Systems & Control Letters 158 (2021) 105066

Contents lists available at ScienceDirect

Systems & Control Letters

journal homepage: www.elsevier.com/locate/sysconle

Resilient redundancy-based control of cyber–physical systems through adaptive randomized switching☆,☆☆

Prashanth Krishnamurthy, Farshad Khorrami *

Department of ECE, NYU Tandon School of Engineering, 5 MetroTech Center, Brooklyn, NY, 11201, USA

ARTICLE INFO

Article history:
Received 13 May 2021
Received in revised form 29 September 2021
Accepted 19 October 2021
Available online 15 November 2021

Keywords:
Resilient control
Cyber–physical systems
Redundancy
Switching controllers
Randomized methods

ABSTRACT

A switching based approach using multiple parallel redundant controller implementations is developed to improve resiliency of cyber–physical systems (CPSs). Hardware/software redundancy is known to be a powerful technique for resiliency to mitigate effects of adversaries who infiltrate and maliciously modify a subset of the redundant subsystems. While redundant subsystems are typically combined using fail-over/backup and voting mechanisms, the proposed approach considers a time-division multiplexer using which one of multiple controller implementations is selected at each time instant to drive the input of the controlled system. Through detailed analysis of the switched system, it is shown that time-division multiplexing between redundant controllers can be used to mitigate the impact to stability and/or performance of the closed-loop CPS due to adversarial modifications of subsets of controllers. Additionally, we show that adversarial impact to the closed-loop CPS can be reduced over time by switching among the controllers in a probabilistic manner (rather than round-robin) and by dynamically adapting probabilities of switching to each controller. The efficacy of the proposed adaptive randomized switching algorithm is shown through simulation studies on two illustrative examples: a simple third-order system and a more real-world single-machine-infinite-bus system.

1. Introduction

Cyber-security for industrial control systems (ICSs) and other cyber–physical systems (CPSs) are becoming increasingly critical [2–8]. While increasing programmability and remote connectivity of controller devices (e.g., Programmable Logic Controllers — PLCs) in modern CPSs provide significant benefits in terms of ease of use and maintenance, they also increase the potential attack surface for a cyber-adversary [9–13]. Hence, to detect and prevent attacks, several approaches have been developed in the literature including hardware, software, network-based and process-aware methods, which can be combined in various ways to achieve robust multi-layer security [2–6,14–23]. In combination with these approaches, a generally useful ingredient in achieving resiliency (both against cyber-adversaries and possible malfunctions, etc.) is redundancy.

Redundancy can be introduced into a CPS at multiple levels including communication channels, software, and hardware (e.g., multiple redundant sensors, actuators, or computing nodes), etc. [24–35]. Several off-the-shelf CPS devices integrate redundancy in recent years based on integrity verification and voting methods (e.g., the PLC-level ControlLogix Redundancy System [36], the compiler-level CODESYS redundancy toolkit [37]). The basic concept in introducing redundancy is that effects of failures/malfunctions/cyber-attacks of a subset of parallel subsystems may be mitigated due to the other redundant subsystems that are operating normally. Redundant subsystems can be combined using multiple approaches such as using subsystems as fail-over (i.e., as backup to primary subsystems), comparing outputs/behaviors of subsystems at real-time (e.g., continuous integrity verification between parallel redundant subsystems), or by aggregating the outputs/behaviors of parallel subsystems (e.g., using voting to determine the "majority opinion") [24–29,31–35]. In the context of cyber-security, redundancy can be combined with heterogeneity at various levels (e.g., by implementing redundant controller instantiations using different processor architectures, operating systems, communication network connectivities, etc.) to pose additional challenges to the adversary and limit the number of subsystems that could be realistically simultaneously infiltrated. Such combinations of redundancy and heterogeneity can be viewed in the context of

☆ An earlier version of this paper was presented (Krishnamurthy and Khorrami, 2020) [1] at the 2020 IEEE Conference on Control Technology and Applications.

☆☆ This work was supported in part by the National Science Foundation (NSF) under grant 2039615 and the Office of Naval Research (ONR) under grant N000141512182.

* Corresponding author.
E-mail addresses: prashanth.krishnamurthy@nyu.edu (P. Krishnamurthy), khorrami@nyu.edu (F. Khorrami).

https://doi.org/10.1016/j.sysconle.2021.105066
0167-6911/

moving-target defense. Additionally, *dynamic* moving-target defense approaches [38–40] can be integrated (e.g., dynamically changing parameters of the system, system dynamics by introducing additional external states or using sensor nonlinearities, communication parameters protocols, hardware or software configurations, etc.) to pose further challenges to attackers. While such moving-target defenses introduce dynamic variations (i.e., switching) to introduce an aspect of unpredictability to the attacker, switching-based methods have also been applied [41–43] to design stabilizing controllers for systems with uncertainties such as time-varying delays and constraints such as actuator saturation. An adaptive round-robin switching scheme has been developed in [44] in the context of observer design for linear systems under sensor spoofing attacks. By using the measured observer errors under different combinations of utilized sensors as a performance index, the method in [44] steps through different candidate subsets of sensors to be utilized to eventually detect and disable the corrupted sensors.

Unlike the above literature, we consider in this paper the problem of designing a controller switching algorithm to achieve resiliency under attacks on controller implementations for nonlinear systems. Specifically, based on our initial development in [1], we consider the problem of temporal switching between multiple parallel redundant controller implementations connected using a time-division multiplexer as shown in Fig. 1. The time-division multiplexer in Fig. 1 is a switching controller that dynamically picks one of the controller nodes as the *active* controller for a time interval of a fixed length and utilizes the output signal of the selected controller node as the input signal to the controlled system. In this paper, we analyze the behavior of the overall closed-loop system under the time-division multiplexing and design switching schemes to dynamically pick active controller nodes. We first analyze the simplest switching logic which is a round-robin switching (RRS) multiplexer that picks the controller nodes in sequence (in a round-robin pattern) and then develop an adaptive randomized switching (ARS) scheme.

It will be seen that the time-division multiplexing based approach provides a very useful design freedom in terms of the switching logic used for selecting controller nodes. In particular, it will be seen that even the simplest switching logic, which is the RRS multiplexer, provides benefits in terms of retaining CPS stability/performance under adversarial modifications of subsets of controller nodes and that the closed-loop behavior under RRS is essentially a balance between how effectively good controllers can stabilize the system vs. how much damage bad controllers can inflict. However, we will see that the ARS scheme can enable much higher resiliency and that specifically, by introspecting the performance of the selected controller over each time interval, it is possible to probabilistically determine bad controller nodes and "tune them out" over time. In particular, by making the switching between controller nodes probabilistic rather than round-robin and by adapting the probabilities of switching to each of the controllers on-line based on the observation of their performance, the impact to the CPS due to adversarial manipulations of a subset of controller nodes can be attenuated over time.

It is to be noted that unlike voting-based or fail-over schemes, the proposed time-division multiplexing based approach does not use comparison of the outputs of the different controller nodes at run-time. This yields several advantages. Firstly, this allows a simpler structure of the multiplexer since it does not need to compute expected control actions and instead only requires to feed through the selected controller node output. Secondly, this approach enables the multiplexer to not require to obtain outputs of inactive controller nodes (in fact, the inactive controller nodes do not even need to run their computations and can be disabled or put into low power mode during their inactive

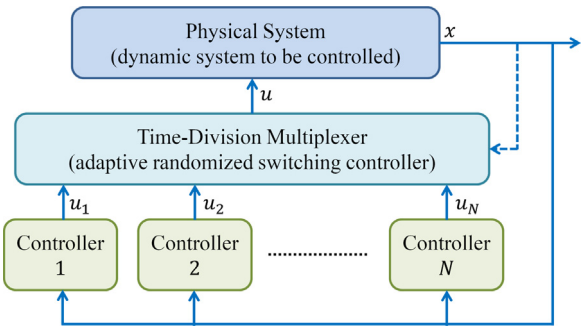

Fig. 1. Overall architecture of the proposed adaptive randomized controller switching scheme for CPS resiliency. The controller nodes are indexed by $1, \ldots, N$. The time-division multiplexer takes the outputs of the controller nodes and selects, over each time interval, one of these outputs to pass through as the control signal to the physical system.

times). Thirdly, since the approach does not require numerical comparisons between outputs of controller nodes, this approach provides robustness to noise and other computation variations between different controller nodes and also allows heterogeneity in controller designs and implementations. Specifically, numerical comparison between nodes for voting schemes would be susceptible to various noise/non-idealities such as sensor measurement and quantization noise, numerical variations due to sensor signal sampling time shifts, and computational variations between controller nodes (e.g., due to different implementation methods and processor architectures). On the other hand, the time-division multiplexer-based scheme is not affected by such noise/non-idealities since it relies instead on observing the dynamic closed-loop behavior of the system and adapting controller switching likelihoods. Furthermore, the controllers in different controller nodes can be different and independently designed in the proposed scheme (e.g., controllers based on different sets of assumptions or based on slightly different physical models of the controlled system).

The novel contributions of this paper include:

- Analysis of the dynamic behavior of the closed-loop system under the time-division multiplexing based switching controller.
- Development of the ARS scheme that dynamically adapts probabilities of switching to each controller using the on-line observed "goodness" of controller nodes.
- Analysis of the convergence properties of the controller switching probabilities for unattacked and attacked controller nodes and the dynamic closed-loop system behavior under the ARS scheme.
- Analysis of the efficacy and robustness of the proposed method for two illustrative example systems (using simulation-based studies).

