Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

Actuation attacks on constrained linear systems: a set-theoretic analysis

P. A. Trodden * **J. M. Maestre** ** **H. Ishii** ***

* *Department of Automatic Control & Systems Engineering, University of Sheffield, Sheffield, UK* p.trodden@sheffield.ac.uk
** *Department of Systems and Automation Engineering, University of Seville, Seville, Spain* pepemaestre@us.es
*** *Department of Computer Science, Tokyo Institute of Technology, Yokohama, Japan* ishii@c.titech.ac.jp

Abstract: This paper considers a constrained discrete-time linear system subject to actuation attacks. The attacks are modelled as false data injections to the system, such that the total input (control input plus injection) satisfies hard input constraints. We establish a sufficient condition under which it is not possible to maintain the states of the system within a compact state constraint set for all possible realizations of the actuation attack. The developed condition is a simple function of the spectral radius of the system, the relative sizes of the input and state constraint sets, and the proportion of the input constraint set allowed to the attacker.

Keywords: Control problems under conflict or uncertainties; Constrained control; Robustness

1. INTRODUCTION

The security of control systems to cyber-attacks has become a pressing issue, owing to the ubiquity of computers and networks and the vulnerabilities that these introduce (Smith, 2015). In the context of feedback control, attention has focused on several salient aspects of the cyber-security problem, including attack detection, synthesis and the analysis of control system stability and performance under different classes of attack, including denial of service (DoS), deception and false data injection (FDI) (Pasqualetti et al., 2013; Teixeira et al., 2015).

In this paper, we study a simple instance of an actuation attack problem—a type of data injection attack—and, using set-theoretic methods, develop fundamental conditions under which it is not possible to robustly defend the system. In particular, we consider the problem of maintaining the states of a constrained linear system within a given state target set while it is subject to adversarial input disturbances. We consider that the input constraint set is partitioned, via a scaling factor, into two portions: the control input is selected from one portion, and the attack input from the other, such that the overall input applied is constraint admissible. The main result of the paper is the characterization of a lower bound on the constraint scaling factor such that robust stabilization of the system—and infinite-time robust constraint satisfaction—for all realizations of the attack is not possible.

We note that although the state-feedback setting is simpler than that typically considered in the cyber-security literature—and renders certain aspects of the problem, such as stealth and detection, trivial—the results we obtain offer some insights into the relative ease of attacking a system according to its dynamics and constraints. The developed bound on the scaling factor depends, in a natural way, on the open-loop stability of the system, via its spectral radius, and the relative shapes and sizes of the input and state constraint sets. Following intuition, the bound confirms that more unstable systems with smaller target sets are easier to attack, in that the proportion of the input constraint set required by the attacker is smaller, which may have implications for the signal power and energy required for a successful attack.

A few other papers have used set-theoretic techniques in the context of cyber-security. Lucia et al. (2016) propose a receding-horizon control law utilizing robust reachability sets in order to mitigate FDI and DoS attacks. Mohajerin Esfahani et al. (2010) and Mo and Sinopoli (2012) use reachability analysis in order to characterize the impact of FDI attacks. The most closely related work, however, appears to be from outside of this literature: Schulze Darup et al. (2017) considered a constrained linear (open-loop stable) autonomous system subject to additive disturbances selected from scaled disturbance set, and developed lower and upper bounds on the critical scaling factor at which robust infinite-time constraint satisfaction is not possible. The present paper considers non-autonomous systems rather than autonomous ones, however, and the techniques employed are necessarily different in order to handle the possibility of open-loop instability.

The organization of this paper is as follows. Section 2 gives the problem statement, which is followed by a preliminary analysis in Section 3. In Section 4, we recall some established results on robust constraint admissible and control invariant sets, and develop some new ones that facilitate our developments. The main results of the paper are presented in Section 5, and are subsequently illustrated in Section 6. Section 7 contains a discussion of the results and the conservativeness of the bounds we develop. Conclusions and directions for future work are presented in Section 8. Proofs of theoretical results are omitted for brevity.

