`FlipDyn`: A game of resource takeovers in dynamical systems

Sandeep Banik and Shaunak D. Bopardikar

***Abstract*— We introduce a game in which two players with opposing objectives seek to repeatedly takeover a common resource. The resource is modeled as a discrete time dynamical system over which a player can gain control after spending a state-dependent amount of energy at each time step. We use a FlipIT-inspired deterministic model that governs which player is in control at every time step. A player's policy is the probability with which it should spend energy to gain control of the resource at a given time step. Our main results are three-fold. First, we present analytic expressions for the cost-to-go as a function of the hybrid state of the system, i.e., the physical state of the dynamical system and the binary `FlipDyn` state for any general system with arbitrary costs. These expressions are exact when the physical state is also discrete and has finite cardinality. Second, for a continuous physical state with linear dynamics and quadratic costs, we derive expressions for Nash equilibrium (NE). For scalar physical states, we show that the NE depends only on the parameters of the value function and costs, and is independent of the state. Third, we derive an approximate value function for higher dimensional linear systems with quadratic costs. Finally, we illustrate our results through a numerical study on the problem of controlling a linear system in a given environment in the presence of an adversary.**

I. Introduction

Rising automation, inexpensive computation and proliferation of the Internet of Things have made cyber-physical systems (CPS) ubiquitous in industrial control systems, home automation, autonomous vehicles, smart grids and medical devices [1], [2]. However, increased levels of connectivity and ease of operations also make CPS vulnerable to cyber and physical attacks [3], [4]. An adversarial takeover can drive the system to undesirable states or can even permanently damage the system causing disruption in services and potential loss of lives. Therefore, it becomes imperative to develop policies to continuously scan for adversarial behavior while striking a balance between operating costs and system integrity. This paper proposes an approach to model and analyze the problem of resource takeovers in CPS.

As opposed to conventional adversaries perturbing the states of the system (actuator attack) or measurements (integrity attack) [5], in this work an adversary completely takes over a resource and can transmit arbitrary values originating from the controlled resource.

There has been a lot of recent research into CPS security in the controls community. The work in [6] focuses on resilience against an adversary who can hijack and replace the control signal while remaining undetected. This idea is generalized in [7], [8] for any linear stochastic system to determine its detectability, while quantifying performance degradation. Reference [9] developed model-based observers to detect and isolate such stealthy deception attacks to make water SCADA systems resilient. The authors in [10] developed a secure estimator with a Kalman filter for CPS.

Game theory has also been extensively applied to model CPS security problems. A two-player non-zero-sum game with asymmetric information and resource constraints between a controller and a jammer was introduced in [11]. In [12], contract design was used at the physical layer to ensure cloud security quality of service. Similarly, a two-player dynamic game between a network designer and an adversary is used to determine policies to keep the infrastructure networks of a CPS protected and enable recovery under an attack [13]. A range of works in designing physical and cyber security policies using game-theoretical frameworks are presented in [14]. A non-cooperative game between a defender (contractive controller) and an adversary (expanding controller) was presented in [15], limited to finite and fixed periods of control by each player. Covert attacks competing against a contractive control subject to control and state constraints were presented in [16].

The setup in this paper is inspired by the cybersecurity game of stealthy takeover known as FlipIt [17]. FlipIT is a two-player game between an adversary and defender competing to control a shared resource such as a computing device, virtual machine or a cloud service [18]. In [19], FlipIT model is extended to a general framework of multiple resource takeovers, termed as FlipThem, where an attacker has to compromise all or only one resource to take over the entire system. The FlipIT model has also been applied to supervisory control and data acquisition (SCADA) [20] system by deriving the probability distribution of time-to-compromise the system and evaluating the impacts of insider assistance for an adversary. Largely, the FlipIT setups have been limited to a *static system*, i.e, the payoff does not change over time. In this work, we model the takeover of a *dynamical* system between an adversary and a defender.

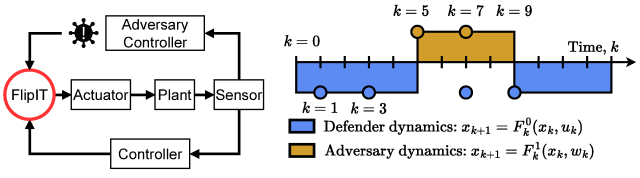
In this paper, we assume that controller policies are known and fixed for both the defender and an adversary. What is not known are the time instants at which each player should act to takeover the system. Thus, our set-up generalizes the formulation considered in [15], [16] by explicitly attaching state-dependent costs on each player.

The contributions of this paper are three-fold.

1. Game-theoretic modeling of dynamic resource takeover: We model a two-player zero-sum game between a defender and an adversary trying to takeover a dynamical system (resource), termed as the `FlipDyn` game. Given the controllers used by each player, this model accounts for state-dependent takeover costs subject to the system dynamics when controlled by either player.

2. FlipDyn control for any general system: We charac-

The authors are with the Department of Electrical and Computer Engineering at Michigan State University, East Lansing, MI, USA. Emails: baniksan@msu.edu; shaunak@egr.msu.edu. This research was supported in part by NSF Award CNS-2134076 under the Secure and Trustworthy Cyberspace (SaTC) program.