The organization of the paper is as follows. The detailed formulation of the problem being addressed and introduced assumptions are discussed in Section 2. The switching-based controller design and its analysis are presented in Section 3. The adaptive randomized switching algorithm is presented in Section 4. Simulation studies of the application of the proposed approach to a third-order system example and a more real-world representative CPS example (a single-machine-infinite-bus system) are provided in Section 5. Concluding remarks are summarized in Section 6.

2. Problem formulation and assumptions

Consider a CPS with dynamics of the form

$$\dot{x} = f(x, u, w) \tag{1}$$

where $x \in \mathcal{R}^{n_x}$ is the state of the system, $u \in \mathcal{R}^{n_u}$ is the control input, and $w \in \mathcal{R}^{n_w}$ is a disturbance input, with n_x, n_u, and n_w representing dimensions of system state, control input, and disturbance input, respectively. The assumptions introduced on this class of systems are listed below and discussed in Remarks 1 and 2.

Assumption A1. Control laws $u_i(x), i = 1, \ldots, N$, and a common Lyapunov function $V(x)$ are given such that, for each $i \in \{1, \ldots, N\}$, the following inequality is satisfied along all trajectories of the closed-loop system formed by (1) and the control law $u_i(x)$

$$\dot{V} \leq -\alpha_i(|x|) + \beta_{(1,i)}(|x|)\mu_{(1,i)}(|w|), \tag{2}$$

with α_i being a class $\mathcal{K}_\infty$ function,[1] $\beta_{(1,i)}$ being a non-negative function, and $\mu_{(1,i)}$ being a class $\mathcal{K}$ function. Additionally, positive constants $\overline{\alpha}_i$, $\underline{\alpha}_i$, and $\overline{\beta}_{(1,i)}$ are known such that

$$\underline{\alpha}_i V(x) \leq \alpha_i(|x|) \leq \overline{\alpha}_i V(x) \tag{3}$$

$$\beta^2_{(1,i)}(|x|) \leq \overline{\beta}_{(1,i)}\alpha_i(|x|). \tag{4}$$

Assumption A2. The Lyapunov function from Assumption A1 satisfies the following inequality along any trajectory of the system (1)

$$\dot{V} \leq \gamma_1(|x|) + \gamma_2(|x|)\gamma_u(|u|) + \beta_2(|x|)\mu_2(|w|) \tag{5}$$

with γ_2 and β_2 being non-negative functions, γ_1 being any function (not necessarily sign-definite), and γ_u and μ_2 being class $\mathcal{K}$ functions. Also, a constant $\overline{\gamma}_1$ and positive constants $\overline{\gamma}_2$ and $\overline{\beta}_2$ are known such that $\gamma_1(|x|) \leq \overline{\gamma}_1 V(x)$, $\gamma_2^2(|x|) \leq \overline{\gamma}_2 V(x)$, and $\beta_2^2(|x|) \leq \overline{\beta}_2 V(x)$. It is assumed that the magnitudes of u and w are bounded (e.g., due to physical constraints in the specific CPS) as $|u| \leq u_{max}$ and $|w| \leq w_{max}$ with u_{max} and w_{max} being positive constants.

Remark 1. Assumption A1 essentially requires that one or more nominal state-feedback control laws have been designed for the system (1). Since the proposed methodology is based on switching among N different controller implementations as shown in Fig. 1, Assumption A1 is stated, for generality, in terms of N known control laws. Some or all of these control laws could be identical. Assumption A2 is essentially a worst-case bound known on the possible adversarial impact (modeled in terms of a Lyapunov inequality) by an attacker by arbitrarily modifying the control input signal. Considering Assumptions A1 and A2, the first part of the problem being addressed is to determine what effect adversarial modifications on a subset of controller implementations can have on the overall closed-loop system when the control input to the system (1) is generated by switching (time-division multiplexing) among the set of controllers. The second part of the problem being addressed is to develop a methodology for adaptively updating the likelihoods of switching to each of the controllers by introspecting the real-time "goodness" of the controllers and to establish how such a methodology can, over time, attenuate the effects of the adversarially modified controllers. These two parts of the problem are discussed in Sections 3 and 4, respectively, and simulation studies are presented in Section 5. ◇

[1] Class $\mathcal{K}$ denotes the set of all continuous functions $\alpha : [0, a) \to [0, \infty)$ that are strictly increasing and satisfy $\alpha(0) = 0$. Class $\mathcal{K}_\infty$ is the subset of class $\mathcal{K}$ wherein furthermore $a = \infty$ and $\alpha(r) \to \infty$ as $r \to \infty$.

Remark 2. Assumptions A1 and A2 are satisfied by several classes of dynamical systems and control designs. For example, the backstepping-based control designs for strict-feedback systems naturally lead to Lyapunov inequalities of the form in Assumptions A1 and A2. The strongest part of the assumptions in A1 and A2 is that the negative term $-\alpha_i(|x|)$ on the right hand side of Lyapunov inequality (2) is of the "same size" (in a nonlinear function sense) as the Lyapunov function $V(x)$. This structure is, for example, automatically generated in a backstepping-based design for a system of the general strict-feedback form $\dot{x}_i = f_i(x_1, \ldots, x_i) + \phi_i(x_1, \ldots, x_i)x_{i+1}, i = 1, \ldots, n-1; \dot{x}_n = f_n(x_1, \ldots, x_n) + \phi_n(x_1, \ldots, x_n)u$ with $f_1, \ldots, f_n, \phi_1, \ldots, \phi_n$ being some functions. In the ith step of the iterative process of backstepping, a virtual control law x^*_{i+1} is designed for x_{i+1} and a transformed state variable is defined as $z_{i+1} = x_{i+1} - x^*_{i+1}$. At the nth step of backstepping, the control law for u is designed. After the completion of this process, the Lyapunov function V will comprise of quadratics in $z_1, \ldots, z_n$ while the right hand side of the expression for $\dot{V}$ will have negative quadratic terms in $z_1, \ldots, z_n$, thus providing a structure (which relates to exponential convergence in terms of the transformed set of state variables $z_1, \ldots, z_n$) as in (2). It can be seen that control design approaches such as feedback linearization and dynamic high-gain control designs also lead to Lyapunov inequalities of the form in Assumptions A1 and A2. Also, these assumptions are automatically satisfied in the special case of linear systems. For example, considering $\dot{x} = Ax + Bu + Hw$ and a feedback control law $u = Kx$ with K being a stabilizing feedback gain, a symmetric positive-definite matrix P can always be found such that $P(A + BK) + (A + BK)^T P \leq -I$. Then, defining $V = x^T Px$, we have

$$\dot{V} \leq -|x|^2 + 2x^T PHw, \tag{6}$$

implying that Assumption A1 is satisfied. Also, for any input signal u, we have

$$\dot{V} \leq x^T(PA + A^T P)x + 2x^T PBu + 2x^T PHw, \tag{7}$$

implying that Assumption A2 is satisfied. In all the example system structures above, it is to be noted that all or some of the control laws u_i can be identical or can be all different (e.g., with slightly or significantly different gains). ◇

Remark 3. For mathematical simplicity and clarity and to focus on the controller switching approach which is the main focus of this paper, Assumptions A1 and A2 are stated based on a common Lyapunov function $V(x)$ shared among all the controller nodes. This is not a particularly strong assumption since the physical system being controlled is the same irrespective of the controller node and the control designs and implementations at each controller node would not in realistic scenarios be dramatically different from each other. The proposed approach can however also be applied to the case where the Lyapunov function is different for each controller node (i.e., separate Lyapunov functions $V_i, i = 1, \ldots, N$, for the control laws u_i implemented at each controller node i) as discussed further in Remarks 6 and 9. ◇

Adversary (Threat Model): The adversary/attacker is modeled as having the ability to arbitrarily modify the control signal (subject to the physical magnitude constraint represented by u_{max}) output by the *attacked controller nodes*. The set of attacked controller nodes is assumed to be an unknown subset of the set of all controller nodes — this subset physically represents the set of controller nodes that the attacker has successfully infiltrated. The adversary's access to the attacked controller nodes (i.e., the infiltration) can be conceptually thought of as resulting from successful cyber-attacks on the controller nodes by exploiting software/network vulnerabilities. As discussed in Section 1,

such vulnerabilities and cyber-attacks are indeed relevant in real-world CPS. As discussed further in Remark 4, the adversary's access is reasonably limited to a subset of controller nodes (the subset being unknown however) due to software/network heterogeneity making it much more difficult for an adversary to gain access to all controller nodes simultaneously. The maximum dynamic effect of the adversary on the closed-loop system is modeled via the Lyapunov inequality in Assumption A2. Since the closed-loop behavior of the CPS is governed by the dynamics of the physical system and the magnitudes of the input signals that can be applied to the system are constrained by the physical instrumentation of the CPS, the model in Assumption A2 of the maximum adversarial impact on the dynamic closed-loop system is physically justified. Assumption A1 characterizes the stabilizing behavior of an unattacked controller and is also physically realistic since the intended control law (unmodified by an adversary) would be designed taking into account the system dynamics to stabilize the closed-loop system. The set of all attacked controller nodes is denoted by $A \subset \{1, \ldots, N\}$ and the number of elements in the set A is denoted by n_A.

