Hybrid Moving Controller: Modified Hybrid Moving Target Defense with Stability Guarantees

Mojtaba Kaheni, Alessandro Vittorio Papadopoulos

***Abstract*— This paper introduces a novel approach, which we refer to as *hybrid moving controller*, designed to ensure closed-loop stability while eliminating the requirement for synchronization between the plant and control unit. In our proposed method, the controller is time-varying and moves the closed-loop eigenvalues along radial trajectories originating from the origin. The sequence of controllers is assumed to be kept confidential from potential adversaries. Given that this moving controller renders the overall closed-loop system time-varying, maintaining the eigenvalues within the unit circle alone is insufficient to guarantee stability. As a result, we explore stability through the lens of contraction theory and present criteria for the sequence of controllers to ensure stability.**

I. Introduction

Cyber-physical systems (CPS) play a pivotal role in our modern lives, seamlessly integrating the digital and physical worlds to enhance efficiency, safety, and convenience across various domains. These systems, which combine computer-based intelligence with physical processes, are at the heart of numerous critical applications, and their importance continues to grow. In the realm of transportation, CPS enables autonomous vehicles that promise safer and more efficient travel [1]. They optimize traffic flow [2] and decrease fuel consumption [3]. In healthcare, CPS assists in remote patient monitoring and developing smart medical devices, revolutionizing healthcare delivery and patient outcomes [4]. In power grids, CPS has numerous applications in demand response [5], integration of renewable energy resources [6], and energy storage management [7], [8].

Alongside the numerous advantages CPSs can bring our lives, they are more vulnerable to cyberattacks than their traditional counterparts. This increased vulnerability arises from CPSs typically consisting of many heterogeneous components that need to communicate and collaborate. We can highlight several notable examples of cyberattacks on real-world CPSs, including Stuxnet [9], which targeted Iran's nuclear enrichment facilities; BlackEnergy [10], which aimed at Ukraine's power grid; and Trisis [10], which attacked a petrochemical plant in Saudi Arabia.

A crucial step in safeguarding CPSs against cyberattacks is *intrusion detection*. The goal of this phase is to detect anomalous behaviors in the system that may have occurred as a result of a cyberattack. Traditional methods for intrusion detection include physical watermarking [11], in which the defender intentionally modifies the control inputs to generate authentication perturbations, AI-based intrusion detectors [12], and encryption [13].

In addition to the mentioned approaches, *Moving Target Defense* has recently attracted significant attention in the research community. This intrusion detection method was initially introduced in [14] and subsequently expanded upon in additional studies [15], [16], [17]. In the context of moving-target, the defender introduces dynamic changes within the control system by incorporating time-varying parameters. These parameters are known to the defender but remain unknown to the attacker. The dynamic variations over time act as a *moving target*, changing rapidly enough to hinder potential adaptive adversaries from effectively identifying the system. Implementing the moving target approach in practical applications such as power grids [18] has shown promising results. Therefore, it seems beneficial to delve into more details and explore opportunities for possible improvements.

One of the primary practical concerns when implementing moving target defense is closed-loop stability. In control theory, achieving closed-loop stability at each time step does not guarantee overall stability in a time-varying discrete system. Specifically, unpredictable or erratic changes in closed-loop eigenvalues can lead to instability. However, in the context of moving target defense, we desire unpredictable behavior in the closed-loop poles. This is because we want the moving target to avoid following a consistent pattern that could be learned and predicted by potential attackers. In this article, our objective is to outline a method for selecting closed-loop pole locations that ensure system stability, regardless of the irregular switching in the hybrid moving target defense strategy.

Another barrier to the practical implementation of hybrid moving target defense is the need for synchronization between the plant and intrusion detection units. This paper investigates the possibility of transferring the system's time-varying features to the controller unit, which is typically located in the same place as the intrusion detection unit. This significantly improves the convenience and reliability of synchronization in practical applications.

A. Statement of Contributions

In summary, this article's main contributions include:

- Introduction of a modified moving target defense with stability guarantees.
- Proposal of a restructured format for implementing hybrid moving target defense, which is called hybrid

This work was supported by the Swedish Research Council (VR) via the project "Pervasive Self-Optimizing Computing Infrastructure (PSI)", and by the Knowledge Foundation (KKS) via the projects FIESTA and SACSys.

M. Kaheni and A. V. Papadopoulos are affiliated with Mälardalen University, Västerås, Sweden. e-mail: mojtaba.kaheni@mdu.se, alessandro.papadopoulos@mdu.se.

moving controller in this paper, removing the necessity for synchronization between the plant and the control center.

B. Organization

Section II reviews the basic structure of the hybrid moving-target approach. The hybrid moving controller approach is presented in Section III. Section IV provides the stability analysis of moving controller defense, and finally, concluding remarks are provided in Section V.

