2015 European Control Conference (ECC)
July 15-17, 2015. Linz, Austria

Covert Attack on a Discrete-Time System with Limited Use of the Available Disruption Resources

Efstathios Kontouras[†], Anthony Tzes[†] and Leonidas Dritsas[††]

***Abstract*— This paper addresses the design of a covert attack on a linear multivariable dynamical system with input hard constraints. The system evolves in the discrete-time domain and is subject to performance and alarm state constraints, both represented by convex and compact polyhedral sets. A contractive control law guarantees positive invariance of the performance set, while ensuring asymptotic stability of the origin with maximum convergence rate. An attacker succeeds in gaining control of the system and sends false control commands, when it is necessary, eventually driving the state vector outside the performance set without violating any alarm constraints. Simulation studies highlight the results of this adversary control scheme.**

I. Introduction

Modern control design methods for linear systems with input and state constraints usually involve the use of polyhedral sets, due to their inherent efficiency and flexibility over their ellipsoidal counterparts [1–3]. Controlled invariance of a polyhedral operating region is quite useful when addressing constrained control problems and has been extensively studied [2–6]. However, recent results indicate that disrupting the invariance property may also be of some interest, especially from an adversary point of view [7, 8].

The motivation for our research is based on security issues arising due to the existence of potential attackers in cyber-physical or networked systems [9–11]. Previous authors have classified generic attack models on such systems emphasizing on the design and detection of stealthy or covert attacks [12, 13]. Generally, a covert attack is a control action that does not create a detectable anomaly in the behaviour of the system. In our context, an anomaly is detected whenever the state vector exits a predefined set of alarm constraints.

This work extends previous results of the authors [14]. In this article, we examine a constrained multivariable discrete-time dynamical system, while a contractive controller and a covert attacker take turns affecting its input. We assume that in steady state, the state vector should always be contained inside a desired operation domain due to performance or safety considerations. The objective of the contractive controller is to ensure that the state trajectories emanating for all initial conditions belonging to the alarm set will enter the desired operation domain in a finite time interval and remain within it for all future time instants. The primary objective of the covert attacker is to use an expanding controller in order to steer and keep the state vector outside the desired operation domain, while always respecting the alarm constraints. Furthermore, the attacker may relinquish its authority over the control input according to a switching logic, since a secondary objective is to achieve the main task with a limited use of the available disruption resources.

In Section II the mathematical model of the system under consideration is established and the problem settings are presented. Sections III and IV introduce the design procedures for the contractive and the expanding controller respectively, while in section V the switching logic is developed. Section VI presents simulation results validating our conceptual approach. Finally, in Section VII we provide some concluding remarks.

Regarding notations, symbols $\mathbb{O}$ and $\mathbb{I}$ stand for the zero and the identity matrix respectively, symbol $\setminus$ stands for the operation of set subtraction, symbols ∂ and int stand for the boundary and the interior of a set respectively, while all inequalities involving matrices or vectors are assumed to be componentwise.

II. Problem Statement

Consider the discrete-time dynamical system S of Fig. 1, described by the difference equation

$$S: \; x[t+1] = Ax[t] + Bu_{\sigma[t]}[t], \quad x[0] = x_0, \qquad (1)$$

where $x[t] \in \mathbb{R}^n$ is the state vector, $u_{\sigma[t]}[t] \in \mathbb{R}^m$ are the controller output vectors, $t \in \mathbb{N}$ is the time variable and $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$ are given matrices. The switching signal $\sigma[t]$ is a mapping $\sigma : \mathbb{N} \to \{1, 2\}$ ensuring that the controllers are mutually exclusive. We establish the notations $u_1[t] = u_c[t]$ and $u_2[t] = u_x[t]$ and we assume that both controller outputs satisfy a saturation constraint of the form

$$u_{\min} \le u_{\sigma[t]}[t] \le u_{\max}, \quad \forall t \in \mathbb{N}, \qquad (2)$$

where $u_{\min} \in \mathbb{R}^m$, $u_{\min} < 0$ and $u_{\max} \in \mathbb{R}^m$, $u_{\max} > 0$ are given vectors.

It is also given a convex and compact polyhedral set

$$\mathcal{A}(G, w) = \{x \in \mathbb{R}^n : Gx \le w\}, \qquad (3)$$

representing alarm constraints, where $G \in \mathbb{R}^{p\times n}$ and $w \in \mathbb{R}^p$ with $w > 0$. We may now introduce the alarm signal

$$a(x) = \begin{cases} 0, & \text{if} \quad x \in \mathcal{A} \\ 1, & \text{if} \quad x \notin \mathcal{A} \end{cases}.$$

We select a convex and compact polyhedral set

$$\mathcal{D}(P, r) = \{x \in \mathbb{R}^n : Px \le r\}, \quad \mathcal{D} \subset \mathcal{A} \qquad (4)$$

[†]The authors are with the Electrical & Computer Engineering Department, University of Patras, Rio 26500, Greece.

[††]The author is with the Department of Electrical & Electronic Engineering Educators, School of Pedagogical & Technological Education, ASPETE, Athens 14121, Greece. Corresponding author's email: tzes@ece.upatras.gr

$$\partial\mathcal{D} \cap \partial\mathcal{A} = \varnothing, \tag{5}$$

representing a desired operation domain, where $P \in \mathbb{R}^{q\times n}$ and $r \in \mathbb{R}^q$ with $r > 0$. Clearly, the inequalities $w > 0$, $r > 0$ imply that the origin is an interior point of both sets $\mathcal{A}$ and $\mathcal{D}$. Since $\mathcal{D} \subset \mathcal{A}$, there exists a tolerance zone

$$\mathcal{H} = \mathcal{A} \setminus \mathcal{D} \tag{6}$$

such that for all $x \in \mathcal{H}$ the desired operation constraints are not satisfied, yet no alarm signal is given. The expanding controller is activated for the first time at $t = 0$ and $x_0 \in \mathcal{D}$.