Notation: The sets of non-negative and positive reals are denoted, respectively, $\mathbb{R}_{0+}$ and $\mathbb{R}_{+}$. The set of natural numbers, including zero, is $\mathbb{N}$. For $a, b \in \mathbb{R}^n$, $a \leq b$ applies element by element. For $X, Y \subset \mathbb{R}^n$, the Minkowski sum is $X \oplus Y \triangleq \{x + y : x \in X, y \in Y\}$; for $Y \subset X$, the Minkowski difference is $X \ominus Y \triangleq \{x \in \mathbb{R}^n : Y + x \subset X\}$. For $X \subset \mathbb{R}^n$ and $a \in \mathbb{R}^n$, $X \oplus a$ means $X \oplus \{a\}$. AX denotes the image of a set $X \subset \mathbb{R}^n$ under the linear mapping $A : \mathbb{R}^n \to \mathbb{R}^p$, and is given by $\{Ax : x \in X\}$. The set $-X \triangleq \{-x : x \in X\}$ is the image of X under reflection in the origin. The support function of a non-empty set $X \subset \mathbb{R}^n$ is $h_X(x) \triangleq \sup\{x^\top z : z \in X\}$. A C-set is a convex and compact (closed and bounded) set containing the origin; a PC-set is a C-set with the origin in its interior.

2. PROBLEM STATEMENT

We consider a discrete-time, linear time-invariant system,

$$x_{k+1} = Ax_k + Bu_k, \qquad k \in \mathbb{N}, \tag{1}$$

where $x_k \in \mathbb{R}^n$ and $u_k \in \mathbb{R}^m$ are the state and input at time k. The states and inputs are constrained as,

$$x_k \in X \text{ and } u_k \in U, \qquad k \in \mathbb{N}.$$

Assumption 1. The pair (A, B) is reachable. X and U are PC-sets; U is symmetrical about the origin, *i.e.*, $U = -U$.

The setting considered in this paper is that the system (1) is subject to attacks on its input. We suppose that these attacks take place via an attacker gaining access to, and injecting data into, the control input signal, u. The system under attack is

$$x_{k+1} = Ax_k + B(v_k + a_k) \tag{2}$$

i.e., the input to the system is $u_k = v_k + a_k$, where $a_k \in U$ is the attack signal, and $v_k \in U$ the control signal provided by the system controller (the defender). More specifically, we consider that the attacker is able to use a proportion $\alpha \in [0, 1)$ of the input constraint space, while the defender is left with the remaining proportion $1 - \alpha$. For $k \in \mathbb{N}$,

$$a_k \in \alpha U \text{ and } v_k \in (1 - \alpha)U.$$

In this way, the overall input constraint—which typically represents a hard actuation limit—is respected, yet the attacker is able to disturb the system and simultaneously reduce the set of actions available to the defender.

The goal of the attacker is to drive the system states out of X. The goal of the defender is, naturally, to keep the state in X, despite the actions of the attacker. Our aim in this paper is to analyse this simple scenario and develop fundamental conditions, in terms of the parameter α, on when an attack is *undefendable*, *i.e.*, such that there exists no control law able to maintain the state within X.

3. PRELIMINARY ANALYSIS

We begin with some definitions relevant to the problem, and then link these to known concepts and results in constrained control. The following refer to the system (2) and constraints $(x_k, v_k, a_k) \in X \times (1 - \alpha)U \times \alpha U$.

Definition 2. (Attack and defence sets and strategies). The *admissible attack {defence} set* is αU $\{(1 - \alpha)U\}$, with $\alpha \in [0, 1)$. An *admissible attack {defence}* is an action $a_k \in \alpha U$ $\{v_k \in (1 - \alpha)U\}$. An *admissible attack {defence} strategy* is a policy $x \mapsto v \in \alpha U$ $\{x \mapsto a \in (1 - \alpha)U\}$.

Definition 3. (Undefendable and defendable attack set). An attack set αU is said to be *undefendable* for the system (2) if, for all $x_0 \in X$, there does not exist an admissible defence strategy that maintains $x_k \in X$ for all $k \geq 0$. Otherwise, an attack set is said to be defendable.

There is a direct link and equivalence between these definitions and established concepts in the literature: infinite reachability, strong reachability and robust control invariance (Bertsekas, 1972; Blanchini, 1999; Kerrigan, 2000).