(a) (b)

Fig. 1: (a) Closed-loop system with a FlipIt setup over the control signal between the defender and adversarial control. (b) Sample sequence of the `FlipDyn` game with the defender action and takeover indicated by the blue circles and region, respectively. Similarly, the adversary action and takeover time period are indicated by the red circles and region, respectively.

terize the Nash equilibrium (NE) of the `FlipDyn` game as a function of both the continuous state of the system and the binary `FlipDyn` state. For finite cardinality of the physical state and arbitrary takeover and stage costs, we obtain the exact value and corresponding policies for the game.

3. NE for linear dynamical systems with quadratic costs: We derive the NE for a linear dynamical system with takeover and stage costs that are quadratic in the state. For scalar systems, we show that the solutions are a function of only the parameters of the system dynamics and costs. For higher dimensional systems, we provide an approximate solution for the value of the `FlipDyn` game. We illustrate our findings through two numerical examples.

The paper is organized as follows. In Section II, we formally define the `FlipDyn` game. We provide a solution methodology for any general system with arbitrary state and takeover costs in Section III. We present the analysis for linear systems with quadratic costs in Section IV. In Section V, we illustrate the efficacy of the solution applied to a linear-time invariant system. We conclude this paper and provide future directions in Section VI. Due to space limitations, we have included all proofs in the online technical report [21].

II. Problem Formulation

Consider a discrete-time dynamical system governed by

$$x_{k+1} = F_k^0(x_k, u_k), \tag{1}$$

where $k \in \mathbb{N}$ denotes the discrete time instant, $x_k \in \mathbb{R}^n$ and $u_k \in \mathbb{R}^m$ are the state and control input of the system, respectively, $F_k^0 : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ is the state transition function. We restrict our attention to a single adversary trying to gain control of the dynamical system resource (1). In particular, we assume the adversary to be located between the controller and actuator, illustrated in Figure 1a. The inclusion of an adversary modifies (1) resulting into

$$x_{k+1} = (1-\alpha_k)F_k^0(x_k, u_k) + \alpha_k F_k^1(x_k, w_k),$$

where $F_k^1 : \mathbb{R}^n \times \mathbb{R}^p \to \mathbb{R}^n$ is the state transition function under the adversary's control, $w_k \in \mathbb{R}^p$ represents the attack signal, and $\alpha_k \in \{0,1\}$ denotes a takeover of the control signal by either the adversary ($\alpha_k = 1$) or the defender ($\alpha_k = 0$), termed as the `FlipDyn` state. A takeover is mutually exclusive, i.e., only one player is in control of the system at any given time.

The control law for each player are pre-designed with different objectives – a defender's objective may be to steer the state towards an equilibrium point. In contrast, the adversary upon gaining access into the system, implements an attack policy to ensure maximum divergence of the state from the corresponding equilibrium point, while keeping the state within any defined set. In particular, we assume that

$$u_k = K_k(x), \quad w_k = W_k(x),$$

where K_k and W_k are specified state feedback control laws. These lead to the following closed-loop evolution

$$x_{k+1} = (1-\alpha_k)f_k^0(x_k) + \alpha_k f_k^1(x_k), \tag{2}$$

where $f_k^0(x_k) := F_k^0(x_k, K_k(x))$ and $f_k^1(x_k) := F_k^1(x_k, W_k(x))$.

To describe a takeover mathematically, the action $\alpha_k^j \in \{0,1\}$ denotes the kth move of the player $j \in \{0,1\}$, with $j=0$ denoting the defender, and $j=1$ as the adversary. The dynamics of this binary `FlipDyn` state based on the player's move satisfies

$$\alpha_k = \begin{cases} \alpha_{k-1}, & \text{if } \alpha_k^1 = \alpha_k^0, \\ j, & \text{if } \alpha_k^j = 1. \end{cases} \tag{3}$$

Equation (3) states that if both players act to obtain control of the resource at the same time, then their actions get nullified and `FlipDyn` state remains unchanged. However, if the resource is in control by one of the players and the other player moves to gain control at time $k+1$ while the first player does not exert control, then the `FlipDyn` state toggles. Finally, if a player is already in control and decides to move while the other player remains inactive, then the `FlipDyn` state is unchanged.

A sample instance over a finite time period is illustrated in Figure 1b, where the defender has a control at time $k=0$, followed by a takeover action at time $k=1$ and 3. The adversary takes over at time $k=5$ under a no defense action, and remains in control till time $k=9$, when the defender takes back control. Additionally, notice at time $k=7$, both the adversary and defender move to takeover, but their actions are cancelled out and therefore, the `FlipDyn` state does not change, i.e, the adversary maintains control.