C. Notation

Throughout this paper, we use the symbols $\mathbb{N}$, $\mathbb{R}$ and $\mathbb{C}$ to represent the sets of integers, real numbers, and complex numbers respectively. Scalars are denoted as x, while $\mathbf{x}$ and $\mathbf{X}$ represent a (column) vector and a matrix, respectively. Additionally, $\mathbf{I}_i$ represents the $i \times i$ identity matrix, $\mathbf{A}_i^{cf}$ denotes an $i \times i$ square matrix in companion form, and $\mathbf{e}_i^j$ is a $j \times 1$ unit elementary vector with a 1 in the i-th row. The symbol $*$ denotes arbitrary vectors or matrices. For instance, $*$, $*_i$, and $*_{i\times j}$ represent a scalar, a $i \times 1$ vector, and a $i \times j$ matrix with arbitrary values, respectively. $\mathbf{0}_{i\times j}$ and $\mathbf{1}_{i\times j}$ represent all-zeros and all-ones matrices, respectively. $\mathbf{0}_i$ and $\mathbf{1}_i$ represent all-zeros and all-ones $i \times 1$ vectors. Finally sets are denoted by uppercase letters, e.g., X, and $\mathrm{diag}\{x_1, \ldots, x_n\}$ denotes a diagonal matrix with the elements $x_1, \ldots, x_n$ on its diagonal.

II. Review of Previous Studies

This section reviews the basic concept of hybrid moving target defense introduced in [16], [17]. Consider that the dynamics of the plant under control can be modeled as a linear time-invariant (LTI) system, as follows:

$$\begin{aligned} \mathbf{x}_{k+1} &= \mathbf{A}\mathbf{x}_k + \mathbf{B}\mathbf{u}_k + \omega_k \\ \mathbf{y}_k &= \mathbf{C}\mathbf{x}_k + \nu_k \end{aligned}, \tag{1}$$

where $k \in \mathbb{N}$ is the index for numbering samples, $\mathbf{x} \in \mathbb{R}^n$ is the state, $\mathbf{u} \in \mathbb{R}^m$ represents the input, and $\mathbf{y} \in \mathbb{R}^p$ denote the output of the system. Furthermore, $\omega \sim \mathcal{N}(0, \mathbf{N})$ and $\nu \sim \mathcal{N}(0, \mathbf{Q})$ are independent and identically distributed (i.i.d) Gaussian process and sensor noise, respectively. We assume that $(\mathbf{A}, \mathbf{B})$ and $(\mathbf{A}, \mathbf{Q}^{\frac{1}{2}})$ are stabilizable, $(\mathbf{A}, \mathbf{C})$ is detectable, and $\mathbf{N} \succ 0$.

In the hybrid moving target approach, we consider that the adversary has detailed system knowledge and can perform integrity attacks and manipulate all outputs. However, the input signals are assumed to be trustworthy. Therefore, (1) is reshaped after an attack as follows:

$$\begin{aligned} \mathbf{x}_{k+1} &= \mathbf{A}\mathbf{x}_k + \mathbf{B}\mathbf{u}_k + \omega_k \\ \mathbf{y}_k^A &= \mathbf{C}\mathbf{x}_k + \mathbf{D}\mathbf{d}_k + \nu_k \end{aligned}. \tag{2}$$

In (2), the term $\mathbf{D}\mathbf{d}(k)$ models the attack. When $\mathbf{D} = \mathbf{I}_p$, it implies that the transmitted data of all sensors can be manipulated by adding the respective index of $\mathbf{d}(k)$. Therefore, if sensor i is trustworthy, the ith row of $\mathbf{D}$ will consist of all zeros. Furthermore, $\mathbf{y}(k)$ is changed to $\mathbf{y}^A(k)$ to clarify that the adversary manipulates the output.

The central concept of the hybrid moving target approach involves dynamically altering the system matrices over time. This sequence of time-varying matrices is assumed to be accessible to the intrusion detection unit while remaining concealed from potential attackers. In other words, the system dynamics can be expressed as follows:

$$\begin{aligned} \mathbf{x}_{k+1} &= \mathbf{A}_k\mathbf{x}_k + \mathbf{B}_k\mathbf{u}_k + \omega_k \\ \mathbf{y}_k &= \mathbf{C}_k\mathbf{x}_k + \nu_k \end{aligned}. \tag{3}$$

Here, the matrices $(\mathbf{A}_k, \mathbf{B}_k, \mathbf{C}_k)$ belong to a set denoted as $\Gamma = \{(\mathbf{A}1, \mathbf{B}1, \mathbf{C}1), \ldots, (\mathbf{A}l, \mathbf{B}l, \mathbf{C}l)\}$. While Γ may be known to potential adversaries, the specific realizations of these system matrices remain undisclosed. Let us denote the information available to the defender and the attacker at time step k as Ψ_k^D and Ψ_k^A, respectively. In summary

$$\begin{aligned} \Psi_k^D &= \{\mathbf{A}_{\{0:k\}}, \mathbf{B}_{\{0:k\}}, \mathbf{C}_{\{0:k\}}, \mathbf{u}_{\{0:k\}}, \mathbf{y}_{\{0:k\}}^A, f(\omega_k, \nu_k)\}, \\ \Psi_k^A &= \{\Gamma, \mathbf{u}_{\{0:k\}}, \mathbf{y}_{\{0:k\}}^A, \mathbf{D}\mathbf{d}_{\{0:k\}}, f(\omega_k, \nu_k)\}. \end{aligned} \tag{4}$$

As discussed in [16], [17], first, we need to perform a posteriori state estimation and subsequently compute the bias in the normalized residues, denoted as $\Delta\mathbf{r}_k$. Since the objective in [16], [17] is to identify malicious sensors, which is independent of the control input, the authors disregard the control input and let $\mathbf{B}_k$ be constant. Therefore, (2) in the deterministic case can be rewritten as

$$\begin{aligned} \mathbf{x}_{k+1} &= \mathbf{A}_k\mathbf{x}_k, \\ \mathbf{y}_k^A &= \mathbf{C}_k\mathbf{x}_k + \mathbf{D}\mathbf{d}_k \end{aligned}. \tag{5}$$