Definition 4. (Bertsekas (1972)). A set $Y \subset R^n$ is:

1. *Infinitely reachable* if there exists a control law $\mu(\cdot)$ and some $x_0 \in Y$ such that $x_k \in Y$ and $v_k = \mu(x_k) \in (1 - \alpha)U$ for all $a_k \in \alpha U$.
2. *Strongly reachable* or *robust control invariant* (RCI) if there exists a control law $\mu(\cdot)$ such that for all $x_0 \in Y$, $x_k \in Y$ and $v_k = \mu(x_k) \in (1 - \alpha)U$ for all $a_k \in \alpha U$.

The link to defendability follows trivially.

Lemma 5. The attack set αU is defendable if, and only if, X is infinitely reachable. X is infinitely reachable if, and only if, it contains a robust control invariant set C.

Remark 6. In establishing a link between these concepts and the results later in the paper, we make a tacit assumption on the information pattern in the problem: the defender selects v_k with knowledge of x_k but without knowledge of a_k, while the attacker may have knowledge of both x_k and v_k. Moreover, we tacitly assume that both attacker and defender know the value of α.

This motivates the remainder of the paper. The question of whether an attack set is defendable or undefendable (as these concepts are defined) amounts exactly to whether or not the state constraint set X contains an RCI set. If it does, then the attack set can be said to be defendable [1] and standard techniques from robust constrained control can be used to keep the state within X. If it does not, then an attack set is undefendable, and there does not exist any defence strategy that keeps the state within X for all time, accounting for *all* possible actions of the attacker [2]. Our more concrete aim is, therefore, to characterize the relation between the constraint scaling factor α and the existence of an RCI set within X.

4. ROBUST CONSTRAINT-ADMISSIBLE AND CONTROL INVARIANT SETS

First we present some known results and new results regarding RCI sets, with respect to a general linear system

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + Ew_k, \\ (x_k, u_k, w_k) &\in X \times U \times W. \end{aligned} \tag{3}$$

[1] Defendability, as it is defined, is a weak notion, in the sense that it does not imply that all $x_0 \in X$ can be kept within X.

[2] Undefendability says nothing about how the attacker may determine an admissible attack strategy that achieves the goal of steering x outside X. This is a less standard control problem than that of the defender, and is beyond the scope of the paper.

These are subsequently specialized to the setting described in the previous section.

4.1 Some known results

The i-step robust constraint-admissible set is the set of all states that can be kept within X for at least i time steps, for any disturbance, respecting the input constraints:

$$C_i := \{x : \exists \mathbf{u}_i \in \mathcal{U}_i \text{ such that } \mathbf{x}_i \in \mathcal{X}_i \text{ for all } \mathbf{w}_i \in \mathcal{W}_i\}$$

where $\mathbf{u}_i$ (respectively $\mathbf{w}_i$) is the sequence of i controls $\{u_0, u_1, \ldots, u_{i-1}\}$ (disturbances $\{w_0, w_1, \ldots, w_{i-1}\}$), the set $\mathcal{U}_i \triangleq U \times \cdots \times U$, with a similar definition for $\mathcal{W}$ and W. The corresponding sequence $\mathbf{x}_i = \{x_0, x_1, \ldots, x_i\}$ is obtained by, starting from x_0, applying the input sequence $\mathbf{u}_j$ and disturbance sequence $\mathbf{w}_j$. The definition requires $\mathbf{x}_i \in \mathcal{X}_i \triangleq X \times \cdots \times X$.

We recall some basic facts about C_i and its limit C_∞ (Bertsekas, 1972; Blanchini, 1994; Kerrigan, 2000):

Lemma 7. Suppose U is a PC-set and W is a C-set. Then (i) $C_0 = X$; (ii) if X is compact [convex], then each C_i is closed [convex]; (ii) $C_{i+1} \subseteq C_i$; (iii) $C_i = \bigcap_{j=0}^{i} C_j$; (iv) $C_\infty := \lim_{i\to\infty} C_i = \bigcap_{i=0}^{\infty} C_i$; (v) if $0 \in$ interior(C_∞) then every C_i is a PC-set; (vi) if $0 \in$ interior(C_∞), then C_∞ is a robust control invariant set for the system (3) and constraint set (X, U, W); (vii) C_∞, if non-empty, is maximal in the sense that it contains all other robust control invariant sets for the system (3).