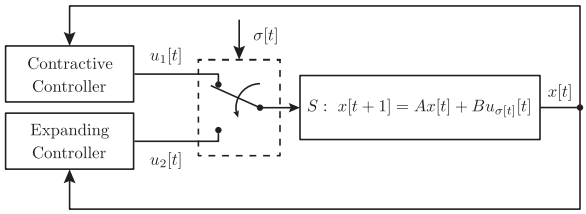


Fig. 1: Block diagram for the closed-loop system.

The contractive controller implements a control policy that ensures positive invariance of set $\mathcal{D}$, while converging the state vector, at a maximum rate, to the origin. Furthermore, if the contractive controller is activated at some t such that $x[t] \in \mathcal{H}$, the control law u_c should guarantee that the emanating state trajectory will respect the alarm constraints and enter set $\mathcal{D}$ in a finite time interval.

On the other hand, the covert attacker affects the system utilizing both the expanding controller and the switching signal. The expanding controller implements a control policy converging the state vector, at a maximum rate, to a state $x_e \in \mathcal{H}$ such that the distance of x with respect to $\mathcal{D}$ is ultimately maximized. In addition, whenever the expanding controller is activated, the control law u_x should guarantee that the emanating state trajectory will respect the alarm constraints.

Finally, the switching signal regulates the dwell time of the expanding controller and ensures that the state trajectory remains exclusively inside zone $\mathcal{H}$ for all $t > T$, for some $T \in \mathbb{N}^*$. We assume that the attacker has full knowledge of the sets $\mathcal{A}$, $\mathcal{D}$ and of the system dynamics (1), (2) as well as unhindered access to perfect state measurements.

III. Contractive Controller Design

Let us consider a state-dependent switched control law

$$u_c[t] = \begin{cases} K_{c_1}x[t], & \text{if} \quad x[t] \in \mathcal{D} \\ K_{c_2}x[t], & \text{if} \quad x[t] \in \mathcal{H} \end{cases},$$

where K_{c_1}, $K_{c_2} \in \mathbb{R}^{m\times n}$. We may determine the matrices K_{c_1}, K_{c_2} according to the following theorem [6]:

Theorem 1: A linear, state-feedback control $u = Kx$, where $K \in \mathbb{R}^{m\times n}$, renders the polyhedral set

$$\mathcal{R}(F, v) = \{x \in \mathbb{R}^n : Fx \le v\},$$

where $F \in \mathbb{R}^{\rho\times n}$ and $v \in \mathbb{R}^\rho$, $v > 0$: (i) positively invariant with respect to the resulting closed-loop system

$$S_{cl}:\ x[t+1] = (A + BK)\,x[t], \quad x[0] = x_0$$

and (ii) a domain of attraction of the equilibrium $x = 0$, while satisfying control constraints $u \in [u_{\min}, u_{\max}]$ for initial states belonging to $\mathcal{R}$ and ensuring maximum rate of convergence, if and only if there exist a number $\varepsilon \in \mathbb{R}_+$ and matrices $H \in \mathbb{R}^{\rho\times\rho}$, $M \in \mathbb{R}^{2m\times\rho}$ such that:

$$F(A + BK) = HF, \quad Hv \le \varepsilon v \tag{7}$$

$$MF = [K \quad -K]^\top, \quad Mv \le [u_{\max} \quad -u_{\min}]^\top \tag{8}$$

$$H \ge \mathbb{0}, \quad M \ge \mathbb{0}, \quad \varepsilon \le 1. \tag{9}$$

If such a control exists, then it can be determined by solving the linear programming problem

$$\min_{\varepsilon,K,H,M} \{\varepsilon\}$$

under linear constraints (7)-(9).

We apply Theorem 1 twice, initially for set $\mathcal{D}(P, r)$ and then for set $\mathcal{A}(G, w)$; parameters K_{c_1}, ε_1 and K_{c_2}, ε_2 are obtained respectively. The control law $K_{c_1}x$ satisfies all design requirements associated with set $\mathcal{D}$. On the other hand, the control law $K_{c_2}x$ ensures that the state trajectories emanating for all initial conditions $x \in \mathcal{H}$, enter set $\mathcal{D}$ in a finite time interval without violating any alarm constraints.

Indeed, let us define $V_{\mathcal{A}} : \mathbb{R}^n \to \mathbb{R}_+$ as

$$V_{\mathcal{A}}(x) = \max_{l=1,2,\ldots,p} \left\{ \frac{(Gx)_l}{w_l} \right\},$$

where $(Gx)_l$ and w_l denote the l-th element of vectors Gx and w respectively. Metric $V_{\mathcal{A}}$ qualifies as a polyhedral Lyapunov function for the closed-loop system

$$S_{cl,2}:\ x[t+1] = (A + BK_{c_2})\,x[t]$$

and set $\mathcal{A}$ is contractive with respect to $S_{cl,2}$, therefore [6] $V_{\mathcal{A}}(x[t+1]) \le \varepsilon_2 V_{\mathcal{A}}(x[t])$. Consequently, if the contractive controller is activated at some time instant t and $x[t] \in \mathcal{H}$ it is always possible to determine an instant $t_f > t$ and a scalar $\beta \in (0, 1)$ such that $V_{\mathcal{A}}(x[t_f]) = \beta$ and $\mathcal{A}_\beta(G, \beta w) \subset \mathcal{D}$, where $\mathcal{A}_\beta$ is a sublevel set of $\mathcal{A}$ and $x[t_f] \in \partial\mathcal{A}_\beta$; thus, our design objectives are met.