The state dynamics as a function of the binary `FlipDyn` state and the `FlipDyn` dynamics are described by (2) and

$$\alpha_{k+1} = \left(\bar{\alpha}_k^0 \bar{\alpha}_k^1 + \alpha_k^0 \alpha_k^1\right)\alpha_k + \bar{\alpha}_k^0(\alpha_k^0 + \alpha_k^1), \tag{4}$$

where any variable $\bar{x} := 1 - x$. We pose the resource control problem as a zero-sum dynamic game described by the dynamics (2) and (4) over a finite time horizon of L, where the defender aims to minimize a net cost given by,

$$J(x_0, \alpha_0, \{\alpha_t^1\}, \{\alpha_t^0\}) = \sum_{t=1}^{L} g(x_t) + \bar{\alpha}_t d(x_t) - \alpha_t a(x_t), \tag{5}$$

where $g(x_t) : \mathbb{R}^n \to \mathbb{R}$ represents the state regulation cost, $d(x_t)$ and $a(x_t)$ are the instantaneous takeover costs for the defender and adversary, respectively. The notation $\{\alpha_t^j\} := \{\alpha_1^j, \ldots, \alpha_L^j\}$. In contrast, the adversary aims to maximize the cost function (5) leading to a zero-sum dynamic game, defining our *`FlipDyn` game*.

We seek to find the NE of the game defined by (5). However, a pure NE may not be guaranteed. For instance, a one-step horizon problem results into solving a 2×2 matrix game, which need not admit a pure NE. To guarantee existence of NE, we expand the set of player policies to behavioral policies – probability distributions over the space of discrete actions at each time step [22]. Specifically, let

$$y_k = \begin{bmatrix} \beta_k & 1-\beta_k \end{bmatrix}^T, \quad z_k = \begin{bmatrix} \gamma_k & 1-\gamma_k \end{bmatrix}^T \tag{6}$$

be a behavioral policy for the defender and adversary at time instant k, such that $\beta_k \in [0,1]$ and $\gamma_k \in [0,1]$, respectively. Thus, $y_k, z_k \in \Delta_2$, where Δ_2 is the probability simplex in two dimensions. The cost (5) is considered in expectation over the player policies. Over the finite horizon L, let $y_{\mathbf{L}} = \{y_1, y_2, \ldots, y_L\} \in \Delta_2^L$ and $z_{\mathbf{L}} = \{z_1, z_2, \ldots, z_L\} \in \Delta_2^L$ be the sequence of defender and adversary behavioral policies. Thus, the expected outcome of the `FlipDyn` game over the finite horizon L is

$$J_E(x_0, \alpha_0, y_{\mathbf{L}}, z_{\mathbf{L}}) := \mathbb{E}_{y_{\mathbf{L}}, z_{\mathbf{L}}}[J(x_0, \alpha_0, \{\alpha_t^1\}, \{\alpha_t^0\})], \tag{7}$$

where the expectation is computed over the distributions $y_{\mathbf{L}}$ and $z_{\mathbf{L}}$. Specifically, we seek a saddle-point solution $(y_{\mathbf{L}}^*, z_{\mathbf{L}}^*)$ in the space of behavioral policies such that $\forall (x_0, \alpha_0)$,

$$J_E(x_0, \alpha_0, y_{\mathbf{L}}^*, z_{\mathbf{L}}) \leq J_E(x_0, \alpha_0, y_{\mathbf{L}}^*, z_{\mathbf{L}}^*) \leq J_E(x_0, \alpha_0, y_{\mathbf{L}}. z_{\mathbf{L}}^*).$$

Together, the `FlipDyn` game is completely defined by the cost in (7) subject to the dynamics in (2) and (4).

III. FlipDyn Control for general systems

In this section, we first compute NE for the `FlipDyn` game. We begin by defining the value function for the `FlipDyn` game.

A. Value function

Our approach is to define a value function in each of the two `FlipDyn` states. Let $V_k^0(x)$ and $V_k^1(x)$ be the two value functions in state x at time instant k corresponding to the `FlipDyn` state of $\alpha = 0$ and 1, respectively. Then for $\alpha = 0$, we have

$$V_k^0(x) = g_k(x) + y_k^T \Xi_k^0 z_k, \tag{8}$$

where $\Xi_k^0 \in \mathbb{R}^{2\times 2}$ is the cost-to-go matrix, and the actions of the defender (row player) and adversary (column player) applied on Ξ_k^0 returns the value corresponding to the state at time $k+1$. This instantaneous payoff matrix has the form

$$\Xi_k^0 = \begin{bmatrix} V_{k+1}^0(f_k^0(x)) & V_{k+1}^1(f_k^1(x)) - a(x) \\ V_{k+1}^0(f_k^0(x)) + d(x) & V_{k+1}^0(f_k^0(x)) + d(x) - a(x) \end{bmatrix}. \tag{9}$$

The matrix entries corresponding to Ξ_k^0 are determined using the `FlipDyn` dynamics (2) and (4). $\Xi_k^0(1,1)$ corresponds to both the defender and adversary staying idle. Similarly, $\Xi_k^0(2,2)$ corresponds to the action of takeover by both the defender and adversary. The off-diagonal entries correspond to a player taking over the resource. We observe that the actions of the defender and adversary couple the value functions in each `FlipDyn` state V_k^0 and V_k^1.