To compute C_i, the following recursion holds:

$$C_{i+1} = Q(C_i) \cap X,$$
with $C_0 = X$,

and where $Q(\cdot)$ is the backwards reachability operation:

$$Q(Y) \triangleq \{x : \exists u \in U \text{ such that } Ax + Bu \oplus EW \subseteq Y\}.$$

More specifically, for the linear time invariant system (3),

$$C_{i+1} = (A)^{-1}\big([C_i \ominus EW] \oplus (-BU)\big) \cap X,$$

where $(A)^{-1}(\cdot)$ denotes the pre-image of the linear transformation $A(\cdot)$, and exists regardless of whether A is invertible; for shorthand we will write $A^{-i}Y$ to denote $(A^i)^{-1}(Y)$.

Lemma 8.

(1) C_∞ is finitely determined if and only if there exists an $i^* < \infty$ such that $C_{i^*+1} = C_{i^*}$.
(2) If C_∞ is a PC-set, then such an i^* exists.

4.2 Some new results

The aim of the paper is to characterize the existence of the set C_∞ in terms of α. This requires the analysing of the sequence of sets $\{C_i\}$, the dynamics of which are characterized by Minkowski additions, subtractions, intersections and preimages, and not readily amenable to analysis. The following result therefore, which appears to be new, gives insight into how C_i (and therefore C_∞) may be characterized in terms of sets with simpler dynamics that are more amenable to analysis.

Proposition 9. The set C_i is bounded as

$$C_i \subseteq \bigcap_{j=0}^{i} A^{-j} T_j \tag{4}$$

where

$$T_{i+1} = (T_i \ominus A^i EW) \oplus A^i(-BU)$$
with $T_0 = X$.

Remark 10. A special case of this result was reported by Schulze Darup et al. (2017), who considered an autonomous system $x_{k+1} = Ax_k + Ew_k$ subject to a disturbance from a scaled set αW. In that setting, *i.e.*, without a control input, what we refer to here as C_∞ is the maximal robust *positively* invariant set. The authors determine conditions on the scaling constant α under which C_∞ exists. Schulze Darup et al. (2017) develop the following relation (5), which we show now to be a corollary of Proposition 9.

Corollary 11. If $U = \{0\}$ then $T_i = X \ominus R_i$ and

$$C_i = \bigcap_{j=0}^{i} (A^j)^{-1}(X \ominus R_i) \text{ where } R_i \triangleq \bigoplus_{j=0}^{i} A^j W. \tag{5}$$

Note that in (5) the relation for C_i holds with equality, and not just the inclusion depicted in Proposition 9. The reason for the weakening of the equality to mere inclusion is the behaviour of the Minkowski sum under the intersection: for sets A, B and C, $(A \cap B) \oplus C \subseteq (A \oplus C) \cap (B \oplus C)$ and not $(A \cap B) \oplus C = (A \oplus C) \cap (B \oplus C)$. The latter equality does hold if the *union* of convex sets A and B is convex, which is generally not the case. This, together with the fact that we consider a non-autonomous system and not a stable autonomous one, means that the methodologies and results of Schulze Darup et al. (2017) do not apply.

We conclude the section by establishing sufficient conditions for emptiness of the set C_i for some $i > 0$ and subsequently C_∞. The results are central to the developments in the next section, when we specialize to the input-attack setting.

Proposition 12.
If, for some $i^\star > 0$, $T_{i^\star} = \emptyset$ then $C_i = \emptyset$ for all $i \geq i^\star$.

Proposition 13.
If, for some $i^\star > 0$, $S_{i^\star} = \emptyset$, where

$$S_i \triangleq X \oplus \left[\bigoplus_{j=0}^{i-2} A^j B(-U)\right] \ominus \left[\bigoplus_{j=0}^{i-1} A^j EW\right],$$

then $T_i = \emptyset$ for all $i \geq i^\star$.