IV. Expanding Controller Design

Let us consider an affine state-feedback control law

$$u_x[t] = u_e + K_x\,(x[t] - x_e), \tag{10}$$

where $u_e \in \mathbb{R}^m$, $x_e \in \mathbb{R}^n$ and $K_x \in \mathbb{R}^{m\times n}$.

A. Computation of Pair (u_e, x_e)

The distance of a point $x \in \mathbb{R}^n$ from a set $\mathcal{S} \subset \mathbb{R}^n$ is commonly defined as

$$d(x, \mathcal{S}) \triangleq \inf_{y\in\mathcal{S}} d(x, y),$$

where mapping $d : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_+$ is an arbitrarily chosen distance function. Let us denote with $x_{\mathcal{H}}$ the most distant state $x \in \mathcal{H}$ with respect to set $\mathcal{D}$. As a matter of fact, $x_{\mathcal{H}}$ is the solution to the optimization problem

$$x_{\mathcal{H}} = \arg\max_{x\in\mathcal{H}} d(x, \mathcal{D}). \tag{11}$$

In the sequel, we develop a simple and efficient method to determine the state $x_{\mathcal{H}}$, based on the selection of a suitable function d.

Definition 1: Let $\mathcal{S} \subset \mathbb{R}^n$ be a given convex and compact set such that $0 \in int(\mathcal{S})$. Then, mapping $\psi_{\mathcal{S}} : \mathbb{R}^n \to \mathbb{R}_+$

$$\psi_{\mathcal{S}}(x) \triangleq \inf\{\lambda \geq 0 : x \in \lambda \mathcal{S}\}$$

is called Minkowski functional and qualifies as a gauge function.

It is known, that positive definite functions are strongly related to the notion of distance according to the following theorem [15]:

Theorem 2: Consider a globally positive definite function $\psi : \mathbb{R}^n \to \mathbb{R}_+$. Then, mapping $d : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_+$

$$d(x,y) = \begin{cases} \psi(x) + \psi(y), & \text{if} \quad x \neq y \\ 0, & \text{if} \quad x = y \end{cases}$$

qualifies as a distance function in $\mathbb{R}^n$.

Taking into account Definition 1 and Theorem 2 we present the following theorem:

Theorem 3: Let $\mathcal{S}_1 \subset \mathbb{R}^n$ be a given convex and compact set such that $0 \in int(\mathcal{S}_1)$ and $\psi_{\mathcal{S}_1}$ be the Minkowski functional associated with $\mathcal{S}_1$. We equip space $\mathbb{R}^n$ with the distance function

$$d(x,y) = \begin{cases} \psi_{\mathcal{S}_1}(x) + \psi_{\mathcal{S}_1}(y), & \text{if} \quad x \neq y \\ 0, & \text{if} \quad x = y \end{cases}$$

and we also consider a set $\mathcal{S}_2 \subset \mathbb{R}^n$. Then, the following equality holds:

$$\arg\max_{x \in \mathcal{S}_2} d(x, \mathcal{S}_1) = \arg\max_{x \in \mathcal{S}_2} \psi_{\mathcal{S}_1}(x), \tag{12}$$

where

$$d(x, \mathcal{S}_1) = \inf_{y \in \mathcal{S}_1} d(x,y).$$

Proof: Beginning from the left hand side of equation (12) we have

$$\begin{aligned} \arg\max_{x \in \mathcal{S}_2} d(x, \mathcal{S}_1) &= \arg\max_{x \in \mathcal{S}_2} \left\{ \inf_{y \in \mathcal{S}_1} d(x,y) \right\} \\ &= \arg\max_{x \in \mathcal{S}_2} \left\{ \inf_{y \in \mathcal{S}_1} \{\psi_{\mathcal{S}_1}(x) + \psi_{\mathcal{S}_1}(y)\} \right\}. \end{aligned}$$

However, $\psi_{\mathcal{S}_1}$ is a positive definite function and $0 \in int(\mathcal{S}_1)$, hence

$$\begin{aligned} \arg\max_{x \in \mathcal{S}_2} d(x, \mathcal{S}_1) &= \arg\max_{x \in \mathcal{S}_2} \left\{ \psi_{\mathcal{S}_1}(x) + \inf_{y \in \mathcal{S}_1} \psi_{\mathcal{S}_1}(y) \right\} \\ &= \arg\max_{x \in \mathcal{S}_2} \{\psi_{\mathcal{S}_1}(x) + 0\} \\ &= \arg\max_{x \in \mathcal{S}_2} \psi_{\mathcal{S}_1}(x), \end{aligned}$$

thus the proof is completed. ■

We are interested in solving equation (11). Since $\mathcal{D}$ is a polyhedral set, the Minkowski functional $\psi_{\mathcal{D}}$ is equivalent to the function $V_{\mathcal{D}} : \mathbb{R}^n \to \mathbb{R}_+$ defined as

$$V_{\mathcal{D}}(x) = \max_{l=1,2,\ldots,q} \left\{ \frac{(Px)_l}{r_l} \right\}.$$

If we define the distance function

$$d(x,y) = \begin{cases} V_{\mathcal{D}}(x) + V_{\mathcal{D}}(y), & \text{if} \quad x \neq y \\ 0, & \text{if} \quad x = y \end{cases}$$

and apply Theorem 3 for $\mathcal{S}_1 = \mathcal{D}$ and $\mathcal{S}_2 = \mathcal{H}$, we obtain

$$x_{\mathcal{H}} = \arg\max_{x \in \mathcal{H}} d(x, \mathcal{D}) = \arg\max_{x \in \mathcal{H}} V_{\mathcal{D}}(x). \tag{13}$$