Remark 4. As discussed in Section 1, the redundancy in controller implementations can be physically coupled with heterogeneity to limit the potential success by the adversary. For example, different controller nodes can be implemented using various hardware architectures (e.g., different types of processors such as Intel and ARM so as to limit effects of architecture-specific malwares to a subset of controller nodes), different operating systems (e.g., VxWorks, Windows, Linux), different network interfaces (e.g., serial, Ethernet, analog), different network connectivities (e.g., physically disjoint network buses/sub-networks), different network protocols (e.g., Modbus, RS232, custom TCP/IP), etc. Introducing "multi-modal" heterogeneity is a well-established cyber-security practice [28,33] in CPSs and poses significant challenges to the adversary and practically limits the number of nodes that an adversary can realistically simultaneously attack in a successful manner since vulnerabilities that would be exploited by the adversary to attack the nodes are specific to one or more of various variables including device type, processor architecture, network connection type and protocol, operating system, etc. ◇

Design Freedom: The control laws $u_i(x)$ for each of the controller nodes are assumed to be known as summarized in Assumption A1. The design problem being addressed is to define a switching logic for the time-division multiplexer, i.e., a decision rule to dynamically pick which of the controller nodes to connect to the actual control signal to the physical system in each time interval. The simplest such logic is RRS wherein each of the controllers is picked in sequence for the same length of time. As discussed in Section 3, even the simple RRS provides stability and performance benefits since the action of the uncompromised controller nodes during their active times can compensate to some extent for destabilizing effects of compromised controller nodes during their active times. However, by observing dynamic behavior in each time interval, an adaptive randomized switching (ARS) logic can be achieved, which, as could be expected, can provide much better stability and performance as discussed in Section 4.

3. Controller switching: Design and analysis

As discussed in Section 2, we are given the system (1) and N control laws $u_i(x)$. The control laws are considered as implemented on N separate computational nodes, therefore providing N separate controller instantiations. The output of the ith controller node is $u_i(x)$. The task of the time-division multiplexer based switching controller as shown in Fig. 1 is to dynamically select one of the controller nodes and feed through its output for a time interval of a specified length T. More precisely, at time instants $t = kT$, $k = 0, 1, 2, \ldots$, the multiplexer chooses an $i \in 1, \ldots, N$; the signal $u_i(x)$ is then passed through as the control input to the system (1) for time interval $[kT, (k+1)T)$. Defining the "selection" signal as s_k, the control input to system (1) is given by

$$u(t) = u_{s_k}(x(t)) \quad \text{for } t \in [kT, (k+1)T)\,, \;\; k = 0, 1, 2, \ldots. \tag{8}$$

The simplest switching logic for this purpose is RRS (round-robin) given by

$$s_k = k \,(\text{mod } N) + 1. \tag{9}$$

Since the control input signal to the system (1) over time interval $[kT, (k+1)T)$ is $u_{s_k}(x)$, the closed-loop system has dynamics given by

$$\dot{x} = f(x, u_{s_k}(x), w). \tag{10}$$

The closed-loop dynamics (10) is of a switched system form with dwell time T. The stability properties of the switched system (10) are analyzed below for any selection signal s_k with RRS (9) being a specific case.

Assumptions A1 and A2 provide characterizations of system behavior (modeled using Lyapunov inequalities) during time intervals corresponding to unattacked or attacked controller nodes, respectively. From Assumption A1, it is seen that during a time interval corresponding to an unattacked controller node i, the following Lyapunov inequality is satisfied:

$$\dot{V} \leq -\underline{\alpha}_i V + \frac{1}{\epsilon_i}\beta^2_{(1,i)}(|x|) + \frac{\epsilon_i}{4}\mu^2_{(1,i)}(|w|) \tag{11}$$

$$\leq -\left(\underline{\alpha}_i - \frac{1}{\epsilon_i}\overline{\beta}_{(1,i)}\overline{\alpha}_i\right) V + \frac{\epsilon_i}{4}\mu^2_{(1,i)}(|w|) \tag{12}$$

where $\epsilon_i > 0$ is any constant.

From Assumption A2, it is seen that during a time interval corresponding to an attacked controller node, the following Lyapunov inequality is satisfied:

$$\dot{V} \leq \overline{\gamma}_1 V + \frac{1}{\epsilon_a}\gamma^2_2(|x|) + \frac{\epsilon_a}{4}\gamma^2_u(|u|) + \frac{1}{\epsilon_b}\beta^2_2(|x|) + \frac{\epsilon_b}{4}\mu^2_2(|w|) \tag{13}$$

$$\leq \left(\overline{\gamma}_1 + \frac{1}{\epsilon_a}\overline{\gamma}_2 + \frac{1}{\epsilon_b}\overline{\beta}_2\right) V + \frac{\epsilon_a}{4}\gamma^2_u(|u|) + \frac{\epsilon_b}{4}\mu^2_2(|w|) \tag{14}$$

where $\epsilon_a > 0$ and $\epsilon_b > 0$ are any constants. Hence, during a time interval $[kT, (k+1)T)$ corresponding to an attacked controller node, i.e., if s_k is in set A of attacked controller nodes, we see[2] using the Bellman–Grönwall Lemma that

$$V_{(k+1)T} \leq e^{\lambda_a T} V_{kT} + \int_{kT}^{(k+1)T} e^{\lambda_a((k+1)T-\tau)}\left[\frac{\epsilon_a}{4}\gamma^2_u(|u|) + \frac{\epsilon_b}{4}\mu^2_2(|w|)\right] d\tau \tag{15}$$

where λ_a is a constant given by

$$\lambda_a = \overline{\gamma}_1 + \frac{1}{\epsilon_a}\overline{\gamma}_2 + \frac{1}{\epsilon_b}\overline{\beta}_2. \tag{16}$$

Noting that γ_u and μ_2 are class $\mathcal{K}$ functions and noting that $|u| \leq u_{max}$ and $|w| \leq w_{max}$, (15) implies

$$V_{(k+1)T} \leq e^{\lambda_a T} V_{kT} + \overline{u}_a + \overline{w}_b \tag{17}$$

where $\overline{u}_a$ and $\overline{w}_b$ are constants given by

$$\overline{u}_a = \frac{e^{\lambda_a T} - 1}{\lambda_a}\frac{\epsilon_a}{4}\gamma^2_u(u_{max})\;;\;\; \overline{w}_a = \frac{e^{\lambda_a T} - 1}{\lambda_a}\frac{\epsilon_b}{4}\mu^2_2(w_{max}). \tag{18}$$

[2] The notation V_t is used to denote the value of $V(x)$ at time t, i.e., V_t denotes $V(x(t))$.

On the other hand, if the time interval $[kT, (k+1)T)$ corresponds to an unattacked controller node i, i.e., if $i = s_k$ is not in A, we see using (12) and the Bellman–Grönwall Lemma that

$$V_{(k+1)T} \leq e^{-\lambda_i T} V_{kT} + \int_{kT}^{(k+1)T} e^{-\lambda_i((k+1)T-\tau)} \frac{\epsilon_i}{4} \mu_{(1,i)}^2(|w|) d\tau \tag{19}$$

where λ_i is a constant defined as

$$\lambda_i = \underline{\alpha}_i - \frac{1}{\epsilon_i} \overline{\beta}_{(1,i)} \overline{\alpha}_i. \tag{20}$$

The constant ϵ_i appearing in (12) is picked such that

$$\epsilon_i \geq \frac{1}{\underline{\alpha}_i} \overline{\beta}_{(1,i)} \overline{\alpha}_i \tag{21}$$

therefore implying that $\lambda_i > 0$. Noting that $\mu_{(1,i)} \in \mathcal{K}$ and noting that $|w| \leq w_{max}$, (19) implies

$$V_{(k+1)T} \leq e^{-\lambda_i T} V_{kT} + \overline{w}_i \tag{22}$$

where $\overline{w}_i$ is a constant given by

$$\overline{w}_i = \frac{1 - e^{-\lambda_i T}}{\lambda_i} \frac{\epsilon_i}{4} \mu_{(1,i)}^2(w_{max}). \tag{23}$$

The inequalities (17) and (22) provide bounds on the temporal evolution of the Lyapunov function V during time intervals corresponding to attacked or unattacked controller nodes, respectively. Hence, considering N time intervals of length T starting from time kT, we have

$$V_{(k+N)T} \leq \left(\prod_{r=k}^{k+N-1} a_r \right) V_{kT} + \sum_{r=k}^{k+N-1} \left(\prod_{j=r}^{k+N-1} a_j \right) b_r \tag{24}$$

where

$$a_r = \begin{cases} e^{-\lambda_{s_r} T} \text{ if } s_r \notin A \\ e^{\lambda_a T} \text{ if } s_r \in A \end{cases} \tag{25}$$

$$b_r = \begin{cases} \overline{w}_{s_r} \text{ if } s_r \notin A \\ \overline{u}_a + \overline{w}_a \text{ if } s_r \in A \end{cases} \tag{26}$$

where, as defined in Section 2, the set of attacked controller nodes is denoted by A, which is a subset of $\{1, \ldots, N\}$. While (24) is satisfied for a general switching signal s_k, the specific example of RRS (9) yields a simplification as shown below:

$$\prod_{r=k}^{k+N-1} a_r = \prod_{\substack{j=1 \\ j \in A}}^{N} e^{\lambda_a T} \prod_{\substack{j=1 \\ j \notin A}}^{N} e^{-\lambda_j T} \tag{27}$$

$$= \exp\left\{ \left(\sum_{\substack{j=1 \\ j \in A}}^{N} \lambda_a - \sum_{\substack{j=1 \\ j \notin A}}^{N} \lambda_j \right) T \right\}. \tag{28}$$

Note that (24) can be considered as an inequality on a scalar discrete-time system (with state variable V) and time step NT. Hence, it can be inferred from (24) that this scalar discrete-time system is stable if the scalar $\prod_{r=k}^{k+N-1} a_r$ is smaller than 1 in magnitude. It can also be seen that since the forcing term $\sum_{r=k}^{k+N-1} \left(\prod_{j=r}^{k+N-1} a_j \right) b_r$ admits a finite upper bound that can be easily written explicitly, the stability analysis only requires analysis of the term $\prod_{r=k}^{k+N-1} a_r$. Furthermore, since V is a Lyapunov function for the original system (1), it follows that stability of the closed-loop system formed by (1) and the switching controller can be inferred from stability of the scalar discrete-time system (24) (with state variable V). Hence, for the case of RRS, (28) implies that the closed-loop system is stable if

$$\sum_{\substack{j=1 \\ j \in A}}^{N} \lambda_a < \sum_{\substack{j=1 \\ j \notin A}}^{N} \lambda_j. \tag{29}$$

The inequality (29) essentially provides an estimated upper bound on how many controller nodes can be adversarially modified and still retain closed-loop stability.

