moreover, he is currently the Chair of the IEEE Montreal Chapters Systems, Man and Cybernetics, and Control Systems. Dr. Lucia research interests include control of unmanned vehicles, model predictive control, and resilient control of cyber-physical systems.