Due to equation (5), set $\mathcal{H}$ is always non-convex. We resolve this problem in terms of the following proposition:

Proposition 1: Let $\mathcal{S}_1 \subset \mathbb{R}^n$ be a given convex and compact set such that $0 \in int(\mathcal{S}_1)$ and $\psi_{\mathcal{S}_1}$ be the Minkowski functional associated with $\mathcal{S}_1$. Then, for every set $\mathcal{S}_2 \subset \mathbb{R}^n$ such that $\mathcal{S}_2 \setminus \mathcal{S}_1 \neq \varnothing$ holds the equality

$$\arg\max_{x \in \mathcal{S}_1 \cup \mathcal{S}_2} \psi_{\mathcal{S}_1}(x) = \arg\max_{x \in \mathcal{S}_2 \setminus \mathcal{S}_1} \psi_{\mathcal{S}_1}(x). \tag{14}$$

Proof: Let $\psi_{\mathcal{S}_1}(x) = \Psi$, for all $x \in \partial\mathcal{S}_1$. Then, the following inequalities may be directly derived:

$$\psi_{\mathcal{S}_1}(x) \leq \Psi, \quad \forall x \in \mathcal{S}_1 \tag{15}$$

$$\psi_{\mathcal{S}_1}(x) > \Psi, \quad \forall x \notin \mathcal{S}_1. \tag{16}$$

Beginning from the left hand side of equation (14) we have

$$\begin{aligned} \arg\max_{x \in \mathcal{S}_1 \cup \mathcal{S}_2} \psi_{\mathcal{S}_1}(x) &= \arg\max_{x} \left\{ \max_{x \in \mathcal{S}_1} \psi_{\mathcal{S}_1}(x), \max_{x \in \mathcal{S}_2 \setminus \mathcal{S}_1} \psi_{\mathcal{S}_1}(x) \right\} \\ &\overset{(15)}{=} \arg\max_{x} \left\{ \Psi, \max_{x \in \mathcal{S}_2 \setminus \mathcal{S}_1} \psi_{\mathcal{S}_1}(x) \right\} \\ &\overset{(16)}{=} \arg\max_{x \in \mathcal{S}_2 \setminus \mathcal{S}_1} \psi_{\mathcal{S}_1}(x), \end{aligned}$$

thus the proof is completed. ■

Proposition 1 for $\mathcal{S}_1 = \mathcal{D}$ and $\mathcal{S}_2 = \mathcal{H}$ yields

$$\arg\max_{x \in \mathcal{D} \cup \mathcal{H}} V_{\mathcal{D}}(x) = \arg\max_{x \in \mathcal{H} \setminus \mathcal{D}} V_{\mathcal{D}}(x). \tag{17}$$

Additionally, equation (6) implies that $\mathcal{H} \setminus \mathcal{D} = \mathcal{H}$. This statement along with equations (13) and (17) result in

$$x_{\mathcal{H}} = \arg\max_{x \in \mathcal{H}} V_{\mathcal{D}}(x) = \arg\max_{x \in \mathcal{D} \cup \mathcal{H}} V_{\mathcal{D}}(x)$$

and since $\mathcal{A} = \mathcal{D} \cup \mathcal{H}$, the pair (u_e, x_e) may be determined by solving the linear programming problem

$$x_e = \arg\max_{x \in \mathcal{A}} V_{\mathcal{D}}(x) \tag{18}$$

$$u_{\min} \leq u_e \leq u_{\max}, \quad (A - \mathbb{I})\, x_e + B u_e = 0, \tag{19}$$

where the last equation is necessary for x_e to be an equilibrium state of the closed-loop system. We assume that the problem has an acceptable solution if and only if $x_e \in \mathcal{H}$.

B. Computation of Matrix K_x

A rather straightforward approach would be to directly determine a matrix K_x that guarantees asymptotic stability of state x_e as well as positive invariance of set $\mathcal{A}$; in this case, the design requirements are immediately satisfied. However, the existence of the affine term u_e in equation (10) essentially alters the initial control bounds $u_{\min}$, $u_{\max}$ and may result in a non-feasible solution for K_x. In an effort to partially deal with this problem, we choose via a systematic procedure a

convex and compact set $\mathcal{M} \subset \mathcal{A}$ such that x_0, $x_e \in \mathcal{M}$ and compute a matrix K_x rendering state x_e asymptotically stable and set $\mathcal{M}$ positively invariant.

Considering that our method should scale well with respect to the number of states, we decided to utilize the hyperplanes induced by the facets of set $\mathcal{D}$. Let us define the index set $\mathcal{J} = \{1, 2, \ldots, q\}$, the hyperplanes

$$h_j = \left\{x \in \mathbb{R}^n : P_j^\top x = r_j\right\}, \quad \forall j \in \mathcal{J} \tag{20}$$

and the corresponding half-spaces

$$\mathcal{H}_j = \left\{x \in \mathbb{R}^n : -P_j^\top x \leq -r_j\right\}, \quad \forall j \in \mathcal{J},$$

where $P_j^\top$ denotes the j-th row of matrix P. Let $\mathcal{H}_\nu$ be an arbitrary half-space such that $x_e \in \mathcal{H}_\nu$ and $\nu \in \mathcal{J}$. We introduce the change of variables $z[t] = x[t] - x_e$ and express sets $\mathcal{A}$, $\mathcal{H}_\nu$ with respect to z, namely

$$\mathcal{A}^{(z)}(G, \bar{w}) = \{z \in \mathbb{R}^n : Gz \leq \bar{w}\}, \quad \bar{w} = w - Gx_e$$
$$\mathcal{H}_\nu^{(z)} = \left\{z \in \mathbb{R}^n : -P_\nu^\top z \leq \bar{r}_\nu\right\}, \quad \bar{r}_\nu = -r_\nu + P_\nu^\top x_e.$$