5. FOR WHICH VALUES OF α IS AN ATTACK SET UNDEFENDABLE?

We now recast some of the results from the previous section in the particular setting of the paper, and develop conditions under which C_∞ does not exist.

Specializing the definitions of C_i and T_i to the system (2) and constraints $(x_k, v_k, a_k) \in X \times (1-\alpha)U \times \alpha U$, and exploiting the symmetry of U, we obtain

$$C^\alpha_{i+1} = A^{-1}([C^\alpha_i \ominus \alpha BU] \oplus (1-\alpha)BU) \cap X$$
with $C^\alpha_0 = X$,

and

$$T^\alpha_{i+1} = (T^\alpha_i \ominus \alpha A^i BU) \oplus (1-\alpha)(A^i BU)$$
with $T^\alpha_0 = X$,

where the sets are super-indexed by α to denote their dependency on this scaling factor. The connection between the two is, following Proposition 9,

$$C_i^\alpha \subseteq \bigcap_{j=0}^{i} A^{-j} T_j^\alpha.$$

In a similar way, the set S_i in Proposition 13 may be specialized to the setting and denoted S_i^α.

Our goal is to determine, for each $i^\star \in \mathbb{N}$, the smallest α for which $C_{i^\star}^\alpha$ is empty:

$$\alpha_{i^\star} \triangleq \inf\{\alpha : C_{i^\star}^\alpha = \emptyset, \alpha \in [0,1]\}.$$

In our main result, Theorem 16, we establish an upper bound on $\alpha_{i^\star}$. We achieve this by characterizing, for each $i^\star \in \mathbb{N}$, an $\bar{\alpha}_{i^\star}$ that renders $S_{i^\star}^\alpha$ empty for all $\alpha > \bar{\alpha}_{i^\star}$. By Propositions 12 and 13, any $\alpha > \bar{\alpha}_{i^\star} \geq \alpha_{i^\star}$ then ensures that $C_{i^\star}^\alpha$ is empty. We find that this bound depends on the relative sizes of the constraint sets X and U, as well as the relative stability or instability (via the spectral radius) of the open-loop system.

The following assumption is key to the development and simplicity of the result:

Assumption 14. The dominant eigenvalue of A is real and positive.

Let ρ_A denote the spectral radius of A, and $\mathcal{Z} \triangleq \{z_A^1, \ldots, z_A^r, -z_A^1, \ldots, -z_A^r\}$ be the set of r linearly independent eigenvectors corresponding to the dominant eigenvalue, plus their additive inverses. Define

$$\bar{z}_A \triangleq \arg\min_{z \in \mathcal{Z}} h_X(z)/h_{BU}(z),$$

and $H_{XU}(\bar{z}_A) \triangleq h_X(z_A)/h_{BU}(z_A)$, the smallest among the ratio of support functions to X and BU evaluated in the directions $\pm z_A^i$, $i = 1 \ldots r$. The next assumption ensures this is well defined.

Assumption 15. The mapped set BU has non-zero support in at least one of the directions $\pm z_A^i, i = 1 \ldots r$.

Theorem 16. Suppose Assumptions 1, 14 and 15 hold. If, for some $i^\star \in \mathbb{N}$,

$$\alpha > \bar{\alpha}_{i^\star} \triangleq \begin{cases} \dfrac{1 + H_{XU}(\bar{z}_A)[1-\rho_A] - \rho_A^{i^\star-1}}{2 - \rho_A^{i^\star-1} - \rho_A^{i^\star}} & \rho_A \neq 1 \\ \dfrac{H_{XU}(\bar{z}_A) + i^\star - 1}{2i^\star - 1} & \rho_A = 1 \end{cases}$$

and $\bar{\alpha}_{i^\star} < 1$ then $C_i^\alpha = \emptyset$ for all $i \geq i^\star$.

Two corollaries of this theorem follow.

Corollary 17. If $\alpha > \bar{\alpha}_{i^\star}$ when $\bar{\alpha}_{i^\star} < 1$ for some $i^\star \in \mathbb{N}$, then the attack set αU is undefendable; moreover, the state is guaranteed to remain in X, for all attack strategies, for at most $i^\star - 1$ steps.