Let Λ^i be the set that contains all eigenvalues of $\mathbf{A}i$. It is proved in [16], [17] that the following design recommendations,

- $\forall i, j \in \{1, \ldots, l\}$, $\Lambda^i \cap \Lambda^j = \emptyset$.
- The system matrices $(\mathbf{A}_k, \mathbf{C}_k)$ are periodically change after every $\kappa \geq 2n$ time steps.
- Let $\{l_k\}$ be a sequence where $l_k \in \{1, \ldots, l\}$. Let q_k denote the indices of a sub-sequence, then

$$\Pr\left((\mathbf{A}q_k, \mathbf{C}q_k) = (\mathbf{A}l_k, \mathbf{C}l_k), \forall k\right) = 0.$$

- the pair $(\mathbf{A}i, \mathbf{C}i)$ is observable for all $i \in \{1, \ldots, l\}$.
- For all $i \in \{1, \ldots, l\}$, $0 \notin \Lambda^i$.

when fulfilled, the bias in the residues grows unbounded in the event of an attack. Therefore, anomalies can be detected by monitoring the value of $\Delta\mathbf{r}(k)$. Fig. 1 illustrates the block diagram depicting the implementation of a hybrid moving target approach within the framework of a CPS.

III. Hybrid Moving Controller

As discussed in Section I, stability guarantees and synchronization are primary concerns in the practical implementation of hybrid moving target defense. To address these concerns, inspired by radial pole path (RPP) results in variable structure control [19], [20], [21], [22], we aim to

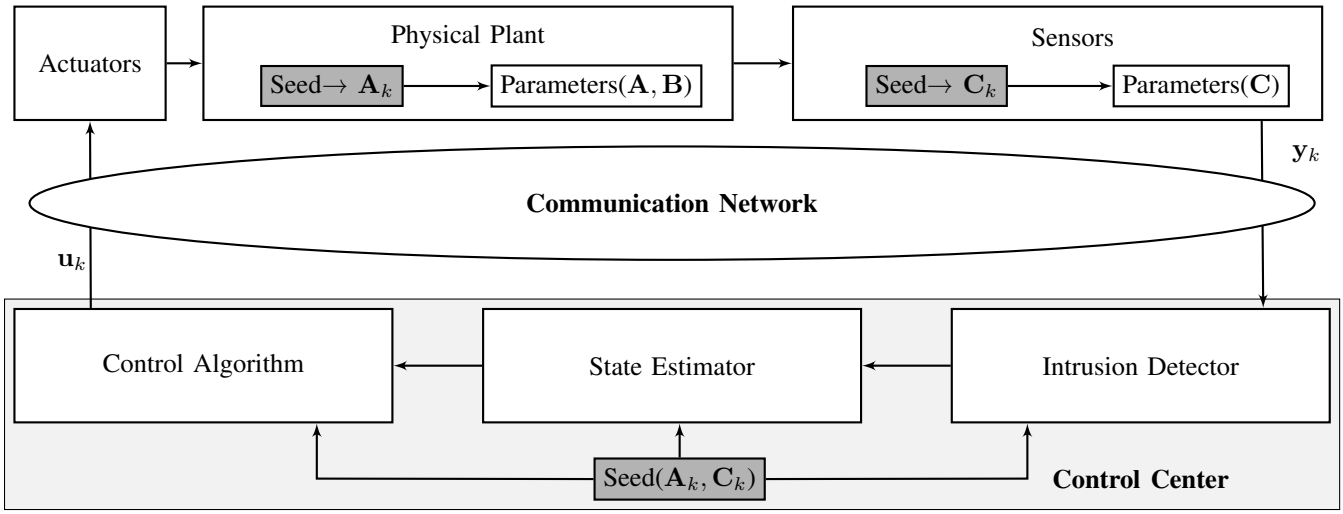

Fig. 1. Block diagram of hybrid moving target implementation on CPS.

design a controller that randomly moves the closed-loop poles on radial paths. Subsequently, we shall guarantee the stability of the time-varying system using the contraction theory. To achieve this goal, we begin by pole placement in multi-input multi-output (MIMO) LTI systems.

A. Pole Placement in MIMO LTI Systems

To continue our mathematical treatments, we need to impose the following assumption.

Assumption 1: The LTI system introduced in (1) is controllable and transformable to Frobenius canonical form. ■

By Assumption 1, (1) can be transformed to Frobenius canonical form as:

$$\mathbf{z}_{k+1} = \mathbf{A}^F \mathbf{z}_k + \mathbf{B}^F \mathbf{u}_k + \omega_k^F \quad , \tag{6}$$

where

$$\mathbf{A}^F = \mathbf{Q}^{-1}\mathbf{A}\mathbf{Q} = \begin{bmatrix} \mathbf{A}_{\mu_1}^{cf} & \underset{*_{1\times\mu_2}}{\mathbf{0}_{(\mu_1-1)\times\mu_2}} & \dots & \underset{*_{1\times\mu_m}}{\mathbf{0}_{(\mu_1-1)\times\mu_m}} \\ \underset{*_{1\times\mu_1}}{\mathbf{0}_{(\mu_2-1)\times\mu_1}} & \mathbf{A}_{\mu_2}^{cf} & \dots & \underset{*_{1\times\mu_m}}{\mathbf{0}_{(\mu_2-1)\times\mu_m}} \\ \vdots & \vdots & \ddots & \vdots \\ \underset{*_{1\times\mu_1}}{\mathbf{0}_{(\mu_m-1)\times\mu_1}} & \underset{*_{1\times\mu_2}}{\mathbf{0}_{(\mu_m-1)\times\mu_2}} & \dots & \mathbf{A}_{\mu_m}^{cf} \end{bmatrix}, \tag{7}$$