Next, we compute the value

$$V_{\mathcal{H}_\nu^{(z)}}(z_0) = \max\left\{\frac{-P_\nu^\top z_0}{\bar{r}_\nu}, 0\right\} = \frac{-P_\nu^\top z_0}{\bar{r}_\nu} = c_0,$$

where $z_0 = x_0 - x_e$ and determine a translated version of the half-space $\mathcal{H}_\nu^{(z)}$ as

$$\mathcal{H}_{\nu,c_0}^{(z)} = \left\{z \in \mathbb{R}^n : -P_\nu^\top z \leq c_0 \bar{r}_\nu\right\}, \quad \mathcal{H}_\nu^{(z)} \subseteq \mathcal{H}_{\nu,c_0}^{(z)}$$

and $z_0 \in \partial\mathcal{H}_{\nu,c_0}^{(z)}$. Now, we may define the set

$$\mathcal{M}^{(z)}(\Phi, \phi) = \mathcal{A}^{(z)} \cap \mathcal{H}_{\nu,c_0}^{(z)} = \{z \in \mathbb{R}^n : \Phi z \leq \phi\},$$

where the quantities $\Phi \in \mathbb{R}^{\omega \times n}$ and $\phi \in \mathbb{R}^\omega$ are obtained from matrix $\begin{bmatrix} G & -P_\nu^\top \end{bmatrix}^\top$ and vector $[\bar{w} \quad c_0 \bar{r}_\nu]^\top$ respectively if we omit the redundant inequalities.

Sets $\mathcal{A}^{(z)}$ and $\mathcal{H}_{\nu,c_0}^{(z)}$ are convex and closed. Hence, the same properties hold for their intersection. In addition, $\mathcal{A}^{(z)}$ is bounded and $\mathcal{M}^{(z)} = \mathcal{A}^{(z)} \cap \mathcal{H}_{\nu,c_0}^{(z)} \subseteq \mathcal{A}^{(z)}$. Therefore, set $\mathcal{M}^{(z)}$ is convex and compact. Expressing $\mathcal{M}^{(z)}$ with respect to x results in set $\mathcal{M}$, which is convex, compact and x_0, $x_e \in \mathcal{M}$. Finally, by virtue of equation (5), set $\mathcal{M}$ will also satisfy the strict inclusion $\mathcal{M} \subset \mathcal{A}$.

In order to compute matrix K_x, we examine two distinct cases.

Case 1: $x_e \in int(\mathcal{M})$. If that is the case, then we may apply Theorem 1, substituting state variable x with z, set $\mathcal{R}(F, v)$ with $\mathcal{M}^{(z)}(\Phi, \phi)$ and saturation limits $u_{\min}$, $u_{\max}$ with $\bar{u}_{\min}$, $\bar{u}_{\max}$ respectively, where $\bar{u}_{\min} = u_{\min} - u_e$ and $\bar{u}_{\max} = u_{\max} - u_e$, thus obtaining parameters K_x, ε_x.

Case 2: $x_e \in \partial\mathcal{M}$. In this case, the desired equilibrium $z = 0$ is not an interior point of set $\mathcal{M}^{(z)}$. Hence, Theorem 1 may not be directly applied. However, recent results on the linear constrained regulation problem allow us to deal with this situation as well.

Without loss of generality, we assume that the state $z = 0$ is situated on the hyperplanes

$$\Phi_l^\top z = \phi_l, \quad l \in \{1, 2, \ldots, s\}.$$

Then, the following relations hold:

$$\phi_l = 0, \quad \forall l \in \{1, 2, \ldots, s\}$$
$$\phi_l > 0, \quad \forall l \in \{s+1, s+2, \ldots, \omega\}.$$

Set $\mathcal{M}^{(z)}$ may be written as $\mathcal{M}^{(z)} = \mathcal{C} \cap \mathcal{P}$, where

$$\mathcal{C}(\Sigma) = \{z \in \mathbb{R}^n : \Sigma z \leq 0\}$$
$$\mathcal{P}(\Xi, \xi) = \{z \in \mathbb{R}^n : \Xi z \leq \xi\},$$

with matrices Σ, Ξ and vector ξ defined as

$$\Sigma = \begin{bmatrix} \Phi_1^\top \\ \Phi_2^\top \\ \vdots \\ \Phi_s^\top \end{bmatrix}, \quad \Xi = \begin{bmatrix} \Phi_{s+1}^\top \\ \Phi_{s+2}^\top \\ \vdots \\ \Phi_\omega^\top \end{bmatrix}, \quad \xi = \begin{bmatrix} \phi_{s+1} \\ \phi_{s+2} \\ \vdots \\ \phi_\omega \end{bmatrix}.$$

We may determine the matrix K_x according to the following theorem [16]:

Theorem 4: A linear, state-feedback control $u = K_x z$, where $K_x \in \mathbb{R}^{m \times n}$, renders the polyhedral set $\mathcal{M}^{(z)}(\Phi, \phi)$: (i) positively invariant with respect to the resulting closed-loop system

$$S_{cl}: \; z[t+1] = (A + BK_x)\, z[t], \quad z[0] = z_0$$

and (ii) a domain of attraction of the equilibrium $z = 0$, while satisfying control constraints $u \in [\bar{u}_{\min}, \bar{u}_{\max}]$ for initial states belonging to $\mathcal{M}^{(z)}$ and ensuring maximum rate of convergence, if and only if there exist a number $\varepsilon_x \in \mathbb{R}_+$ and matrices $H_{11} \in \mathbb{R}^{s \times s}$, $H_{21} \in \mathbb{R}^{(\omega - s) \times s}$, $H_{22} \in \mathbb{R}^{(\omega - s) \times (\omega - s)}$, $M \in \mathbb{R}^{2m \times \omega}$ such that:

$$\Sigma(A + BK_x) = H_{11}\Sigma \tag{21}$$
$$\Xi(A + BK_x) = H_{21}\Sigma + H_{22}\Xi \tag{22}$$
$$H_{22}\xi \leq \varepsilon_x \xi, \quad \varepsilon_x \leq 1 \tag{23}$$
$$H_{11} \geq \mathbb{O}, \quad H_{21} \geq \mathbb{O}, \quad H_{22} \geq \mathbb{O}, \quad M \geq \mathbb{O} \tag{24}$$
$$M \begin{bmatrix} \Sigma \\ \Xi \end{bmatrix} = \begin{bmatrix} K_x \\ -K_x \end{bmatrix}, \quad M \begin{bmatrix} 0 \\ \xi \end{bmatrix} \leq \begin{bmatrix} \bar{u}_{\max} \\ -\bar{u}_{\min} \end{bmatrix}. \tag{25}$$

If such a control exists, then it can be determined by solving the linear programming problem

$$\min_{\varepsilon_x, K_x, H_{11}, H_{21}, H_{22}, M} \{\varepsilon_x\}$$

under linear constraints (21)-(25).

V. Switching Signal Design

In the previous section, we developed an expanding policy u_x rendering set $\mathcal{M}^{(z)}$ contractive with respect to the closed-loop system. However, u_x ensures that the same property holds for all sublevel sets of $\mathcal{M}^{(z)}$, namely sets $\mathcal{M}_c^{(z)}(\Phi, c\phi)$ with $c \in (0, 1)$. In the sequel, we will exploit this property aiming to ultimately "force" the state vector inside zone $\mathcal{H}$.

All hyperplanes defined in equation (20) qualify as supporting hyperplanes of set $\mathcal{D}$. Let us now determine the maximum sublevel set of $\mathcal{M}^{(z)}$ that satisfies the inclusion $\mathcal{M}_c^{(z)} \subset \mathcal{H}_\nu^{(z)}$. Based on Farkas' Lemma, we may compute

the constant c as the solution to the linear programming problem

$$\max_{c,E}\{c\}$$

$$E\Phi = -P_\nu^\top, \quad E(c\phi) \leq \bar{r}_\nu, \quad E \geq \mathbb{O}, \quad 0 < c < 1.$$

Next, we may apply equation $z[t] = x[t] - x_e$ and obtain set $\mathcal{M}_c$, which is merely the representation of set $\mathcal{M}_c^{(z)}$ with respect to the state variable x. Clearly, the only elements $x \in \mathcal{M}_c$ that do not belong to set $\mathcal{H}$, are those that satisfy the inclusion $x \in \partial\mathcal{M}_c \cap \partial\mathcal{D}$. Consequently, we may choose parameters T, σ such that $x \in int(\mathcal{M}_c) \subset \mathcal{H}$ for all $t > T$.

In order to compute the constant T, we define the polyhedral Lyapunov function $V_{\mathcal{M}^{(z)}} : \mathbb{R}^n \to \mathbb{R}_+$ associated with set $\mathcal{M}^{(z)}$ as

$$V_{\mathcal{M}^{(z)}}(z) = \begin{cases} \max\limits_{l=1,2,\ldots,\omega} \left\{ \dfrac{(\Phi z)_l}{\phi_l} \right\}, & \text{if } \ 0 \in int\left(\mathcal{M}^{(z)}\right) \\ \\ \max\limits_{l=1,2,\ldots,\omega-s} \left\{ \dfrac{(\Xi z)_l}{\xi_l}, 0 \right\}, & \text{if } \ 0 \in \partial\mathcal{M}^{(z)} \end{cases}.$$

The control law u_x renders set $\mathcal{M}^{(z)}$ contractive, that is

$$V_{\mathcal{M}^{(z)}}(z[t+1]) \leq \varepsilon_x V_{\mathcal{M}^{(z)}}(z[t]). \tag{26}$$

By demanding $V_{\mathcal{M}^{(z)}}(z[T]) < c$ and based on inequality (26) we may obtain a lower bound of T as

$$T > \frac{\ln \dfrac{c}{V_{\mathcal{M}^{(z)}}(z_0)}}{\ln \varepsilon_x}.$$

Since the switching logic is dictated by the attacker, signal σ has to regulate, at some extent, the dwell time of the expanding controller. Specifically, the attacker may consider to relinquish the control of the system only after the state trajectory has entered a predefined set $\mathcal{M}_{c'}$ such that $\mathcal{M}_{c'}^{(z)}(\Phi, c'\phi)$ is a sublevel set of $\mathcal{M}^{(z)}$ and $c' \in (0, c]$. Consequently, the switching signal may be defined as

$$\sigma[t] = \begin{cases} 2, & \text{if} \quad t \leq \lceil T \rceil \quad \text{or} \quad \exists u^* \in \mathcal{U} \\ 1, & \text{if} \quad x[t] \in \mathcal{M}_{c'} \quad \text{and} \quad \nexists u^* \in \mathcal{U} \\ \sigma[t-1], & \text{otherwise} \end{cases}, \tag{27}$$

where $\mathcal{U} = [u_{\min}, u_{\max}]$ and u^* is a control capable of driving the state vector outside set $\mathcal{M}_c$ in one step. We state that if the attacker remains completely unaware of the contractive policy, then it is necessary to scan all the admissible values of u^*. Obviously, the feasibility problem

$$Ax[t] + Bu^* \notin int\left(\mathcal{M}_c\right), \quad u^* \in \mathcal{U} \tag{28}$$

may be decomposed into ω separate convex problems, one for every facet of $\mathcal{M}_c$.