Corollary 18. If

$$\alpha > \bar{\alpha}_\infty \triangleq \begin{cases} \dfrac{1 + H_{XU}(\bar{z}_A)[1-\rho_A]}{2} & \rho_A < 1 \\ \dfrac{1}{1+\rho_A} & \rho_A \geq 1 \end{cases}$$

and $\bar{\alpha}_\infty < 1$ then $C_\infty^\alpha = \emptyset$.

The bounds obtained here provide insight into the relative ease of attacking a system depending on its dynamics and constraints. More specifically, the critical scaling factor depends on the most unstable eigenvalue of the system and the relative sizes of the state and input constraint sets in the direction of the corresponding eigenvector. The result implies that unstable systems are easier to attack (for example, if $\rho_A > 1$ then $\bar{\alpha}_\infty < 1/2$, so the attack set does not need to be as large as the defence set to render the system undefendable) and also that (un)defendability depends on the relative sizes of the sets BU (the mapped inputs) and X (for example, even if $\rho_A = 0$, the system can be rendered undefendable if $\bar{\alpha}_\infty < 1$, which requires $H_{XU}(\bar{z}_A) < 1 \implies h_{BU}(\bar{z}_A) > h_X(\bar{z}_A)$).

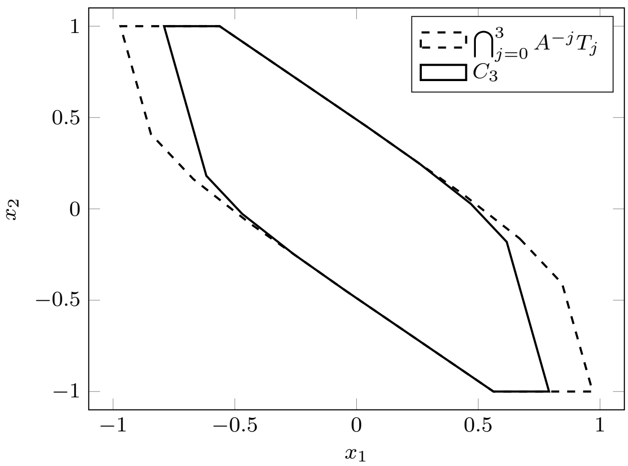


Fig. 1. Comparison of C_3 and its bounding set $\bigcap_{j=0}^{3} A^{-j}T_j$ for system $\mathbf{S}_3$ with $\alpha = 0.1$.

Remark 19. It should be noted that Assumption 14 places restrictions only on the dominant eigenvalues. Under this assumption, the long-term critical evolution of the set $A^iEW = \alpha A^iBU$, by which the intermediate sets are restricted, is in the direction $\bar{z}_A$, which enables the simple result obtained. It is possible to extend the result to more general A matrices, such as those with complex dominant poles. However, because the long-term growth of the set αA^iBU is then not in single direction, it is more involved to determine the number of steps after which the set T_i becomes empty.

Remark 20. It is interesting to note that the derived bound is consistent with the obvious strategy for attacking an unstable system, namely $a(x,v) = -v(x)$ if the information pattern permits it, which guarantees that the state leaves X in finite time. Indeed, since $\bar{\alpha}_\infty < 1/2$ for all $\rho_A > 1$, the attacker can choose $\alpha = 1/2$, permitting this strategy.

6. ILLUSTRATIVE EXAMPLES

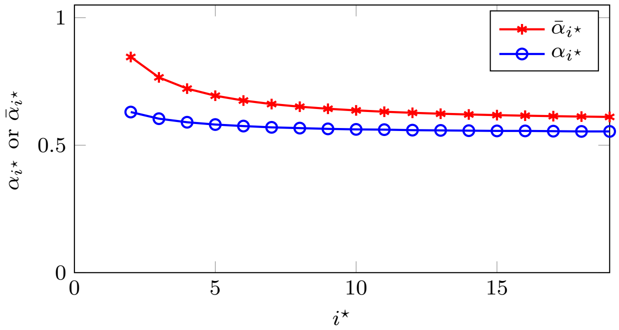
We illustrate the results via three example systems:

$$\mathbf{S}_1 : A = \begin{bmatrix} 0.5 & 1 \\ 0 & 0.7 \end{bmatrix} \quad \mathbf{S}_2 : A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \mathbf{S}_3 : A = \begin{bmatrix} 1.9 & 1.1 \\ 0.5 & 1.5 \end{bmatrix}$$