Remark 5. As an illustration, consider the very specific case of when the size of the stabilizing effect of the unattacked controllers (as quantitatively measured by the size of $-\lambda_j$) is equal to the size of the destabilizing effect of the attacked controller nodes (as quantitatively measured by the size of λ_a). In this specific case, the inequality (29) reduces to $n_A < (N - n_A)$ where n_A is the number of adversarially modified controller nodes. This is equivalent to the condition $N > 2n_A$, which can be simply stated as the condition that if at most n_A controller nodes can be simultaneously compromised by an attacker, then it suffices to have $2n_A + 1$ controller nodes to retain closed-loop stability. This kind of condition (i.e., that to accommodate failures/malfunctions of at most k elements in a collection, it is sufficient to have $2k + 1$ elements in the overall collection) is commonly seen in redundancy-based resiliency analysis and it is intuitively satisfying to note that the obtained conditions do reduce, as can be expected, to this condition in the special case when the stabilizing and destabilizing effects of unattacked and attacked nodes, respectively, are equal. ◇

Remark 6. Under the case of separate Lyapunov functions V_i, $i = 1, \ldots, N$, for the control laws at the different controller nodes as discussed in Remark 3, an analysis analogous to the discussion in this section can be carried out. The primary modification under this case is that since the corresponding Lyapunov functions would change when switching between different controller nodes, an inequality such as (17) would need to be written to form an upper bound for $V_{s_{k+1},(k+1)T} \triangleq V_{s_{k+1}}(x((k+1)T))$ in terms of $V_{s_k,kT} \triangleq V_{s_k}(x(kT))$. For this purpose, it is to be noted that since V_i, $i = 1, \ldots, N$, are Lyapunov functions, it is reasonable to write known lower and upper bounds for these functions as $\underline{V}_i(|x|) \leq V_i(x) \leq \overline{V}_i(|x|)$ with $\underline{V}_i$ and $\overline{V}_i$ being class $\mathcal{K}_\infty$ functions. Hence, we would have, for example, the inequalities $V_j(x) \leq \overline{V}_j(\underline{V}_i^{-1}(V_i(x)))$ and $V_j(x) \geq \underline{V}_j(\overline{V}_i^{-1}(V_i(x)))$ for any i and j in $1 \ldots, N$. Hence, an inequality analogous to (17) can be written as

$$\underline{V}_{s_k}(\overline{V}_{s_{k+1}}^{-1}(V_{s_{k+1},(k+1)T})) \leq e^{\lambda_a T} V_{s_k,kT} + \overline{u}_a + \overline{w}_b \tag{30}$$

and similarly for (22). Using these inequalities, the analysis of the closed-loop system under the time-division multiplexing can be carried out (under, for example, simplifying assumptions on the relative sizes of $\underline{V}_i$ and $\overline{V}_i$ for different $i = 1, \ldots, N$) analogous to the analysis in this section. The details are omitted for brevity. ◇

4. Adaptive Randomized Switching (ARS)

While the conditions in (28) and (29) in Section 3 considered RRS, we now consider a time-division multiplexer that uses ARS. Based on a set of probabilities $p_1, \ldots, p_N$ such that $\sum_{j=1}^{N} p_j = 1$, ARS selects, at each switching time, one of the N controller nodes (with probability p_j for picking the jth controller node) with the choices of controller nodes at successive time intervals being independent random variables. Then, instead of the deterministic form of a_r in (24) and (25), we can write instead at time instant r:

$$E(a_r) = \sum_{\substack{j=1 \\ j \in A}}^{N} p_j e^{\lambda_a T} + \sum_{\substack{j=1 \\ j \notin A}}^{N} p_j e^{-\lambda_j T} \tag{31}$$

where the notation $E(.)$ is used to denote the expected value. The Eq. (31) can be considered as essentially a probabilistic version of an application of the averaging method in switched systems [45–47] based on the identification of the possible candidate

subsystems. It is noted that if it were possible to pick the probabilities p_j for attacked nodes (i.e., $j \in A$) to be relatively small and to pick probabilities p_j for unattacked nodes (i.e., $j \notin A$) to be large, then the expected value $E(a_r)$ can be ensured to be smaller than 1. Also, noting that the controller nodes over successive time intervals are independently picked, we have $E\left(\prod_{r=k}^{k+N-1} a_r\right) = \prod_{r=k}^{k+N-1} E(a_r)$. Hence, if p_j are small for $j \in A$ and relatively large for $j \notin A$, we would have $E\left(\prod_{r=k}^{k+N-1} a_r\right) < 1$. Hence, noting (24), we would ensure stability of the scalar discrete-time system with state variable $E(V)$. However, it is to be noted that it is not possible to directly pick p_j based on whether nodes are attacked/unattacked since it is not known which nodes are attacked/unattacked (even the number of attacked nodes, if any, is unknown). Nevertheless, while it is not possible to directly observe which nodes are attacked or unattacked, it is indeed possible to observe the "goodness" of a controller node during time intervals in which it is active. These observed goodness values can then be used to dynamically update the switching probabilities p_j for each controller node $j \in \{1 \ldots, N\}$. For this purpose, goodness estimates can be defined to characterize closed-loop system performance using, in general, application-specific criteria by considering for example combinations of the system state variables that best capture the control objectives (e.g., application-specific efficiency or CPS stability criteria). Alternatively, a general signal of goodness can be derived from the Lyapunov function V itself, which is as defined in Assumptions A1 and A2. Specifically, since $-\int_{kT}^{(k+1)T} \dot{V} d\tau = V_{kT} - V_{(k+1)T}$, an estimate of the goodness of the controller node s_k over the time interval $[kT, (k+1)T)$ can be computed by first caching the value of V at the time kT at which the controller node s_k becomes active, then observing the value of V at the time $(k+1)T$ when another controller is picked, and calculating the difference between the values at time instants kT and $(k+1)T$. To address noise and other uncertainties (including the possibility that the set of attacked controller nodes could change over time), these goodness estimates over time intervals can be averaged/filtered over time to derive a robust indicator of goodness of each controller node. Denoting $Q_{[kT,(k+1)T)} = V_{kT} - V_{(k+1)T}$, a simple filter for averaging these values for each controller node over time is given by

$$q_{s_k} \leftarrow \alpha q_{s_k} + (1-\alpha) Q_{[kT,(k+1)T)}. \tag{32}$$

The update rule (32) is executed at time $(k+1)T$ to update the temporally averaged estimate q_{s_k} of controller node s_k. The state variables $q_1, \ldots, q_N$ of the switching controller will be referred to as *switching likelihood states*; these state variables will be used below to compute probabilities for switching to each of the controller nodes. The parameter α in (32) can be picked to be any constant in the interval [0, 1]. At each time kT, the probabilities p_j of picking each of the controller nodes $j \in \{1, \ldots, N\}$ are defined as

$$\hat{p}_j = \max(q_j, c_0(t - t_{last,j})) \tag{33}$$

$$p_j = \frac{\hat{p}_j}{\sum_{j=1}^{N} \hat{p}_j} \tag{34}$$

where $c_0 > 0$ is any constant and $t_{last,j}$ denotes the last time (before the current switching time kT) at which the controller node j was selected. The second term in (33) is introduced to provide robustness to possible spurious reductions in switching likelihood states (e.g., due to intermittent noise) or possible changes in the sets of nodes that are unattacked/attacked. This second term in (33) ensures that even if the probability of switching to a particular controller j becomes very small, the controller will be tested again (for at least one time interval) at some point in time in the future to detect if its behavior has changed. The probabilities p_j computed in (34) are normalized, i.e., $\sum_{j=1}^{N} p_j = 1$.