The value function V_k^1 for the `FlipDyn` state $\alpha = 1$, and its corresponding cost-to-go matrix Ξ_k^1 is

$$V_k^1(x) = g_k(x) + y_k^T \Xi_k^1 z_k, \tag{10}$$

$$\Xi_k^1 = \begin{bmatrix} V_{k+1}^1\left(f_k^1(x)\right) & V_{k+1}^1\left(f_k^1(x)\right) - a(x) \\ V_{k+1}^0\left(f_k^0(x)\right) + d(x) & V_{k+1}^1\left(f_k^1(x)\right) + d(x) - a(x) \end{bmatrix}. \tag{11}$$

B. Expected Value of the `FlipDyn` game

In each `FlipDyn` state ($\alpha = \{0,1\}$), the corresponding cost-to-go matrix defines a one-step zero-sum game with the defender aiming to minimize the value function, and the adversary trying to maximize the same. When a row or column domination [22] exists, it leads to a pure policy for at least one player. However, we first show that this game does not admit dominated policies in the following result.

Lemma 1 *For any $k \in \mathbb{N}$, there is no pure policy equilibrium for the one-step zero-sum games defined by the matrices Ξ_k^0 and Ξ_k^1 under the condition*

$$V_k^1(f_k^1(x)) > V_k^0(f_k^0(x)) + \max\{d(x), a(x)\}, \tag{12}$$

Please refer to [21] for the proof.

The analysis of Lemma 1, particularly (12) provides a condition for a mixed policy NE of the one-step game. Using this condition, we recursively derive the (mixed) value at any time instant k for each binary `FlipDyn` state as summarized in Theorem 1.

Theorem 1 *Given the cost-to-go matrices* (9) *and* (11) *for $\alpha_k = 0$ and* 1*, respectively, the value of the state x at time k satisfies,*

$$V_k^0(x) = g(x) + d(x) + V_{k+1}^0(f_k^0(x)) - \frac{d(x)a(x)}{\tilde{V}_{k+1}(x)}, \tag{13}$$

$$V_k^1(x) = g(x) - a(x) + V_{k+1}^1(f_k^0(x)) + \frac{d(x)a(x)}{\tilde{V}_{k+1}(x)}, \tag{14}$$

where $\tilde{V}_{k+1}(x) := V_{k+1}^1(f_k^1(x)) - V_{k+1}^0(f_k^0(x))$. □

Given any zero-sum game matrix with no row or column domination, the unique mixed policy of the row and column player and the value of the game can be found in [23] with the complete proof in [21]

For a finite cardinality of the state x and a finite horizon L, Theorem 1 yields an exact value of the state and saddle point of the `FlipDyn` game. However, the computational and storage complexity scales undesirably for continuous state spaces. For this purpose, we will provide a parametric form of the value function for the case of linear dynamics with quadratic costs in the next section.

IV. FlipDyn Control for LQ Problems

For linear dynamics and quadratic costs, we split our analysis into two cases, a 1-dimensional and an n-dimensional system. The `FlipDyn` setup (2) reduces to

$$x_{k+1} = F_k x_k + (1-\alpha_k) B_k u_k + \alpha_k B_k w_k, \tag{15}$$

where $F_k \in \mathbb{R}^{n\times n}$ is the state transition matrix, $B_k \in \mathbb{R}^{n\times m}$ is the control matrix.

It has been shown in [24] that the optimal control law for any linear time system is achieved using state-feedback

information. Therefore, in this work, we will assume a state-feedback controller for both players of the form

$$u_k = -K_k x_k, \qquad w_k = W_k x_k, \tag{16}$$

where $K_k \in \mathbb{R}^{m\times n}, W_k \in \mathbb{R}^{m\times n}$ are possibly time varying matrices denoting the defender's and adversary's control gains, respectively. We will now simplify the recursive equations (13) and (14) under the following assumed costs.

Assumption 1 (Quadratic state-dependent costs) *The stage and takeover costs for each player satisfy*

$$g(x) = x^T Q x, \quad d(x) = x^T D x, \quad a(x) = x^T A x, \tag{17}$$

where Q, D and A are given positive definite matrices.

Under Assumption 1, the recursions in (13) and (14) yield

$$V_k^0(x) = x^T(Q+D)x + V_{k+1}^0(f_k^0(x)) - \frac{x^T D x x^T A x}{\widetilde{V}_{k+1}(x)} \tag{18}$$

$$V_k^1(x) = x^T(Q-A)x + V_{k+1}^1(f_k^1(x)) + \frac{x^T D x x^T A x}{\widetilde{V}_{k+1}(x)}, \tag{19}$$

where $\tilde{V}_{k+1}(x)$ has been defined in Theorem 1.

Assuming a parametric form for the value function corresponding to $\alpha = 0$ and 1 as,

$$V_k^0(x) := x^T P_k^0 x, \quad V_k^1(x) := x^T P_k^1 x,$$

where P_k^0 and P_k^1 are positive semi-definite matrices corresponding to the `FlipDyn` states $\alpha = 0$ and 1, respectively. Therefore, the value function (18) and (19) under this parametric form satisfy

$$V_k^0(x) = x^T(Q+D+\widetilde{B}_k^T P_{k+1}^0 \widetilde{B}_k)x - \frac{x^T D x x^T A x}{x^T \widetilde{P}_{k+1} x}, \tag{20}$$

$$V_k^1(x) = x^T(Q-A+\widetilde{W}_k^T P_{k+1}^1 \widetilde{W}_k)x + \frac{x^T D x x^T A x}{x^T \widetilde{P}_{k+1} x}, \tag{21}$$

where $\widetilde{W}_k := (F_k + B_k W_k), \widetilde{B}_k := (F_k - B_k K_k)$ and $\widetilde{P}_{k+1} := \widetilde{W}_k^T P_{k+1}^1 \widetilde{W}_k - \widetilde{B}_k^T P_{k+1}^0 \widetilde{B}_k$. This quadratic form yields the following expressions for the mixed policies of each player at time k as summarized in the following result.