$$\mathbf{B}^F = \mathbf{Q}^{-1}\mathbf{B} = \begin{bmatrix} \mathbf{e}_{\mu_1}^{\mu_1} & \underset{*}{\mathbf{0}_{(\mu_1-1)}} & \dots & \underset{*}{\mathbf{0}_{(\mu_1-1)}} \\ \mathbf{0}_{\mu_2} & \mathbf{e}_{\mu_2}^{\mu_2} & \dots & \underset{*}{\mathbf{0}_{(\mu_2-1)}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0}_{\mu_m} & \mathbf{0}_{\mu_m} & \dots & \mathbf{e}_{\mu_m}^{\mu_m} \end{bmatrix}, \tag{8}$$

μ_i denotes the controllability index corresponding to the i-th column of $\mathbf{B}$, $\mathbf{Q}$ is the transformation matrix, and the other parameters are as introduced in Section I-C. We aim to design a state feedback controller denoted as $\mathbf{K}$. This matrix will be employed in the closed-loop system defined by $\mathbf{z}_{k+1} = \mathbf{A}^c\mathbf{z}_k$, where $\mathbf{A}^c = \mathbf{A}^F + \mathbf{B}^F\mathbf{K}$. The goal is to ensure this closed-loop system exhibits the desired characteristic polynomial.

Let us define the controllability matrix by

$$\mathbf{R} = \left[\mathbf{b}_1^F, \mathbf{A}^F\mathbf{b}_1^F, \dots, (\mathbf{A}^F)^{\mu_1-1}\mathbf{b}_1^F, \dots, \mathbf{b}_m^F, \dots, (\mathbf{A}^F)^{\mu_m-1}\mathbf{b}_m^F\right], \tag{9}$$

where $\mathbf{b}_i^F$ represents the i-th column of $\mathbf{B}^F$. In addition, let

$$\mathbf{q}_d = \mathbf{e}_{w_d}^{n\,\intercal}\mathbf{R}^{-1}, \quad w_d = \sum_{i=1}^{d}\mu_i, \quad d = 1, \dots, m. \tag{10}$$

Then the matrices $\mathbf{A}^F$ and $\mathbf{B}^F$ can be partitioned as [23]:

$$\mathbf{A}^F = \mathbf{A}^{P_0} + \mathbf{A}^{P_1}(\mathbf{A}^{P_2} - \mathbf{A}^{P_3}), \tag{11}$$

$$\mathbf{B}^F = \mathbf{A}^{P_1}\mathbf{B}^{P_1}, \tag{12}$$

where $\mathbf{A}^{P_0} \in \mathbb{R}^{n\times n}$, $\mathbf{A}^{P_1} \in \mathbb{R}^{n\times m}$, $\mathbf{A}^{P_2} \in \mathbb{R}^{m\times n}$, $\mathbf{A}^{P_3} \in \mathbb{R}^{m\times n}$, and $\mathbf{B}^{P_1} \in \mathbb{R}^{m\times m}$ are

$$\mathbf{A}^{P_0} = \begin{bmatrix} \mathbf{0}_{(n-1)} & \mathbf{I}_{n-1} \\ & \mathbf{0}_{1\times n} \end{bmatrix}, \tag{13}$$

$$\mathbf{A}^{P_1} = \mathrm{diag}\{\mathbf{e}_{\mu_1}^{\mu_1}, \mathbf{e}_{\mu_2}^{\mu_2}, \dots, \mathbf{e}_{\mu_m}^{\mu_m}\}, \tag{14}$$

$$\mathbf{A}^{P_2} = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}, \quad \alpha_i = \mathbf{q}_i\left(\mathbf{A}^F\right)^{\mu_i}, \tag{15}$$

$$\mathbf{A}^{P_3} = \begin{bmatrix} \mathbf{0}_{(m-1)}, & \mathbf{DE}, & \mathbf{0}_{(m-1)\times(\mu_m-1)} \\ & \mathbf{0}_{1\times n} & \end{bmatrix}, \tag{16}$$

where

$$\mathbf{DE} = \mathrm{diag}\{\mathbf{e}_{\mu_1}^{\mu_1\,\intercal}, \dots, \mathbf{e}_{\mu_m-1}^{\mu_m-1\,\intercal}\}, \tag{17}$$

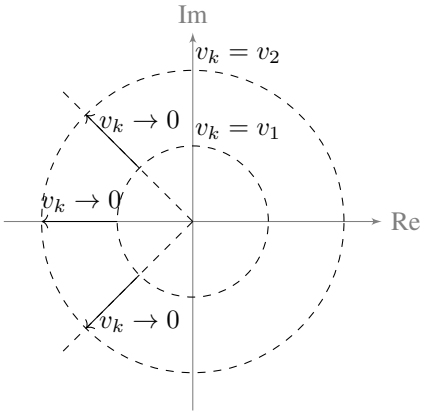

Fig. 2. A sample of radial pole paths in a third-order system ($v_2 < v_1$).