Remark 7. To ensure that system behaviors during large transients do not inordinately dominate in the computations of q_j, additional normalization components can be integrated into the definition of $Q_{[kT,(k+1)T)}$ as

$$Q_{[kT,(k+1)T)} = \text{sat}\left(\frac{V_{kT} - V_{(k+1)T}}{\max(V_{(k+1)T}, \epsilon_V)}, Q_{min}, Q_{max}\right). \tag{35}$$

With this normalization, $Q_{[kT,(k+1)T)}$ and therefore the probability updates above are independent of the actual size of V (and thereby sizes of the states x), but are instead dependent on the relative rate of change of V. In (35), $\epsilon_V > 0$ can be picked to be any constant and is used in (35) to prevent a numerical singularity for values of $V_{(k+1)T}$ close to 0. Also, $\text{sat}(\delta, Q_{min}, Q_{max})$ denotes a saturation of the value δ to the interval $[Q_{min}, Q_{max}]$. As with the normalization, the saturation is also introduced to ensure that "noise" due to large transients do not cause inordinately large effects in computations of q_j. ◇

Remark 8. To further provide an intuitive interpretation of the ARS design in (32)–(35), the primary motivating considerations for the design are summarized in this remark. Firstly, since what is observable from the perspective of the time-division multiplexer is the variation of V over the time interval in which a controller is active, a goodness estimate of the active controller is defined in (35) in terms of V to capture a metric of the extent to which the active controller is being effective in achieving the stabilization objective. Secondly, since the goodness estimates are inherently stochastic indicators due to the presence of the disturbance input and the unknown adversarial modifications, (32) is used as a low pass filtering to attenuate such noise and obtain the switching likelihood states q_j, which provide more robust indicators of the goodness of each controller node. Thirdly, since the transient performance (as quantified by the goodness estimates in (35)) would be expected to be positive (and relatively large) for unattacked controllers and small/negative for attacked controllers, the switching probabilities are defined in (33) such that nodes with larger q_j would tend to correspond to higher probabilities than nodes with smaller q_j. The additional time-dependent term in (33) is introduced to guard against instances where intermittent noise (e.g., due to disturbance inputs) results in observations of temporary low goodness estimates of an unattacked controller leading to spurious reduction in the corresponding switching likelihood states. In such an instance, the presence of the time-dependent term in (33) ensures that the controller will be retested eventually since the switching probability for that controller node increases over time until it happens to be activated. The computed values $\hat{p}_j$ from (33) are normalized (to make sum equal to 1) to obtain the switching probabilities $p_j, j = 1, \ldots, N$. ◇

Some of the salient properties of the closed-loop system under time-division multiplexing with the ARS scheme are summarized below. For simplicity and brevity, we consider the case $\max(V_{(k+1)T}, \epsilon_V) = V_{(k+1)T}$ in the analysis below. This is reasonable since the small positive constant ϵ_V is introduced in (35) only to prevent numerical singularities when $V_{(k+1)T} \approx 0$ and is therefore only relevant when V reduces down to close to 0 (i.e., when the switching-based controller has successfully stabilized the system) while the analysis below addresses the transient behavior of the closed-loop system to show that the switching-based controller will indeed stabilize the system.

(1) **Increase of the switching likelihood states of unattacked controller nodes to large values:** Positive constants $\overline{W}$ and $\underline{q}$ exist such that if $w_{max} \leq \overline{W}$, then with probability 1, we have $\liminf_{t\to\infty} q_j \geq \underline{q}$ for all $j \in \{1, \ldots, N\} - A$. To see this, note that an inequality of the form (22) is satisfied with

$\lambda_i > 0$ for all unattacked controller nodes i where ϵ_i and $\overline{w}_i$ are as shown in (20) and (23), respectively. From (22) and noting that $\max(V_{(k+1)T}, \epsilon_V) = V_{(k+1)T}$ as noted above and $\max(V_{(k+1)T}, \epsilon_V) \geq \epsilon_V$, we see that the term appearing in the goodness estimate defined in (35) satisfies

$$\frac{V_{kT} - V_{(k+1)T}}{\max(V_{(k+1)T}, \epsilon_V)} \geq (e^{\lambda_i T} - 1) - \frac{(e^{\lambda_i T} - 1)}{\lambda_i \epsilon_V} \frac{\epsilon_i}{4} \mu_{(1,i)}^2(w_{max}). \tag{36}$$

Hence, defining $\underline{q} = \min\left(Q_{max}, \min_{i \in \{1,\ldots,N\}} \frac{e^{\lambda_i T} - 1}{2}\right)$, we have $Q_{[kT,(k+1)T)} \geq \underline{q}$ if the following inequality holds:

$$\frac{(e^{\lambda_i T} - 1)}{\lambda_i \epsilon_V} \frac{\epsilon_i}{4} \mu_{(1,i)}^2(w_{max}) \leq \frac{e^{\lambda_i T} - 1}{2}. \tag{37}$$

Defining the function $\overline{W}_{max}(z) = \sup_{w_{max} \leq z}\left(\frac{\epsilon_i}{2\lambda_i \epsilon_V} \mu_{(1,i)}^2(w_{max})\right)$ and defining the constant $\overline{W} = \sup\{z \in \mathcal{R}^+ | \overline{W}_{max}(z) \leq 1\}$, the inequality (37) is seen to definitely hold if $w_{max} \leq \overline{W}$. Since the inequality $Q_{[kT,(k+1)T)} \geq \underline{q}$ therefore holds over each time interval $[kT, (k+1)T)$ in which an unattacked controller $j = s_k$ is active, the switching likelihood state q_j computed using the filter (32) will also be greater than or equal to $\underline{q}$ in the limit as $t \to \infty$. Since this convergence property relates to the stochastic closed-loop system, this statement is seen to hold with probability 1 under the randomized switching.

(2) **Decrease of the switching likelihood states of attacked controller nodes to small values:** To model the minimum adversarial impact of an attacked controller node, we consider that over a time interval $[kT, (k+1)T)$ in which an attacked controller is active, we have an inequality of the form

$$V_{(k+1)T} \geq \tilde{\alpha}_k V_{kT} + \tilde{\beta}_k \tag{38}$$

with $\tilde{\alpha}_k \geq 1$ and $\tilde{\beta}_k \geq 0$ being constants (that could be time-varying, i.e., dependent on k). A Lyapunov inequality such as (38) is reasonable since one would expect that an adversary should at least have some level of destabilizing dynamic effect on the closed-loop system for it to even be considered an adversarial modification. With this adversarial model, it can be shown that with probability 1, the inequality $\limsup_{t \to \infty} q_j \leq \max\{Q_{min}, 0\}$ is satisfied for all $j \in A$. To see this, note that

$$\frac{V_{kT} - V_{(k+1)T}}{\max(V_{(k+1)T}, \epsilon_V)} \leq (\tilde{\alpha}_k^{-1} - 1) - \frac{\tilde{\alpha}_k^{-1} \tilde{\beta}_k}{\max(V_{(k+1)T}, \epsilon_V)} \leq 0, \tag{39}$$

from which it follows that $\limsup_{t \to \infty} q_j \leq \max\{Q_{min}, 0\}$ for all $j \in A$ with probability 1 under the randomized switching in the closed-loop system.

(3) **Eventual retesting of each controller node, i.e., infinitely many activations of all controllers:** For all $j \in \{1, \ldots, N\}$, the non-negative integers k for which $s_k = j$ are infinite in number with probability 1. This is a simple consequence of the time-dependent second term in (33). To show this statement using a proof by contradiction, consider that a controller node j is activated only a finite number of times, i.e., there exists a last time $t_{last,j}$ at which the controller node j is activated after which it is never activated. In this case, as $t \to \infty$, it can be shown from (33) and (34) that $\liminf_{t \to \infty} p_j \geq \frac{1}{N}$. To see this, note that any other controller nodes i activated after time $t_{last,j}$ will have p_i smaller than p_j while controller nodes i that were last activated before time $t_{last,j}$ will asymptotically have $\lim_{t \to \infty} \frac{p_i}{p_j} = 1$ since $\lim_{t \to \infty} \frac{t-a}{t-b} = 1$ for any real numbers a and b. Therefore, p_j will increase asymptotically to $\frac{1}{N}$ or higher implying that with probability 1, the controller node j will be activated again. This contradicts the assumption that a finite $t_{last,j}$ is the last ever activation time of controller node j implying that all controllers will be activated infinitely many times (possibly very infrequently however as discussed in (4)).

(4) **Asymptotically low frequencies of activation of attacked controllers:** Picking $Q_{min} \leq 0$ and using (2) above, it can be shown that given any $\Delta_A > 0$, the constant c_0 can be picked small enough to make the asymptotic (as $t \to \infty$) mean time (in units of number of time intervals of length T) between activations of an attacked controller larger than or equal to Δ_A. To show this, consider an attacked controller node j; using (2), it is seen that asymptotically $\hat{p}_j \approx c_0(t - t_{last,j})$ with $t_{last,j}$ being the last activation time of controller node j before time t. We want to find the expected time (in units of T) before the next activation of controller node j. Denote the next activation time by $t_{next,j} \triangleq t_{last,j} + n_{next,j}T$. We want to find $E(n_{next,j})$. It can be seen that to find the form of the dependence of a lower bound of $E(n_{next,j})$ on the parameter c_0, it suffices to consider that $\sum_{\substack{i=1 \\ i \neq j}}^{N} p_i$ is some constant p_0. This is because if any other controller nodes i have not been activated recently and for which therefore $\hat{p}_i$ has a relatively large component $c_0(t - t_{last,i})$, the presence of such controller nodes will only tend to compete for activation with the controller node j thereby increasing $E(n_{next,j})$. Denote by ζ_1 the probability that the controller node j will be activated in the next time interval after $t_{last,j}$. It is seen that $\zeta_1 = \frac{\eta}{1+\eta}$ where η denotes $\frac{cT_0}{p_0}$. Denoting by ζ_2 the probability that controller node j will only be activated in the second time interval after $t_{last,j}$ and not in the first time interval (i.e., that $n_{next,j} = 2$), we have $\zeta_2 = (1-\zeta_1)\frac{2\eta}{1+2\eta}$. Similarly, denoting by ζ_k the probability that $n_{next,j} = k$, we have