Corollary 1 *For the linear dynamics* (15) *and affine controls* (16)*, under Assumption 1 the players' policies satisfy*

$$y_{k|\alpha_k=0}^*(x) = \begin{bmatrix}\hat{\beta}_k^*(x) & 1-\hat{\beta}_k^*(x)\end{bmatrix}^T, \tag{22}$$

$$z_{k|\alpha_k=1}^*(x) = \begin{bmatrix}1-\hat{\gamma}_k^*(x) & \hat{\gamma}_k^*(x)\end{bmatrix}^T, \tag{23}$$

$$z_{k|\alpha_k=0}^*(x) = 1 - z_{k|\alpha_k=1}^*(x), \quad y_{k|\alpha_k=1}^*(x) = 1 - y_{k|\alpha_k=0}^*(x),$$

where,

$$\hat{\beta}_k^* = \frac{x^T A x}{x^T \widetilde{P}_{k+1} x}, \quad 1-\hat{\gamma}_k^* = \frac{x^T D x}{x^T \widetilde{P}_{k+1} x}.$$

The terms $y_{k|\alpha_k}^*$ and $z_{k|\alpha_k}^*$ correspond to the defender's and adversary's policy for the `FlipDyn` state α_k at time k, respectively. □

Substituting β_k^* from (22) in (20), and $1-\gamma_k^*$ from (23) in (21), we obtain the following form,

$$V_k^0(x) = x^T(Q+D+\widetilde{B}^T P_{k+1}^0 \widetilde{B})x - x^T D x(\hat{\beta}_k^*(x)), \tag{24}$$

$$V_k^1(x) = x^T(Q-A+\widetilde{W}^T P_{k+1}^1 \widetilde{W})x + x^T A x(1-\hat{\gamma}_k^*(x)). \tag{25}$$

We observe that both (24) and (25) are nonlinear in x. Therefore, a quadratic parameterization cannot necessarily represent the value function with quadratic costs. However, we show that for a scalar system (1-dimensional), this parameterization is sufficient.

1) **Scalar/1-dimensional system:** The state, defense and attack costs for a scalar system simplify to

$$g(x) = gx^2, \quad d(x) = dx^2, \quad a(x) = ax^2, \tag{26}$$

where g, d and a are positive constants and $x \in \mathbb{R}$. The following result provides a closed-form expression for the NE of the `FlipDyn` game and the corresponding value of the state at time instant k.

Theorem 2 *The unique mixed Nash equilibrium at any time k for the `FlipDyn` state of $\alpha_k = 0$ for a scalar system with costs* (26) *and dynamics* (15) *is given by,*

$$y_{k|\alpha_k=0}^* = \begin{bmatrix}\dfrac{a}{\tilde{\mathbf{p}}_{k+1}} & \dfrac{\tilde{\mathbf{p}}_{k+1}-a}{\tilde{\mathbf{p}}_{k+1}}\end{bmatrix}^T, \tag{27}$$

$$z_{k|\alpha_k=0}^* = \begin{bmatrix}\dfrac{\tilde{\mathbf{p}}_{k+1}-d}{\tilde{\mathbf{p}}_{k+1}} & \dfrac{d}{\tilde{\mathbf{p}}_{k+1}}\end{bmatrix}^T. \tag{28}$$

The saddle-point value at time instant k is parameterized by,

$$\mathbf{p}_k^0 = g + (F_k - B_k K_k)^2 \mathbf{p}_{k+1}^0 + d - \frac{da}{\tilde{\mathbf{p}}_{k+1}}, \tag{29}$$

where $\tilde{\mathbf{p}}_{k+1} := (F_k + B_k W_k)^2 \mathbf{p}_{k+1}^1 - (F_k - B_k K_k)^2 \mathbf{p}_{k+1}^0$.

Similarly, for the `FlipDyn` state of $\alpha_k = 1$, the unique Nash equilibrium at time k is,

$$y_{k|\alpha_k=1}^* = \begin{bmatrix}\dfrac{\tilde{\mathbf{p}}_{k+1}-a}{\tilde{\mathbf{p}}_{k+1}} & \dfrac{a}{\tilde{\mathbf{p}}_{k+1}}\end{bmatrix}^T, \tag{30}$$

$$z_{k|\alpha_k=1}^* = \begin{bmatrix}\dfrac{d}{\tilde{\mathbf{p}}_{k+1}} & \dfrac{\tilde{\mathbf{p}}_{k+1}-d}{\tilde{\mathbf{p}}_{k+1}}\end{bmatrix}^T. \tag{31}$$