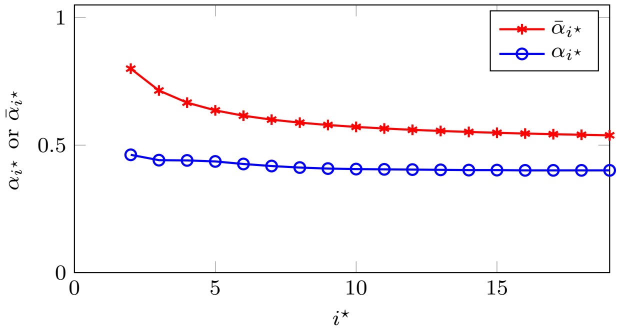
where, in each case, $B = [0.5\ 1]^\top$. The sets X and U are the unit hypercubes.

First we illustrate Proposition 9. Fig. 1 compares, for system $\mathbf{S}_3$ and a scaling factor of $\alpha = 0.25$, the three-step constraint admissible set C_3 with the outer bounding set $\bigcap_{j=0}^{3} A^{-j}T_j$ derived in Proposition 9. The inclusion is not tight, as pointed out in Remark 10.

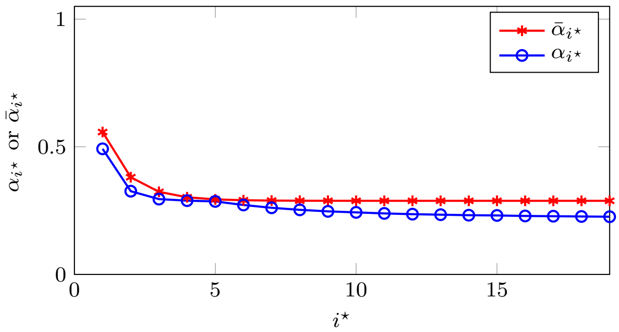
Next, we illustrate and investigate the result of Theorem 16 and its corollaries. Figure 2 shows, for the systems $\mathbf{S}_1$ to



(a) Stable system $\mathbf{S}_1$



(b) Double integrator $\mathbf{S}_2$



(c) Unstable system $\mathbf{S}_3$

Fig. 2. Comparison of the bound $\bar{\alpha}_{i^\star}$ obtained from Theorem 16 with the true bound $\alpha_{i^\star}$.

$\mathbf{S}_3$, the exact critical scaling factors $\alpha_{i^\star}$ and the upper bound $\bar{\alpha}_{i^\star}$ from Theorem 16. The exact scaling factors were found by trial and error, searching over $\alpha \in (0, 1)$ until the smallest value is found for which the reachability recursion $C^\alpha_{i+1} = Q(C^\alpha_i) \cap X$ results in $C^\alpha_i = \emptyset$ for $i = i^\star$.

7. DISCUSSION

The bound on critical α is merely sufficient and, as the numerical results indicate, it is not tight—C^α_i may become empty at some smaller i or α than the bound of Theorem 16 suggests. The sources of conservatism are threefold:

(1) Proposition 12 is sufficient, but not necessary, to guarantee emptiness of $C_{i^\star}$ at some $i^\star$. The lack of necessity arises from the lack of tightness (illustrated in Fig. 1) in the inclusion relation between C_i and T_i established in Proposition 9. This itself is, as explained in Remark 10, because Minkowski addition is not distributive over set intersections. To avoid this, and guarantee equality in the relation of Proposition 9 and necessity of the condition in Proposition 12, strong and unusual assumptions on the system and constraints would be required.
(2) Similarly, Proposition 13 is merely sufficient to ensure emptiness of T_i at a given $i = i^\star$. The source of conservatism again arises from the basic properties of Minkowski addition and subtraction, and in particular that these operations do not commute: Proposition 13 uses the fact that, for sets A, B and C, $A \oplus C \ominus B \supseteq A \ominus B \oplus C$.
(3) Theorem 16 is sufficient, but not necessary, to ensure emptiness of $S^\alpha_{i^\star}$. The condition was developed by considering the dynamics of S^α_i over times $i \in \mathbb{N}$ in *only one* direction in $\mathbb{R}^n$, the eigenvector associated with the dominant (real) eigenvalue. It is possible, but this depends on the system and constraints, that emptiness of $S^\alpha_{i^\star}$ could be concluded at some smaller α than $\bar{\alpha}_{i^\star}$ by considering other directions. On the other hand, the long-term change in S^α_i will tend to be dominated by activity in the direction of the dominant eigenvalue; our numerical results show relatively good agreement between the theoretical bound and the exact bound as $i^\star$ grows.