$$\zeta_k = (1 - \sum_{i=1}^{k-1} \zeta_i) \frac{k\eta}{1 + k\eta}. \tag{40}$$

Note that from (40), we have $\zeta_k \leq k\eta$ for all k. Now, pick any $\epsilon \in (0, 1)$ and using the given $\Delta_A > 0$, define $M = \frac{\Delta_A}{1-\epsilon}$. Then, picking $c_0 \leq \frac{2\epsilon p_0}{M(M+1)T}$, we have $\eta \leq \frac{2\epsilon}{M(M+1)}$ and $\sum_{k=1}^{M} \zeta_k \leq \sum_{k=1}^{M} k\eta \leq \epsilon$. Since $\sum_{k=1}^{\infty} \zeta_k = 1$, we have $\sum_{k=M+1}^{\infty} \zeta_k \geq 1 - \epsilon$ implying that $\sum_{k=M+1}^{\infty} k\zeta_k \geq (M+1)(1-\epsilon)$. Since by the definition of expected value, we have $E(n_{next,j}) = \sum_{k=1}^{\infty} k\zeta_k$, we see that $E(n_{next,j}) \geq \sum_{k=M+1}^{\infty} k\zeta_k \geq (M+1)(1-\epsilon) > \Delta_A$ from the choice of M above. Therefore, by picking c_0 small enough, the frequency of activation of attacked controllers can be asymptotically made arbitrarily small.

(5) **Asymptotic boundedness and convergence of closed-loop system states:** Given (1)–(4), it follows that the state x of the closed-loop system remains uniformly bounded over the time interval $[0, \infty)$ with probability 1. To see this, note from (4) that the mean time between activations of attacked controller nodes can be asymptotically made larger than any given Δ_A. Hence, as $t \to \infty$, each attacked controller node is active on around a fraction $\frac{1}{\Delta_A}$ of the time intervals while the unattacked controller nodes considered all together are active for around a fraction $1 - \frac{n_A}{\Delta_A}$ of the time intervals where n_A denotes the number of attacked controllers. Since Δ_A can be made arbitrarily large by picking c_0 appropriately small, this implies that asymptotically the effects of the attacked controllers can be arbitrarily attenuated by appropriate choice of c_0 and the region of convergence of the system state is governed essentially by the disturbance input w and the performance of the unattacked controllers. Furthermore, under the case that the disturbance w goes to 0 as $t \to \infty$, it is seen that the closed-loop system state converges (with probability 1) as $t \to \infty$ to within a region $|x| \leq \epsilon_A$ where ϵ_A is a constant dependent on Δ_A such that if $\Delta_A \to \infty$ (which from (4) is equivalent to picking $c_0 \to 0$), then $\epsilon_A \to 0$.

Remark 9. While the analysis above considered the case of a common Lyapunov function V shared among all the controller nodes, the ARS design in (32)–(35) can also be applied under the case discussed in Remarks 3 and 6 of separate Lyapunov functions $V_i, i = 1, \ldots, N$, for the control laws at the different controller nodes. The design of the goodness estimates in (35) still applies under this case with $V_{s_k,kT} \triangleq V_{s_k}(x(kT))$ and $V_{s_k,(k+1)T} \triangleq V_{s_k}(x((k+1)T))$ being used in place of V_{kT} and $V_{(k+1)T}$, respectively, since what is being measured is the observed efficacy of the controller utilized over time interval $[kT, (k+1)T)$ in terms of a scalar metric of relevance for that controller, i.e., V_{s_k}. Using these goodness estimates, the switching likelihood states can be defined as in (32) and the switching probabilities can be defined as shown in (33) and (34). The subsequent analysis of the convergence properties of the switching likelihood states and the dynamic closed-loop system can be carried out analogously as discussed in this section. The details are omitted for brevity. ◇

Remark 10. While the analysis in this paper focused on the resilient control application (in the state-feedback setting as formalized in Assumption A1), the proposed ARS approach can be conceptually applied to a secure state estimation problem as well, i.e., to enable resiliency of state estimation under adversarial modifications of subsets of available sensors. Consider, for example, m multiple redundant sensors (which could measure the same or different physical signals) such that a given dynamic system is observable using any subset of sensors. Then denoting the sensor measurements as $y_1, \ldots, y_m$, the goodness estimation concept discussed in this section could be applied using indicators of goodness of sensors based on, for example, the residuals $y_i - \hat{y}_i$ where signals $\hat{y}_i$ are computed using dynamic observers. Then, the ARS approach could be applied using these dynamic goodness estimates of sensors during run-time to iteratively tune out sensors detected as bad so as to improve state estimation resiliency under sensor attacks. The details are omitted for brevity. ◇

5. Simulation studies

To evaluate the efficacy of the proposed switching controller approaches based on time-domain multiplexing using RRS and ARS schemes, we consider two illustrative examples below, the first with a simple third-order system and the second with a more real-world CPS example of a single-machine-infinite-bus (SMIB) system.

Example 1. Consider the system with dynamics:

$$\begin{aligned}\dot{x}_1 &= x_2\\ \dot{x}_2 &= -x_2 + \sin(0.1x_1)w + x_3\\ \dot{x}_3 &= -x_3 + u\end{aligned} \tag{41}$$

where the system state is $x = [x_1, x_2, x_3]^T$, u is the control input, and w is the disturbance input. Considering the linear system obtained with $w = 0$, the controller can be designed as $u = Kx$ with the controller gain vector K picked to place the closed-loop poles at any desired locations. For example, taking the desired pole locations as -5 and $-3 \pm j$, the controller gain vector is obtained as $K = [-65, -33, -9]$. With this controller gain vector, the linear closed-loop system with $w = 0$ is given by $\dot{x} = A_c x$ with

$$A_c = \begin{bmatrix} 0 & 1 & 0\\ 0 & -1 & 1\\ -65 & -33 & -10\end{bmatrix}. \tag{42}$$

Solving the Lyapunov equation $PA_c + A_c^T P = -\text{diag}(1, 1, 1)$ where diag denotes a diagonal matrix with the indicated elements on the diagonal and defining $V = 0.02x^T Px$, the goodness estimate $Q_{[kT,(k+1)T)}$ is defined as discussed in Section 4 as $V_{kT} - V_{(k+1)T}$. The controller magnitude limit is defined as $u_{max} = 100$. For the simulation study, consider $w = \sin(0.2t)$. The adversary is modeled as setting the control signal to a constant given by u_{max}. The switching time T for the time-division multiplexer is picked to be 0.05 s. The parameters in the ARS controller are picked as $\alpha = 0.95$, $c_0 = 10^{-4}$, $Q_{min} = -2$, $Q_{max} = 2$, and $\epsilon_V = 10^{-3}$. The initial condition is picked as $x = [5, 2, 2]^T$. With a single unattacked controller node, the closed-loop signals x and u will go to zero rapidly since A_c is a strict Hurwitz matrix. On the other hand, with a single adversarially modified controller node, it can be seen that x_1 will grow unbounded since a non-zero value of u at steady-state will drive x_2 to a non-zero steady-state value even in the absence of the disturbance input w resulting in unbounded growth of x_1. Simulation plots for single unattacked and attacked nodes are omitted for brevity. Now, using $N = 4$ parallel controller nodes with $n_A = 2$ nodes being adversarially modified starting at time $T_{adv} = 10$ s, it is seen from Fig. 2 that unbounded growth of x_1 is prevented even with RRS. Since only a subset of the controllers are adversarially modified, it is seen that the stabilizing effect of the good controllers is able to compensate for the destabilizing effect of the bad controllers during the round-robin switching among all the controllers. However, there are considerable oscillations (and non-zero offset) in x_1. It is seen in Fig. 3 that the adversarial impact by the attacker can be reduced using ARS and x_1 can be regulated to 0. The switching likelihood states q_j and switching probabilities p_j are computed as discussed in Section 4 using Eqs. (32), (33), and (34). As discussed in Section 4, the dynamic update of the switching likelihood states ensures that over time, the good controllers are likely to be more frequently picked than the bad controllers. The dynamic evolution of the switching probabilities is shown in Fig. 4. Using these switching probabilities for randomized switching among the controllers, it is seen in Fig. 3 that ARS tunes out the attacked controller nodes over time. The efficacy of RRS and ARS are discussed in greater detail in the "real-world" example below.