The saddle-point value at time k is parameterized by,

$$\mathbf{p}_k^1 = g + (F_k + B_k W_k)^2 \mathbf{p}_{k+1}^1 - a + \frac{da}{\tilde{\mathbf{p}}_{k+1}}, \tag{32}$$

such that (recursively) $\mathbf{p}_k^0 \geq 0$ and $(F_k + B_k W_k)^2 \mathbf{p}_{k+1}^1 \geq (F_k - B_k K_k)^2 \mathbf{p}_{k+1}^0 + \max\{d, a\}$, hold $\forall k \in \mathbb{N}$. □

Proof: [Sketch] Beginning with the cost at terminal time L and substituting (26) in Corollary 1, we obtain (27), (28) and (29). The details of the proof are found in [21]. ■

Observe that the policy for the `FlipDyn` state $\alpha = 1$ is complementary to the policy corresponding to $\alpha = 0$ indicating the need to compute the policy for any one of

the FlipDyn states. Using Theorem 2, the saddle points of the FlipDyn game for $\alpha = 0$ and 1 are,

$$J_E(x,0,y^*_{\mathbf{L}},z^*_{\mathbf{L}}) = x^{\mathrm{T}}\mathbf{p}^0_0 x, \quad J_E(x,1,y^*_{\mathbf{L}},z^*_{\mathbf{L}}) = x^{\mathrm{T}}\mathbf{p}^1_0 x. \quad (33)$$

Thus, we have obtained an exact solution for the 1-dimensional system with the parameterized value function and the player policies for both the FlipDyn states. Next, we extend this approach to derive an approximate solution for an n-dimensional system.

2) n-dimensional system: To address the nonlinearity of the value function, we first introduce an approximation that will enable recursive computation of the parameters defining the value function, thus making it independent of the state.

Theorem 3 *At any time instant $k \in \mathbb{N}$, under Assumption 1, suppose that the nonlinear terms $x^T Dx\,\hat{\beta}^*_k(x)$ and $x^T Ax(1-\hat{\gamma}^*_k(x))$ in* (24) *and in* (25) *can be upper bounded by a common quadratic form in the state, i.e.,*

$$(x^T Dx)\hat{\beta}^*_k(x) \le x^T D(\widetilde{P}_{k+1})^{-1}Ax, \quad (34)$$

$$(x^T Ax)(1-\hat{\gamma}^*_k(x)) \le x^T D(\widetilde{P}_{k+1})^{-1}Ax, \quad (35)$$

where $\widetilde{P}_{k+1} := \widetilde{W}_k^T P^1_{k+1}\widetilde{W}_k - \widetilde{B}_k^T P^0_{k+1}\widetilde{B}_k$, $\widetilde{W}_k := (F_k + B_k W_k)$ and $\widetilde{B}_k := (F_k - B_k K_k)$.

Then, the value functions corresponding to each FlipDyn state are given by $V^0_k(x) := x^T P^0_k x$, $V^1_k(x) := x^T P^1_k x$, where the matrices P^0_k and P^1_k are chosen to satisfy

$$P^0_k \preceq Q + D + \widetilde{B}_k^T P^0_{k+1}\widetilde{B}_k - D\widetilde{P}^{-1}_{k+1}A,$$
$$P^1_k \succeq Q - A + \widetilde{W}_k^T P^1_{k+1}\widetilde{W}_k + D\widetilde{P}^{-1}_{k+1}A.$$

Proof: [Sketch] Similar to the scalar case of substituting (34) and (35) into (24) and (25), respectively. Details of the proof are be found in [21]. ∎

The next result shows that conditions (34) and (35) do hold for a special class of matrices A and D.

Proposition 1 *Conditions* (34) *and* (35) *hold for any positive definite matrix $\widetilde{P}_{k+1}$ if*

$$A = aI, \text{ and } D = dI, \quad \text{for any } a,d > 0.$$

Please refer to [21] for the detailed proof.

Theorem 3 enables a recursive computation for an approximate value function independently of the state as,

$$\hat{P}^0_k = Q + D + \widetilde{B}_k^T \hat{P}^0_{k+1}\widetilde{B}_k - D\check{P}^{-1}_{k+1}A, \quad (36)$$

$$\hat{P}^1_k = Q - A + \widetilde{W}_k^T \hat{P}^1_{k+1}\widetilde{W}_k + D\check{P}^{-1}_{k+1}A, \quad (37)$$

where $\check{P}_{k+1} := \widetilde{W}_k^T \hat{P}^1_{k+1}\widetilde{W}_k - \widetilde{B}_k^T \hat{P}^0_{k+1}\widetilde{B}_k$, $\widetilde{W}_k := (F_k + B_k W_k)$ and $\widetilde{B}_k := (F_k - B_k K_k)$ such that

$$\check{P}_{k+1} \succcurlyeq A \text{ and } \check{P}_{k+1} \succcurlyeq D, \quad \forall k \in \{1,2,\ldots,L\}.$$

We initialize the parameterized value function at the terminal time instant L as,

$$\hat{P}^0_L = Q, \quad \hat{P}^1_L = \begin{cases} Q + A + \mu I, & \text{if } A \succcurlyeq D, \\ Q + D + \mu I, & \text{otherwise}, \end{cases} \quad (38)$$

where μ is a constant.