and finally

$$\mathbf{B}^{P_1} = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix}, \quad \beta_i = \mathbf{q}_i \left(\mathbf{A}^F\right)^{\mu_i - 1} \mathbf{B}^F, \tag{18}$$

If we follow the design procedure in [23], the desirable $\mathbf{K}$ is given by:

$$\mathbf{K} = (\mathbf{B}^{P_1})^{-1}(\mathbf{A}^{P_4} - \mathbf{A}^{P_2}). \tag{19}$$

There are various possible selections of $\mathbf{A}^{P_4}$ that guarantee the location of poles at the desired locations. One possibility is that $\mathbf{A}^{P_4}$ divides the desired pole locations among Frobenius blocks so that the largest eigenvalue lies within the smallest block. Consider the desired characteristic polynomial, $P(z)$, factored into m polynomials $P^i(z)$, with a degree of μ_i:

$$P(z) = \prod_{i=1}^{m} P^i(z), \tag{20}$$

$$P^i(z) = z^{\mu_i} + p^i_{\mu_i - 1} z^{\mu_i - 1} + \cdots + p^i_1 z + p^i_0, \tag{21}$$

then, if for $i = 1, \ldots, m$

$$\mathbf{p}^i = \begin{bmatrix} p^i_0, & p^i_1, & \ldots, & p^i_{\mu_i - 2}, & p^i_{\mu_i - 1} \end{bmatrix}, \tag{22}$$

The following $\mathbf{A}^{P_4}$, when inserted into (19), can potentially result in the desired closed-loop characteristic polynomial as described in (20).

$$\mathbf{A}^{P_4} = \mathbf{A}^{P_3} + \begin{bmatrix} -\mathbf{p}^1 & & \mathbf{0}_{1\times(n-\mu_1)} \\ \mathbf{0}_{1\times\mu_1} & -\mathbf{p}^2 & \mathbf{0}_{1\times(n-\mu_1-\mu_2)} \\ \vdots & \ddots & \vdots \\ \mathbf{0}_{1\times(n-\mu_m)} & & -\mathbf{p}^m \end{bmatrix}. \tag{23}$$

By implementing the controller designed in (19), $\mathbf{A}^c = \mathbf{A}^F + \mathbf{B}^F\mathbf{K}$ will be in Frobenius canonical form where $\Lambda^F_i = \mathrm{eig}\left(\mathbf{A}^{cf}_{\mu_i}\right)$ are the roots of $P^i(z)$.

B. Moving Controller

At this step, we assume that we are interested in adding a parameter in our feedback controller at each time step k, such as v_k, that allows us to move the closed loop poles along radial paths starting from the origin, as depicted in Fig. 2. This objective can be achieved by modifying (22) as follows [24]:

$$\mathbf{p}^i_{v_k} = \left[p^i_0 v_k^{-\mu_i}, p^i_1 v_k^{-(\mu_i - 1)}, \ldots, p^i_{\mu_i - 2} v_k^{-2}, p^i_{\mu_i - 1} v_k^{-1}\right], \tag{24}$$

With these modifications, the state feedback controller becomes a function of the parameter v_k, denoted as $\mathbf{K}(v_k)$. In this context, the value of v_k plays a crucial role in determining the precise location of the closed-loop poles. i.e. $\Lambda_i \to v_k^{-1}\Lambda_i$ by (24).

Taking into account (6) and the design recommendations provided for hybrid moving target in Section II, it becomes evident that if $\mathbf{C}^F$ is chosen such that the pair $(\mathbf{A}^c(v_k), \mathbf{C}^F)$, where $\mathbf{A}^c(v_k) = \mathbf{A}^F + \mathbf{B}^F\mathbf{K}(v_k)$, is observable, then all the necessary design criteria are met. Therefore, It would be possible to remove the requirement for synchronization between the plant and the control center and, instead, detect anomalies solely based on the information available at the control center unit as depicted in Fig. 3.

The design recommendations of the hybrid moving controller approach simplify the design recommendations of hybrid moving target defense as follows.

Design Recommendations:

- Design $\mathbf{K}(v_k)$ such that all eigenvalues of $\mathbf{A}^c(v_k)$ become distinct and inside the unit circle for $v_k = 1$.
- At each time step k find $v_{k+1} \in \left[v^{\min}_{k+1}, v^{\max}_{k+1}\right]$ that guarantees the stability of the system (will be discussed in Section IV).
- The system matrices $(\mathbf{A}^c(v_k), \mathbf{C}^F)$ periodically change after every $\kappa \geq 2n$ time steps by changing v_k.
- The pair $(\mathbf{A}^c(v_k), \mathbf{C}^F)$ is observable.

IV. Stability Analysis

In this section, we aim to establish guarantees for the stability of the hybrid moving controller approach using contraction theory [25]. First, we recall a lemma generally proposed for nonlinear time-varying discrete systems in [26]. However, for the sake of simplicity, we have restricted it to linear time-varying systems and expressed it in our notations.

Lemma 1: The system $\mathbf{z}_{k+1} = \mathbf{A}^c(v_k)\mathbf{z}_k$ is globally and exponentially stable if there exists a regular map, $\mathbf{\Theta}_k$, such that

$$\exists \beta > 0, \quad \mathbf{F}_k^\intercal \mathbf{F}_k - \mathbf{I}_n \leq -\beta \mathbf{I}_n < 0,$$

where $\mathbf{F}_k = \mathbf{\Theta}_{k+1}\mathbf{A}^c(v_k)\mathbf{\Theta}_k^{-1}$. ■

In the following Theorem, we employ Lemma 1 to establish the sufficient condition for the sequence $\boldsymbol{v}_{1:k} \triangleq \{v_1, \ldots, v_k\}$ to ensure system stability using contraction theory.