Example 2. Consider the dynamics of a SMIB system [48,49]

$$\begin{aligned}\dot{\delta} &= \omega\\ \dot{\omega} &= \frac{1}{2H}[-D\omega + \omega_0(P_{m0} - P_e)]\\ \dot{E}_{q1} &= \frac{1}{T_{d0}}[E_f - E_q - \hat{E}_q]\end{aligned} \tag{43}$$

where δ, ω, and E_{q1} denote the power angle, relative speed, and quadrature-axis transient electromotive force (EMF), respectively, of the generator. E_q denotes the quadrature-axis EMF, $\hat{E}_q$ the noise/disturbance, and E_f the equivalent EMF in the excitation coil. P_{m0} is the mechanical input power. ω_0 is the synchronous machine speed ($\omega_0 = 2\pi f_0$). P_e is the active electrical power delivered by the generator. T_{d0} is the direct-axis transient short circuit time constant. The parameters D and H are the per unit damping constant and inertia constant, respectively. P_e, E_q, and E_{q1} are related through the algebraic equations [48]

$$P_e = \frac{V_s E_q \sin(\delta)}{x_{ds}} \tag{44}$$

$$E_q = \frac{x_{ds}}{x_{ds1}} E_{q1} - \frac{(x_d - x_{d1})}{x_{ds1}} V_s \cos(\delta) \tag{45}$$

where V_s is the infinite bus voltage, and x_d, x_{d1}, x_{ds}, and x_{ds1} are reactance parameters as in [48]. The control input to system (43) is $u = E_f$. A controller based on external feedback linearization can be designed for system (43) as [48]:

$$v_f = K[\delta - \delta_0, \omega, P_e - P_{m0}]^T + P_{m0} \tag{46}$$

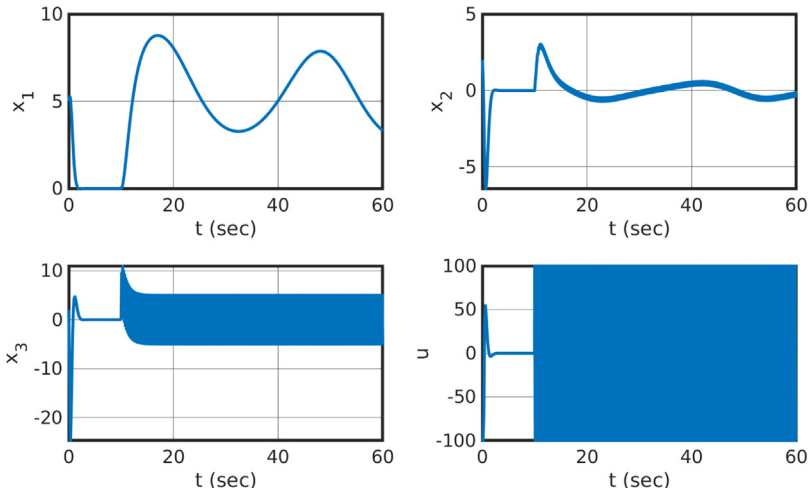

Fig. 2. Simulation of closed-loop system for Example 1 with RRS ($N = 4$) with adversarial modification of controllers 1 and 2 from $T_{adv} = 10$ s.

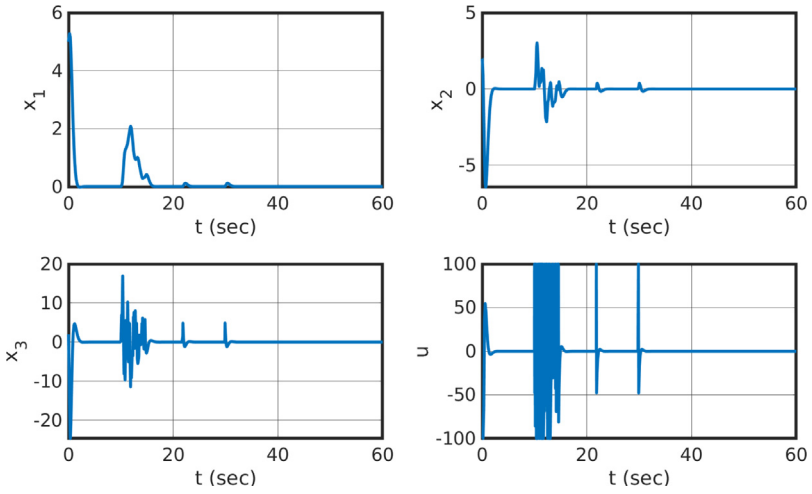

Fig. 3. Simulation of closed-loop system for Example 1 with ARS ($N = 4$) with adversarial modification of controllers 1 and 2 from $T_{adv} = 10$ s.

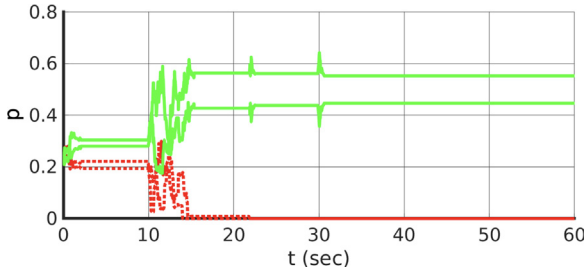

Fig. 4. Controller switching probabilities $(p_i(t), i = 1, \ldots, N)$ for simulation with ARS in Fig. 3. The "ground truth" of attacked and unattacked controllers are denoted with red dotted and green solid lines, respectively.

$$u = \frac{1}{I_q}\left(v_f - \frac{(x_d - x_{d1})}{x_{ds1}} T_{d01} I_q V_s \sin(\delta)\omega - \frac{V_s T_{d01}}{x_{ds}} E_q \cos(\delta)\omega\right) \tag{47}$$

where $I_q = \frac{V_s \sin(\delta)}{x_{ds}}$ and $T_{d01} = \frac{x_{ds1}}{x_{ds}} T_{d0}$. K in (46) is a gain vector of dimension 1×3. δ_0 is the desired operating point for the power angle δ. As in [48], the parameters of the SMIB system are given by $P_{m0} = 0.9$ p.u., $\omega_0 = 314.159$ rad/s, $T_{d0} = 6.9$ s, $D = 5$ p.u., $H = 4$ s, $V_s = 1.0$ p.u., $x_d = 1.863$, $x_{d1} = 0.257$, $x_{ds} = 2.2327$, and $x_{ds1} = 0.6267$. As in [48], the gain vector K is chosen to be $K = [19.3, 6.43, -47.6]$. Also, $\delta_0 = 75^\circ = 1.309$ rad and $u_{max} = 2.3$ p.u. The disturbance input signal is defined as $w = \hat{E}_q$ and is chosen to be $w = 0.01\cos(0.5\pi t)$.

As in Example 1, the switching time is chosen as $T = 0.05$ sec for the time-division multiplexer. Considering the structure of the feedback linearization control law in (46) and (47), the goodness estimate $Q_{[kT,(k+1)T)}$ is defined using $\bar{x}^T P \bar{x}$ where $\bar{x} = [\delta - \delta_0, \omega, P_e - P_{m0}]$. The 3×3 matrix P is computed by solving the Lyapunov equation $P\bar{A} + \bar{A}^T P = -10^3 \mathrm{diag}(25, 5, 2)$ where $\bar{A}$ is defined based on the closed-loop dynamics of $\bar{x}$ given by

$$\bar{A} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & -\frac{D}{2H} & -\frac{\omega_0}{2H} \\ 0 & 0 & -\frac{1}{T_{d01}} \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ \frac{1}{T_{d01}} \end{bmatrix} K. \tag{48}$$

The parameters α, c_0, Q_{min}, Q_{max}, and ϵ_V in the ARS controller are picked to be the same as in Example 1.

From a simulation with a single non-attacked controller node shown in Fig. 5, it can be observed that except for small oscillations (due to disturbance input $\hat{E}_q$), the baseline controller achieves very good regulation performance. To evaluate the possible performance degradation that an adversary can effect, a simulation with a single controller node, that is adversarially modified starting at time $T_{adv} = 10$ s, is shown in Fig. 6. The adversary is modeled in the simulation studies below as holding the control signal to a constant given by $0.75u_{max}$. It is seen in

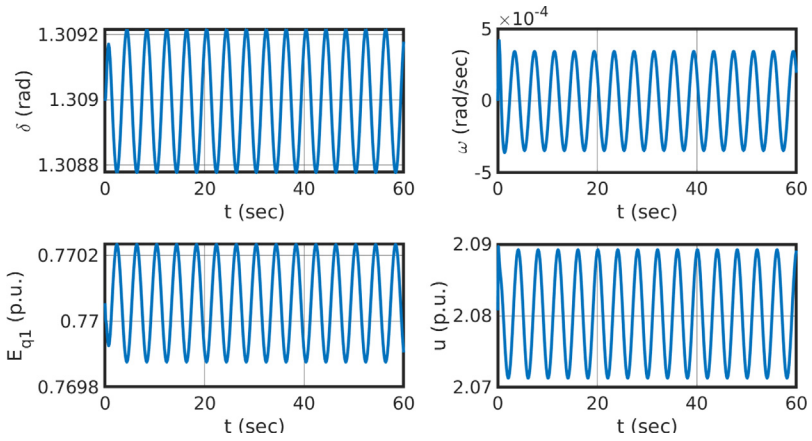

Fig. 5. Simulation of closed-loop system for Example 2 with a single unattacked controller implementation.

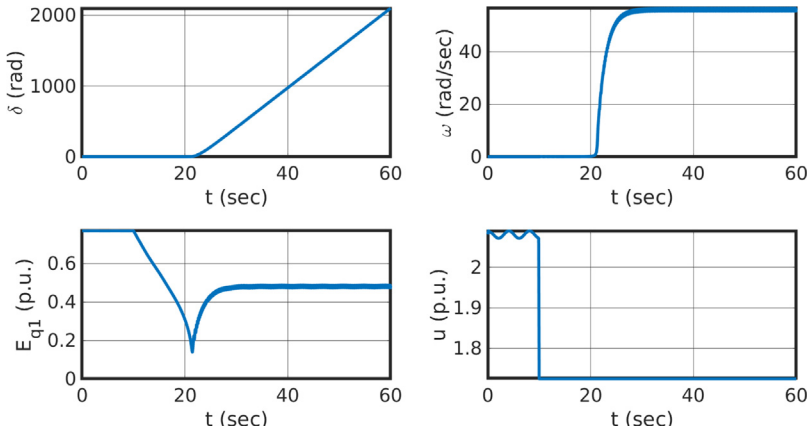

Fig. 6. Simulation of closed-loop system for Example 2 with a single controller implementation, that is adversarially modified from $T_{adv} = 10$ s.