Remark 1 *Given an initial state x_0, we can create a game tree in an extensive form [22] and compute the policy for each player at every stage $k \in \{1,2,\ldots,L\}$. However, the memory requirement for such an extensive form scales exponentially in the horizon length. The memory requirement is $4^L 2^L$ and the number of zero-sum games to be solved is $4^{L-1}2^L$. In contrast, the approximation* (36) *and* (37) *has a memory requirement of $4L$ and L number of zero-sum game evaluation for the entire state space.*

V. Numerical Evaluation

In this section, we will evaluate our analytic results on a linear time-invariant system (LTI) with a linear quadratic regulator (LQR) control law used by the defender. Without any loss of generality, we make the following assumption.

Assumption 2 *The system is under the defender's control at time $k = 0$, i.e, $\alpha_0 := 0$.*

Assumption 2 is only for convenience and is reasonable to expect that the system designer would have complete control of the system upon initialization.

We will now specify the parameters of the FlipDyn game. The dynamical system is assumed to be given by

$$f^0_k(x_k) = (F - BK)x_k, \quad f^1_k(x_k) = (F + BW)x_k = Fx_k,$$

where we have assumed that the adversary's control gain $W_k = W = \mathbf{0}, \forall k \in \{1,2,\ldots,L\}$, i.e., the adversary applies zero control input commands deterring or deviating the state from reaching its equilibrium state. We use a double integrator dynamics ($n = 2$) of the form

$$f^0_k(x_k) = \left(\underbrace{\begin{bmatrix} \hat{f} & \Delta \\ 0 & \hat{f} \end{bmatrix}}_{F} - \underbrace{\begin{bmatrix} 0.5\Delta^2 \\ \Delta \end{bmatrix}}_{B} K \right) x_k, \quad f^1_k(x_k) = Fx_k,$$

where $\Delta > 0$ is the sample time. The system represents a second order system with acceleration as the control input. We obtain the defender's gain K using the LQR method. We solve the approximate parameterized value function matrices ($\hat{P}^0_k, \hat{P}^1_k, \forall k \in \{1,\ldots,L\}$) for both FlipDyn states over a horizon length $L = 100$. The minimum eigenvalue of the value function matrices are shown in Figures 2a and 2c, corresponding to $\hat{f} := 0.99$ and $\hat{f} := 1.01$, respectively.

We observe a trend of converging coefficients when $\hat{f} \le 1$, i.e., the system remains bounded upon lack of control, whereas the coefficients diverge for $\hat{f} > 1$ indicating a large incentive for an adversary in the initial time instants of the FlipDyn game. Since the player policies for the n-dimensional case are functions of state, and the FlipDyn state is a random variable, the attack and defense policies averaged over 500 independent simulations for $\hat{f} := 0.99$ and $\hat{f} := 1.01$ are shown in Figures 2b and 2d, respectively, with the initial state $x_0 = \begin{bmatrix} 0 & 1 \end{bmatrix}^T$. We observe a dynamic policy over the horizon length for the case of $\hat{f} := 0.99$, and a converging pure policy for $\hat{f} := 1.01$ for the FlipDyn state $\alpha = 0$, respectively. The converging pure policy for $\hat{f} := 1.01$ is reflective of the ever increasing value of the adversary over the horizon length.

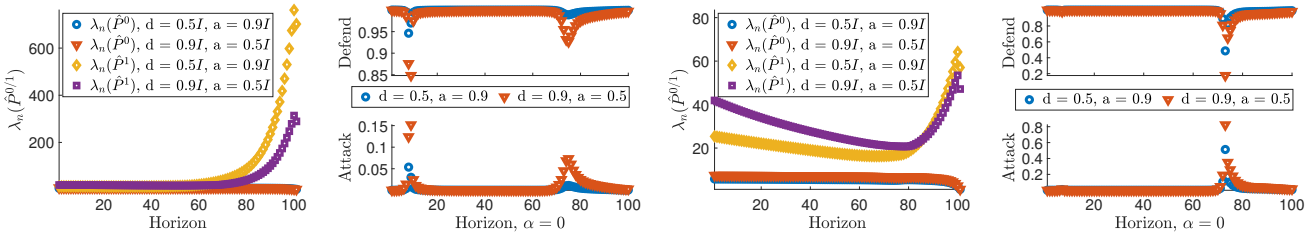


Fig. 2: (a) Minimum eigenvalue of the parameterized semi-definite value function matrices, $\lambda_n(\hat{P}^0)$ and $\lambda_n(\hat{P}^1)$ for a bounded ($\hat{f} \leq 1$) n-dimensional system. (b) Attack and defense policies corresponding to the value function in Figure 2a for the given set of state, defense and attack costs. (c) Minimum eigenvalue of the parameterized semi-definite value function matrices, $\lambda_n(\hat{P}^0)$ and $\lambda_n(\hat{P}^1)$ for an unbounded ($\hat{f} \geq 1$) n-dimensional system. (d) Attack and defense policies for the value function from Figure 2c given the `FlipDyn` state $\alpha = 0$.