A sufficiently small value of c', say $c' \to 0^+$, allows the attacker to control the system for all $t \geq 0$, ultimately driving the state trajectory to x_e. Divergently, the dwell time of the expanding controller decreases as the values of c' increase. For $c' = c$ equation (27) degenerates to

$$\sigma[t] = \begin{cases} 2, & \text{if} \quad t \leq \lceil T \rceil \quad \text{or} \quad \exists u^* \in \mathcal{U} \\ 1, & \text{otherwise} \end{cases}. \tag{29}$$

Equation (29) is quite important, since it provides the attacker with a switching logic that keeps the state trajectory inside set $\mathcal{H}$ for all $t > T$, while also limiting the dwell time of the expanding controller.

VI. Simulation Studies

Consider a system S described by equation (1), where matrices A, B and the initial condition x_0 are given as

$$A = \begin{bmatrix} 0.9 & 0.2 \\ 0 & 0.9 \end{bmatrix}, \quad B = \begin{bmatrix} -0.3 \\ -0.2 \end{bmatrix}, \quad x_0 = \begin{bmatrix} 2 \\ 0.5 \end{bmatrix}.$$

The set of alarm constraints $\mathcal{A}$ described by equation (3) is determined, since matrix G and vector w are given as

$$G = \begin{bmatrix} -1 & -0.1 \\ -0.5 & 0.9 \\ 0.9 & 0.4 \\ -0.2 & -1 \end{bmatrix}, \quad w = \begin{bmatrix} 2.59 \\ 2.14 \\ 3.25 \\ 2.84 \end{bmatrix}.$$

The desired operation domain $\mathcal{D}$ described by equation (4) is also determined, with matrix P and vector r selected as

$$P = \begin{bmatrix} -0.22 & 0.98 \\ -0.66 & -0.75 \\ -0.96 & 0.29 \\ 0.91 & -0.41 \\ 0.62 & 0.78 \end{bmatrix}, \quad r = \begin{bmatrix} 0.53 \\ 0.71 \\ 0.34 \\ 2.66 \\ 2.03 \end{bmatrix}.$$

Finally, the control constraints are given values $u_{\min} = -1.9$ and $u_{\max} = 3$.

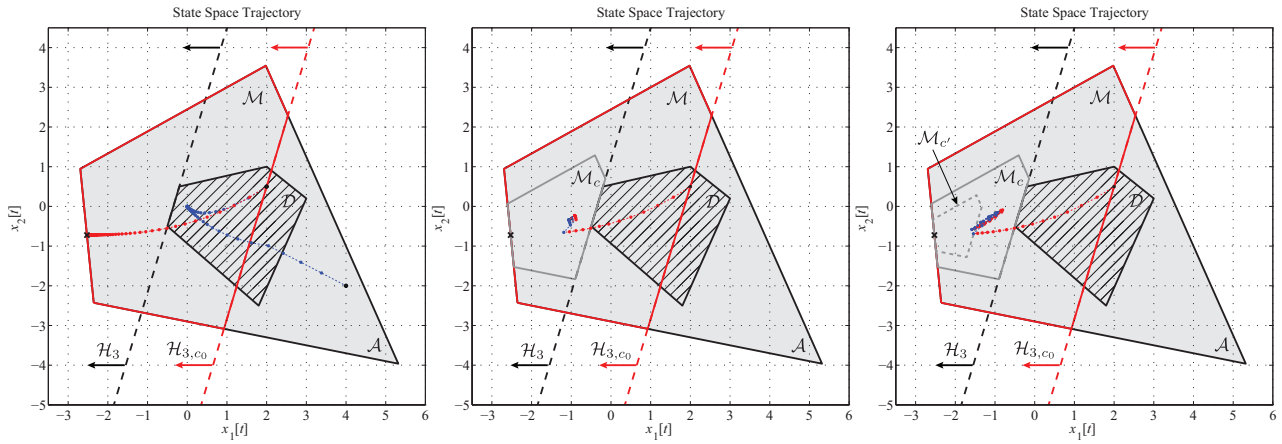
Set $\mathcal{A}$ is highlighted with light grey (●), set $\mathcal{D}$ appears hatched, and the state space trajectory is printed in blue (●) while the contractive controller is active, and in red (●) while the expanding controller is active. The boundaries of sets $\mathcal{M}$, $\mathcal{M}_c$ and $\mathcal{M}_{c'}$ are depicted with solid red, solid dark grey (●) and dashed dark grey lines respectively, whereas x_0, x_e are printed as a black bullet and a black "x" mark respectively.

A. Contractive and Expanding Controllers

In this subsection we study the behaviour of system S in the cases where only one controller is affecting it.

Case 1: Contractive controller only, that is $\sigma[t] = 1$ for all $t \geq 0$. Direct application of Theorem 1 results in gain matrices $K_{c_1} = [0.1586 \quad 0.6226]$, $K_{c_2} = [0.4128 \quad 0.7451]$ and decay rates $\varepsilon_1 = 0.8547$, $\varepsilon_2 = 0.8131$. In Fig. 2(a) we depict the state space trajectory for two separate cases. As expected, the motion emanating from the initial condition $x_0 \in \mathcal{D}$ remains inside $\mathcal{D}$ for all future time instances and converges to the origin $x = 0$ as $t \to \infty$. On the other hand, the motion emanating from the initial condition $x_0 \in \mathcal{H}$ respects the alarm constraints, enters set $\mathcal{D}$ in a finite time interval (whereupon a switching occurs) and converges to the origin $x = 0$ as $t \to \infty$.