Finally, it is worth remarking that the developed theoretical bounds are simple to determine, requiring only the spectral information about the open-loop system and a couple of support function evaluations on the constraint sets X and U. In comparison, to determine the exact $\alpha(i^\star)$ requires a search over the space $\alpha \in (0, 1)$, computing the sequence $\{C^\alpha_i\}_{i \geq 0}$ until it is found that $C^\alpha_{i^\star}$ is empty.

8. CONCLUSIONS AND FUTURE WORK

We have analysed a simple instance of a constrained linear system subject to actuation attacks and, using set-theoretic methods, derived a lower bound on the sufficient size of the attack set in order that robust infinite-time constraint satisfaction can not be guaranteed. The bound depends, in an intuitive way, on the spectral radius of the system and size and shape of the constraint sets. Future work will investigate lowering conservatism (*e.g.*, by deriving results considering more than one eigenvector direction), consider more general instances of A (*e.g.*, with dominant complex eigenvalues) and a more sophisticated setting (*e.g.*, with outputs and sensor data injection).

ACKNOWLEDGEMENTS

Financial support from the JSPS fellowship PE16048 and the MINECO-Spain project C3PO (ref: DPI2017-86918-R) is gratefully acknowledged.

REFERENCES

D. P. Bertsekas. Infinite-time reachability of state-space regions by using feedback control. *IEEE Transactions on Automatic Control*, 17(5):604–613, 1972.

F. Blanchini. Ultimate boundedness control for uncertain discrete-time systems via set-induced Lyapunov functions. *IEEE Transactions on Automatic Control*, 39(2): 428–433, 1994.

F. Blanchini. Set invariance in control. *Automatica*, 35(11): 1747–1767, 1999.

E. C. Kerrigan. *Robust Constraint Satisfaction: Invariant Sets and Predictive Control*. PhD thesis, University of Cambridge, 2000.

I. Kolmanovsky and E. G. Gilbert. Theory and computation of disturbance invariant sets for discrete-time linear systems. *Mathematical Problems in Engineering*, 4:317–367, 1998.

W. Lucia, B. Sinopoli, and G. Franze. A set-theoretic approach for secure and resilient control of cyber-physical systems subject to false data injection attacks. In *2016 Science of Security for Cyber-Physical Systems Workshop*, pages 1–5, 2016.

Y. Mo and B. Sinopoli. Integrity attacks on cyber-physical systems. In *Proceedings of the 1st International Conference on High Confidence Networked Systems*, pages 47–54, 2012.

P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson. Cyber attack in a two-area power system: Impact identification using reachability. In *Proceedings of the 2010 American Control Conference*, pages 962–967, 2010.

F. Pasqualetti, F. Dörfler, and F. Bullo. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 58(11):2715–2729, 2013.

R. Schneider. *Convex Bodies: The Brunn-Minkowski Theory*, volume 44 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 1993.

M. Schulze Darup, R. Schaich, and M. Cannon. How scaling of the disturbance set affects robust positively invariant sets for linear systems. *International Journal of Robust and Nonlinear Control*, 27(16):3236–3258, 2017.

R. S. Smith. Covert misappropriation of networked control systems: Presenting a feedback structure. *IEEE Control Systems*, 35(1):82–92, 2015.

A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson. Secure control systems: A quantitative risk management approach. *IEEE Control Systems*, 35(1):24–45, 2015.