VI. Conclusion and Future Directions

We introduced a resource takeover game between a defender and an adversary, in which the resource represents the control input signals of a dynamical system. We posed the takeover problem as a zero-sum two-player game over a finite time period, inspired by the well-studied FlipIT model. The payoffs for our `FlipDyn` game are modeled as state-dependent costs incurred by both the defender and adversary. We computed for the policy of each player, i.e., at what time instances should a player choose to takeover the resource. We derived the value of the physical state for a given `FlipDyn` state for any general system. In particular, we derived closed-form expressions for linear dynamical system leading to an exact value function computation for the 1-dimensional case, and an approximate value function for n-dimensional systems. Finally, we illustrate the results of the FlipDyn game on numerical examples and comment on the recovery of such a setup from loss of control.

Our current work relies on full state observability of even the `FlipDyn` state. In future works, we will infer the `FlipDyn` state of the system. We also plan to include bounded process and measurement noise and evaluate its impact on the policy of the `FlipDyn` game. Finally, we will compare the existing solution against a learning-based method for general systems and costs.

References

[1] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Design Automation Conference*. IEEE, 2010, pp. 731–736.

[2] R. Baheti and H. Gill, "Cyber-physical systems," *The Impact of Control Technology*, vol. 12, no. 1, pp. 161–166, 2011.

[3] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in *Proceedings of the 3rd Conference on Hot Topics in Security*, ser. HOTSEC'08. USA: USENIX Association, 2008.

[4] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 11, pp. 2898–2915, 2017.

[5] H. Fawzi, P. Tabuada, and S. Diggavi, "Security for control systems under sensor and actuator attacks," in *2012 IEEE 51st IEEE conference on Decision and Control (CDC)*. IEEE, 2012, pp. 3412–3417.

[6] C.-Z. Bai, F. Pasqualetti, and V. Gupta, "Security in stochastic control systems: Fundamental limitations and performance bounds," in *2015 American Control Conference (ACC)*. IEEE, 2015, pp. 195–200.

[7] ——, "Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs," *Automatica*, vol. 82, pp. 251–260, 2017.

[8] V. Katewa, C.-Z. Bai, V. Gupta, and F. Pasqualetti, "Detection of attacks in cyber-physical systems: Theory and applications," in *Safety, Security and Privacy for Cyber-Physical Systems*. Springer, 2021, pp. 79–98.

[9] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems - Part II: Attack detection using enhanced hydrodynamic models," *IEEE Transactions on Control Systems Technology*, vol. 21, no. 5, pp. 1679–1693, 2013.

[10] Y. H. Chang, Q. Hu, and C. J. Tomlin, "Secure estimation based kalman filter for cyber–physical systems against sensor attacks," *Automatica*, vol. 95, pp. 399–412, 2018.

[11] A. Gupta, C. Langbort, and T. Başar, "Dynamic games with asymmetric information and resource constrained players with applications to security of cyberphysical systems," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 71–81, 2016.

[12] J. Chen and Q. Zhu, "Security as a service for cloud-enabled Internet of controlled things under advanced persistent threats: a contract design approach," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2736–2750, 2017.

[13] J. Chen, C. Touati, and Q. Zhu, "A dynamic game approach to strategic design of secure and resilient infrastructure network," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 462–474, 2019.

[14] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 46–65, 2015.

[15] E. Kontouras, A. Tzes, and L. Dritsas, "Adversary control strategies for discrete-time systems," in *2014 European Control Conference (ECC)*. IEEE, 2014, pp. 2508–2513.

[16] ——, "Covert attack on a discrete-time system with limited use of the available disruption resources," in *2015 European Control Conference (ECC)*. IEEE, 2015, pp. 812–817.

[17] M. Van Dijk, A. Juels, A. Oprea, and R. L. Rivest, "Flipit: The game of stealthy takeover," *Journal of Cryptology*, vol. 26, no. 4, pp. 655–713, 2013.

[18] K. D. Bowers, M. v. Dijk, R. Griffin, A. Juels, A. Oprea, R. L. Rivest, and N. Triandopoulos, "Defending against the unknown enemy: Applying Flipit to system security," in *International Conference on Decision and Game Theory for Security*. Springer, 2012, pp. 248–263.

[19] A. Laszka, G. Horvath, M. Felegyhazi, and L. Buttyán, "FlipThem: Modeling targeted attacks with FlipIt for multiple resources," in *International Conference on Decision and Game Theory for Security*. Springer, 2014, pp. 175–194.

[20] Z. Liu and L. Wang, "FlipIt Game Model-Based Defense Strategy Against Cyberattacks on SCADA Systems Considering Insider Assistance," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2791–2804, 2021.

[21] S. Banik and S. D. Bopardikar, "FlipDyn: A game of resource takeovers in dynamical systems," 2022. [Online]. Available: https://arxiv.org/abs/2209.05574

[22] J. P. Hespanha, *Noncooperative game theory: An introduction for engineers and computer scientists*. Princeton University Press, 2017.

[23] S. Banik and S. D. Bopardikar, "Secure route planning using dynamic games with stopping states," in *2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 2020, pp. 2404–2409.

[24] H. Kwakernaak and R. Sivan, *Linear optimal control systems*. Wiley-interscience New York, 1972, vol. 1.