Case 2: Expanding controller only, that is $\sigma[t] = 2$ for all $t \geq 0$. Direct application of relations (18)-(19) results in parameters $u_e = 0.3611$ and $x_e = [-2.5278 \quad -0.7222]^\top$. State x_e belongs to both half-spaces $\mathcal{H}_2$, $\mathcal{H}_3$ and we have arbitrarily chosen $\mathcal{H}_\nu = \mathcal{H}_3$. Let us observe again Fig. 2(a). Since $x_e \in \partial\mathcal{M}$, we may apply Theorem 4, thus obtaining a gain matrix $K_x = [-0.0056 \quad 0.6244]$ and a



(a) (b) (c)

Fig. 2: State vector behaviour for $\sigma(t) = 1$, $\forall t \geq 0$ and for $\sigma(t) = 2$, $\forall t \geq 0$ (left). The state response during an actual attack is also illustrated, considering different values of c', namely $c' = c$ (middle) and $c' = 0.5c$ (right).

decay rate $\varepsilon_x = 0.9380$. Clearly, the motion emanating from the initial condition $x_0 \in \mathcal{D}$ remains inside $\mathcal{M}$ for all future time instances (thus respecting the alarm constraints) and converges to the equilibrium $x = x_e$ as $t \to \infty$.

B. Adversary Control

In Figs. 2(b)-2(c) we present simulations for indicative values of c', while an actual attack on the system under consideration is taking place. We observe that in both figures the attacker policy is successful, keeping the state vector inside the zone $\mathcal{H}$ for all $t > T$; the lower bound of T being computed as $T > 11.74$. For the case where $c' = c$ and for $t > T$, the expanding controller demonstrates a minimum dwell time, being activated for a single time instant whenever necessary. Since the state space trajectory remains close to the boundary of $\mathcal{M}_c$, a chattering mode is inevitable. However, for the case where $c' = 0.5c$, the expanding controller acquires a larger dwell time and is deactivated only after $x \in \mathcal{M}_{c'}$. Finally, for the case where $c' \to 0^+$ the simulation results are exactly the same with those depicted in Fig. 2(a) (with $\sigma(t) = 2$ for all $t \geq 0$), since the possibility of a feasible solution to the problem (28) increases as the state trajectory approaches a $x_e \in \partial\mathcal{M}_c$.

VII. Conclusions

This article concerns the behaviour of a discrete-time system being under the influence of a contractive controller and a covert attacker. The two adversaries take turns on the control input of the system in an attempt to achieve two different performance objectives. Specific design procedures for their policies are presented, based on recent results on linear constrained control, while simulation studies further delineate the efficiency of our methods.

Acknowledgments

The authors thank Prof. G. Bitsoris of the Electrical & Computer Engineering Department, University of Patras, for his assistance in certain mathematical aspects.

References

[1] J.C. Hennet, Discrete-Time Constrained Systems in Control and Dynamic Systems, ed. C.T. Leondes, vol. 71. pp. 157-213, Academic Press, 1994.
[2] F. Blanchini, Set invariance in control, Automatica 35, 1999, 1747-1767.
[3] F. Blanchini, S. Miani, Set-Theoretic Methods in Control, Birkhäuser, 2008.
[4] G. Bitsoris, On the positive invariance of polyhedral sets for discrete-time systems, Systems & Control Letters 11(3), 1988a, 243-248.
[5] G. Bitsoris, Positively invariant polyhedral sets of discrete-time linear systems, International Journal of Control, 47(6), 1988b, 1713-1727.
[6] M. Vassilaki, J. C. Hennet and G. Bitsoris, Feedback control of linear discrete-time systems under state and control constraints, International Journal of Control, 1988, 47(6), 1727-1735.
[7] P. Caravani, E. De Santis, A polytopic game, Automatica, vol. 36, 2000, 973-981.
[8] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, G. Andersson, Cyber Attack in a Two-Area Power System: Impact Identification using Reachability, American Control Conference, 2010, 962-967.
[9] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, G. Andersson, A Robust Policy for Automatic Generation Control Cyber Attack in Two Area Power Network, Conference on Decision and Control, 2010, 5973-5978.
[10] F. Pasqualetti, F. Dörfler, F. Bullo, Cyber-Physical Attacks in Power Networks: Models, Fundamental Limitations and Monitor Design, IEEE Conference on Decision and Control and European Control Conference, Orlando, FL, USA, 2011, pp. 2195 - 2201.
[11] A. Teixeira, H. Sandberg, K. H. Johansson, Networked Control Systems under Cyber Attacks with Applications to Power Networks, American Control Conference, Baltimore, MD, USA, 2010, pp. 3690-3696.
[12] A. Teixeira, D. Pérez, H. Sandberg, K. H. Johansson, Attack Models and Scenarios for Networked Control Systems, Proceedings of the 1st international conference on High Confidence Networked Systems, Beijing, China, 2012, 55-64.
[13] F. Pasqualetti, F. Dörfler, and F. Bullo, Attack Detection and Identification in Cyber-Physical Systems, IEEE Transactions on Automatic Control, 58(11), 2013, pp. 2715-2729.
[14] E. Kontouras, A. Tzes, L. Dritsas, Adversary Control Strategies for Discrete-Time Systems, European Control Conference, Strasbourg, France, 2014, 2508-2513.
[15] S. Wegrzyn, J. C. Gille, P. Vidal, D. Palusinski, Introduction à l'étude de la stabilité dans les espaces métriques, Dunod, Paris, France, 1971.
[16] G. Bitsoris, S. Olaru, Further Results on the Linear Constrained Regulation Problem, Mediterranean Conference on Control and Automation, Chania, Greece, 2013, 824-830.
[17] D. Liberzon, Switching in Systems and Control, Systems & Control: Foundations & Applications, Birkhäuser, 2003.