Theorem 1: Assume that all eigenvalues of $\mathbf{A}^c(v_k)$ are distinct and inside the unit circle for $v_k = 1$, and $v_1 \geq 1$.

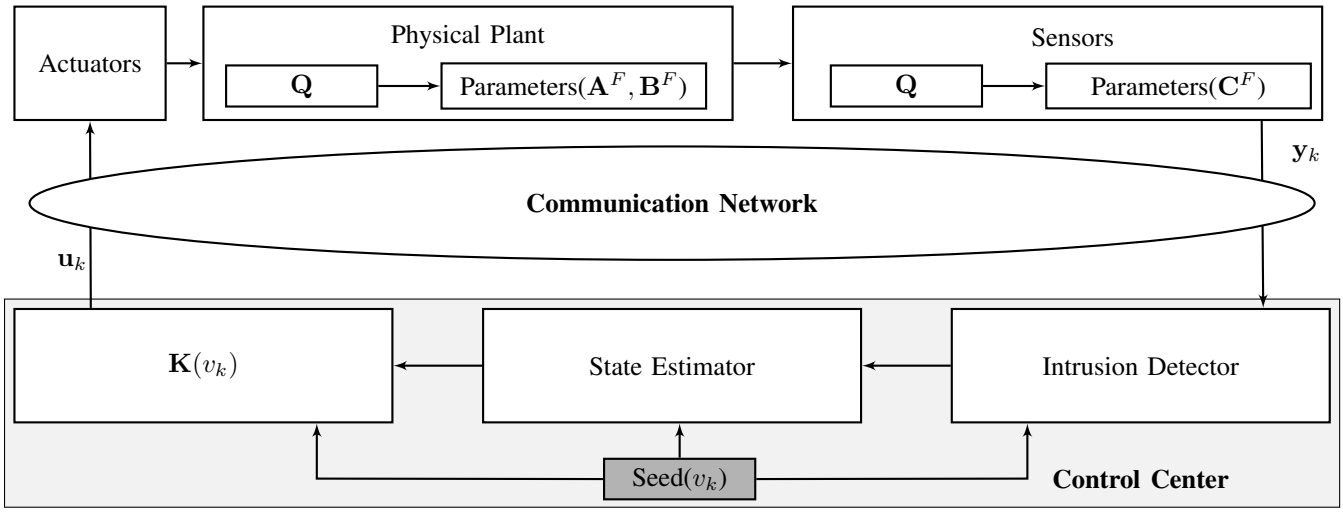

Fig. 3. Block diagram of hybrid moving controller.

Then if

$$\forall k \geq 2, \begin{cases} v_k \geq 1, \quad \text{and,} \\ v_k^{-1} \left(\frac{v_{k+1}}{v_{k-1}} \right)^{(n-1)} \leq 1, \end{cases}$$

then the closed loop dynamic $\mathbf{z}_{k+1} = \mathbf{A}^c(v_k)\mathbf{z}_k$ is globally and exponentially stable, when $\mathbf{A}^c(v_k) = \mathbf{A}^F + \mathbf{B}^F\mathbf{K}(v_k)$ and $\mathbf{K}(v_k)$ is design as discussed in Section III. ■

Proof: First, assume that $\Lambda = \{\lambda_1, \ldots, \lambda_n\}$ represents the set of all distinct eigenvalues of the system, $\mathbf{A}^c(v_k)$, when $v_k = 1$. We can assume this system is represented in canonical controllable form. Recall from linear control theory that when a system is in canonical controllable form, $\mathbf{T} \in \mathbb{C}^{n \times n}$ defined by:

$$\mathbf{T} = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \lambda_1 & \lambda_2 & \ldots & \lambda_n \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{n-1} & \lambda_2^{n-1} & \ldots & \lambda_n^{n-1} \end{bmatrix}. \tag{25}$$

is a transformation matrix that transforms $\mathbf{A}^c(1)$ into $\mathbf{DA}^c(1) = \text{diag}\{\lambda_1, \ldots, \lambda_n\}$ through the transformation $\mathbf{T}^{-1}\mathbf{A}^c(1)\mathbf{T}$.

Additionally, we define $\mathbf{DV}(v_k) \in \mathbb{R}^{n \times n}$ as:

$$\mathbf{DV}(v_k) = \text{diag}\{1, v_k^{-1}, \ldots, v_k^{-(n-1)}\}, \tag{26}$$

Then, recalling that the eigenvalues divide by v_k when they move on the pole paths, $\mathbf{DV}(v_k)\mathbf{T}$ serves as a transformation matrix that converts $\mathbf{A}^c(v_k)$ into the modal form, $\mathbf{DA}^c(v_k) = \text{diag}\{\lambda_1 v_k^{-1}, \ldots, \lambda_n v_k^{-1}\} = v_k^{-1}\mathbf{DA}^c(1)$.

With that in mind, we suggest defining $\mathbf{\Theta}(k)$ as:

$$\mathbf{\Theta}_k = \mathbf{DV}^{-1}(v_{k-1})\mathbf{DV}^{-1}(v_k)\mathbf{T}^{-1}, \tag{27}$$

which, according to the definition of $\mathbf{F}_k$ in Lemma 1, results in:

$$\begin{aligned} \mathbf{F}_k =& \mathbf{DV}^{-1}(v_{k+1}) \ldots \\ & \underbrace{\mathbf{DV}^{-1}(v_k)\mathbf{T}^{-1}\mathbf{A}^c(v_k)\mathbf{DV}(v_k)\mathbf{T}}_{=\mathbf{DA}^c(v_k) = v_k^{-1}\mathbf{DA}^c(1)} \ldots \\ & \mathbf{DV}(v_{k-1}). \end{aligned} \tag{28}$$

Noticing that $\mathbf{F}$ is diagonal and therefore, $\mathbf{F}_k^\intercal = \mathbf{F}_k$, we have

$$\begin{aligned} \mathbf{F}_k^\intercal \mathbf{F}_k =& \mathbf{DV}^{-2}(v_{k+1})\mathbf{DV}^2(v_{k-1}) \ldots \\ & v_k^{-2}\mathbf{DA}^{c2}(1). \end{aligned} \tag{29}$$

Since we have assumed that the eigenvalues for $v = 1$ are inside the unit circle, then $\mathbf{DA}^{c2}(1) < \mathbf{I}_n$. Therefore, to prove $\mathbf{F}_k^\intercal \mathbf{F}_k - \mathbf{I}_n < 0$, we only need to ensure that:

$$\mathbf{DV}^{-2}(v_{k+1})\mathbf{DV}^2(v_{k-1})v_k^{-2} \leq \mathbf{I}_n \tag{30}$$

On the other hand,

$$\begin{aligned} \mathbf{DV}^{-2}(v_{k+1})\mathbf{DV}^2(v_{k-1}) = \ldots \\ \text{diag}\left\{1, \ldots, \left(\frac{v_{k+1}}{v_{k-1}}\right)^{2(n-1)}\right\}. \end{aligned} \tag{31}$$

Therefore, the maximum value of the diagonal elements of the left-hand side of (30) is:

$$\max\left\{v_k^{-2}, v_k^{-2}\left(\frac{v_{k+1}}{v_{k-1}}\right)^{2(n-1)}\right\}. \tag{32}$$

So, (30) is satisfied if $v_1 \geq 1$, and

$$\forall k \geq 2, \begin{cases} v_k \geq 1, \quad \text{and,} \\ v_k^{-1}\left(\frac{v_{k+1}}{v_{k-1}}\right)^{(n-1)} \leq 1, \end{cases} \tag{33}$$

which proves the theorem. ■

Since our design recommendations include changes to $\mathbf{A}^c(v_k)$ after every $\kappa \geq 2n$ time steps, Corollary 1 guarantees that if v_{k+1} is found to be admissible for $\{v_k, v_{k-1}\}$, its value can be maintained until $k + i$ for all $i > 2$.

Corollary 1: If $v_k = v_{k-1} = \alpha_1$ and $v_{k+1} = \alpha_2$ meet the conditions of Theorem 1, then $\forall q > 2$, maintaining $v_{k+i} = \alpha_2$ for $i = \{2, \ldots, q\}$ will not jeopardize the stability.

Proof: Since $v_{k+1} = \alpha_2$ must satisfy the conditions of Theorem 1, $\alpha_2 \geq 1$. Therefore, we can observe that $\{v_{k+i}, v_{k+i+1}, v_{k+i+2}\} = \{\alpha_2, \alpha_2, \alpha_2\}$ is admissible according to Theorem 1 for all $i > 1$.

Furthermore, $\{v_{k-1}, v_k, v_{k+1}\} = \{\alpha_1, \alpha_1, \alpha_2\}$ is assumed to meet the conditions of Theorem 1. Thus, we only need to verify the case where $\{v_k, v_{k+1}, v_{k+2}\} = \{\alpha_1, \alpha_2, \alpha_2\}$.

In the event that $\alpha_2 \leq \alpha_1$, we have

$$\left(\frac{v_{k+2}}{v_k}\right) = \left(\frac{\alpha_2}{\alpha_1}\right) \leq 1,$$

and therefore,

$$v_{k+1}^{-1}\left(\frac{v_{k+2}}{v_k}\right)^{(n-1)} = \alpha_2^{-1}\left(\frac{\alpha_2}{\alpha_1}\right)^{(n-1)} \leq 1.$$

Since we have assumed that $\{v_{k-1}, v_k, v_{k+1}\} = \{\alpha_1, \alpha_1, \alpha_2\}$ meet the conditions of Theorem 1, we have

$$\alpha_1^{-1}\left(\frac{\alpha_2}{\alpha_1}\right)^{(n-1)} \leq 1.$$

Therefore in the event that $\alpha_2 > \alpha_1$,

$$\alpha_2^{-1}\left(\frac{\alpha_2}{\alpha_1}\right)^{(n-1)} \leq \alpha_1^{-1}\left(\frac{\alpha_2}{\alpha_1}\right)^{(n-1)} \leq 1,$$

which yields to

$$v_{k+1}^{-1}\left(\frac{v_{k+2}}{v_k}\right)^{(n-1)} = \alpha_2^{-1}\left(\frac{\alpha_2}{\alpha_1}\right)^{(n-1)} \leq 1.$$

This concludes the proof. ■

Remark 1: From Theorem 1, we observe that the feasible interval for moving v_k becomes narrower as v_k tends to 1. Since the concept of the moving controller relies on time-varying dynamics, it is advisable to establish a lower bound for v_k to ensure sufficient room for meaningful modifications of the closed-loop eigenvalues. ■

V. Conclusion

The hybrid moving controller approach presented in this paper addresses concerns related to the stability of the moving target approaches. Additionally, it eliminates the need for synchronization between the plant and control unit, facilitating smoother practical implementation. Future work can extend the concept of the hybrid moving controller to continuous-time systems and explore more compromised systems where even the input signal may not be secure.

References

[1] J. Guo, L. Li, J. Wang, and K. Li, "Cyber-physical system-based path tracking control of autonomous vehicles under cyber-attacks," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 5, pp. 6624–6635, 2023.

[2] O. Younis and N. Moayeri, "Employing cyber-physical systems: Dynamic traffic light control at road intersections," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2286–2296, 2017.

[3] J. Wan, H. Yan, D. Li, K. Zhou, and L. Zeng, "Cyber-physical systems for optimal energy management scheme of autonomous electric vehicle," *The Computer Journal*, vol. 56, no. 8, pp. 947–956, 2013.

[4] M. W. Condry and X. I. Quan, "Remote patient monitoring technologies and markets," *IEEE Engineering Management Review*, vol. 51, no. 3, pp. 59–64, 2023.

[5] M. Kaheni, A. Pilloni, G. S. Ruda, E. Usai, and M. Franceschelli, "Distributed asynchronous greedy control of large networks of thermostatically controlled loads for electric demand response," *IEEE Control Systems Letters*, vol. 7, pp. 169–174, 2023.

[6] M. Abdelmalak, V. Venkataramanan, and R. Macwan, "A survey of cyber-physical power system modeling methods for future energy systems," *IEEE Access*, vol. 10, pp. 99 875–99 896, 2022.

[7] M. Kaheni, E. Usai, and M. Franceschelli, "Resilient and privacy-preserving multi-agent optimization and control of a network of battery energy storage systems under attack," *IEEE Transactions on Automation Science and Engineering*, pp. 1–13, 2023.

[8] ——, "A distributed optimization and control framework for a network of constraint coupled residential besss," in *2021 IEEE 17th International Conference on Automation Science and Engineering (CASE)*, 2021, pp. 2202–2207.

[9] T. M. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, 2011.

[10] M. Geiger, J. Bauer, M. Masuch, and J. Franke, "An analysis of black energy 3, crashoverride, and trisis, three malware approaches targeting operational technology systems," in *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, vol. 1, 2020, pp. 1537–1543.

[11] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2009, pp. 911–918.

[12] W. Yan, L. K. Mestha, and M. Abbaszadeh, "Attack detection for securing cyber physical systems," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8471–8481, 2019.

[13] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding sensor outputs for injection attacks detection," in *53rd IEEE Conference on Decision and Control*, 2014, pp. 5776–5781.

[14] S. Weerakkody and B. Sinopoli, "Detecting integrity attacks on control systems using a moving target approach," in *2015 54th IEEE Conference on Decision and Control (CDC)*, 2015, pp. 5820–5826.

[15] P. Griffioen, S. Weerakkody, and B. Sinopoli, "An optimal design of a moving target defense for attack detection in control systems," in *2019 American Control Conference (ACC)*, 2019, pp. 4527–4534.

[16] S. Weerakkody and B. Sinopoli, "A moving target approach for identifying malicious sensors in control systems," in *2016 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2016, pp. 1149–1156.

[17] P. Griffioen, S. Weerakkody, and B. Sinopoli, "A moving target defense for securing cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 66, no. 5, pp. 2016–2031, 2021.

[18] J. Tian, R. Tan, X. Guan, Z. Xu, and T. Liu, "Moving target defense approach to detecting stuxnet-like attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 291–300, 2020.

[19] M. Kaheni, M. Hadad Zarif, A. Akbarzadeh Kalat, and M. S. Fadali, "Soft variable structure control of linear systems via desired pole paths," *Information Technology and Control*, vol. 47, no. 3, pp. 447–456, 2018.

[20] ——, "Radial pole paths svsc for linear time invariant multi input systems with constrained inputs," *Asian Journal of Control*, vol. 22, no. 1, pp. 547–555, 2020.

[21] M. Kaheni, M. Hadad Zarif, A. Akbarzadeh Kalat, and L. Chisci, "Radial pole path approach for fast response of affine constrained nonlinear systems with matched uncertainties," *International Journal of Robust and Nonlinear Control*, vol. 30, no. 1, pp. 142–158, 2020.

[22] M. Kaheni, M. Hadad Zarif, A. Akbarzadeh Kalat, and M. S. Fadali, "Pole path assignment of constrained siso affine nonlinear systems," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 47, pp. 785–795, 2019.

[23] C. C. Nguyen, "Arbitrary eigenvalue assignments for linear time-varying multivariable control systems," *International Journal of Control*, vol. 45, no. 3, pp. 1051–1057, 1987.

[24] J. Adamy and A. Flemming, "Soft variable-structure controls: a survey," *Automatica*, vol. 40, no. 11, pp. 1821–1844, 2004.

[25] F. Bullo, *Contraction Theory for Dynamical Systems*, 1.1 ed. Kindle Direct Publishing, 2023.

[26] W. Lohmiller and J.-J. E. Slotine, "On contraction analysis for nonlinear systems," *Automatica*, vol. 34, no. 6, pp. 683–696, 1998.