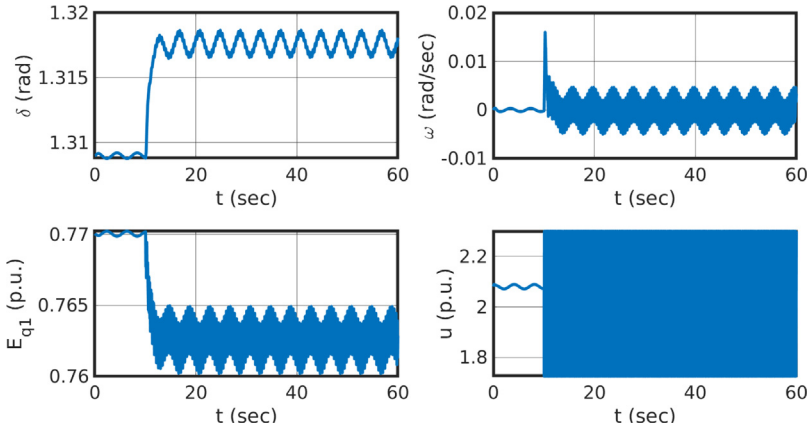

Fig. 7. Simulation of closed-loop system for Example 2 with RRS ($N = 8$) with adversarial modification of controllers 2, 4, and 7 from $T_{adv} = 10$ s.

Fig. 6 that using the adversarially injected input, the attacker can dramatically impact system stability (specifically, unbounded drift of δ seen in Fig. 6). However, through round-robin switching among $N = 8$ parallel controller nodes, it is seen that (Fig. 7) a considerable amount of the closed-loop system performance can be regained even under adversarial modifications of $n_A = 3$ nodes. Since only $n_A = 3$ out of $N = 8$ controllers are adversarially modified, the good controllers are active for over half the total time in the closed-loop CPS enabling the stabilizing effect of the good controllers to compensate for the destabilizing effect of the bad controllers during round-robin switching. However, it is seen in Fig. 7 that there are still significant oscillations compared to Fig. 5. Using ARS, Fig. 8 shows that the adversarial impact can be further reduced. The switching states (i.e., signal given by s_k over time intervals $[kT, (k+1)T)$) for RRS and ARS are shown in Figs. 9 and 10, respectively. As expected, the switching pattern in Fig. 10 is non-uniform (unlike RRS in Fig. 9) tending to avoid the adversarially modified controller nodes. This avoidance of attacked controller nodes is enabled by the estimation of the switching likelihood states q_j and switching probabilities p_j as

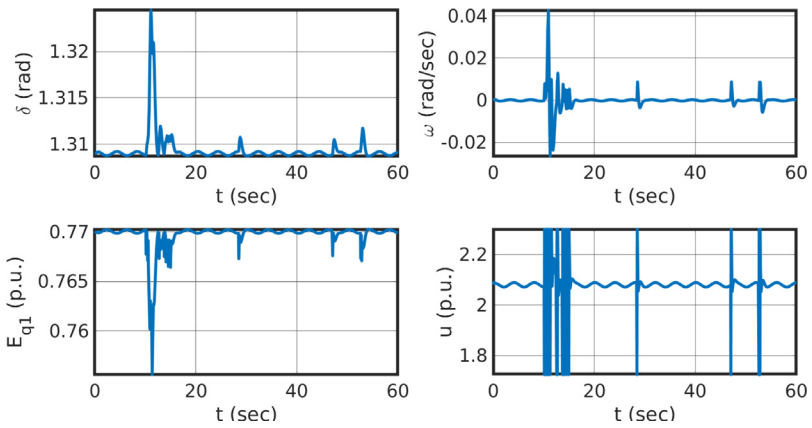

Fig. 8. Simulation of closed-loop system for Example 2 with ARS ($N = 8$) with adversarial modification of controllers 2, 4, and 7 from $T_{adv} = 10$ s.

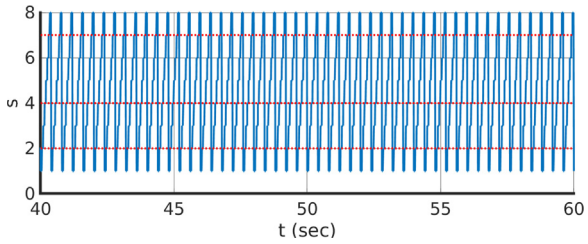

Fig. 9. Controller switching state ($s(t)$) for simulation with RRS in Fig. 7. Attacked nodes (2, 4, 7) are denoted with horizontal red dotted lines.

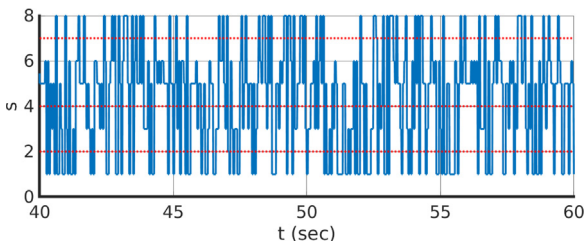

Fig. 10. Controller switching state ($s(t)$) for simulation with ARS in Fig. 8. Attacked nodes (2, 4, 7) are denoted with horizontal red dotted lines.

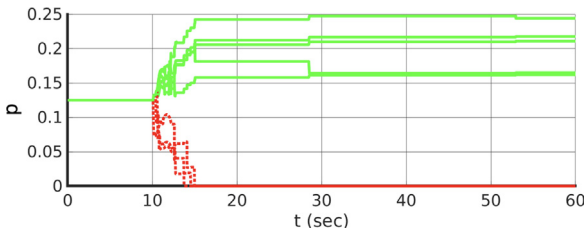

Fig. 11. Controller switching probabilities ($p_i(t), i = 1, \ldots, N$) for simulation with ARS in Fig. 8. As in Fig. 4, attacked and unattacked controllers are denoted with red dotted and green solid lines, respectively.

discussed in Section 4 using Eqs. (32), (33), and (34). By evaluating the observed performance of the activated controller over each switching time interval, the switching likelihood states are dynamically updated and used to compute the switching probabilities at each switching time so as to over time favor picking the apparently good controller nodes rather than the apparently bad controller nodes. As seen in Fig. 11, the dynamic updates of the switching likelihood states q_j, tend to reduce the values of q_j (and therefore p_j) for controller nodes detected as having low goodness and therefore to attenuate effects of attacked controller nodes over time. The "ground truth" denoting the *a priori unknown* information as to which controller nodes are unattacked/attacked is also shown in Fig. 11 using two different line types (attacked: red dotted, unattacked: green solid). It is seen that the switching probabilities for attacked controllers are reduced over time while the switching probabilities for unattacked controllers remain relatively large. In similar simulations performed with number of attacked nodes increased to $n_A = 4$, it is seen that while the round-robin switcher (Fig. 12) results in significant growing drift of δ, ARS (Fig. 13) still retains performance close to the unattacked baseline. The switching state s and the switching probabilities p_j for the simulation in Fig. 13 are shown in Figs. 14 and 15, respectively, and it is observed that the adversarially modified controllers can be dynamically tuned out over time by the ARS controller (by dynamically adapting the corresponding switching likelihoods using on-line observations of the controller nodes' relative goodness).

6. Conclusion

The possibility of using multiple parallel controller implementations and dynamically switching among the controller nodes at run-time to improve resiliency to adversarial modifications was considered. In particular, RRS and ARS methodologies were considered. The efficacy of the proposed approach was shown in simulation studies on a simple third-order system and a more real-world example of a SMIB system. It was shown that if a cyber-attacker arbitrarily changes a subset of controllers, the overall closed-loop system can still be kept stable and impact of adversarial modifications to controllers can be bounded. It was shown that over time, the adaptation of switching likelihoods enables reduction of impact to the CPS due to adversarially modified controllers. Furthermore, the likelihood adaptation has components to adapt to changes over time of which controllers are adversarially modified. Future work will address applicability of the methodology to additional classes of systems (e.g., decentralized systems with distributed controller implementations) and analysis of more precise bounds on adversarial CPS impact including in output-feedback scenarios.

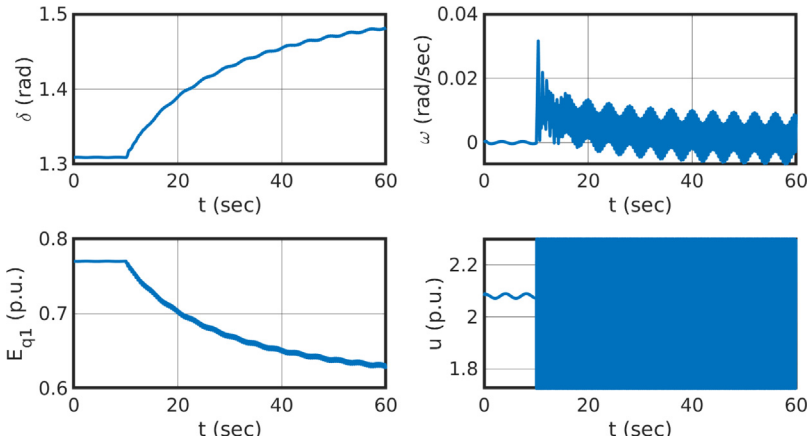

Fig. 12. Simulation of closed-loop system for Example 2 with RRS ($N = 8$) with adversarial modification of controllers 2, 4, 6, and 7 from $T_{adv} = 10$ s.

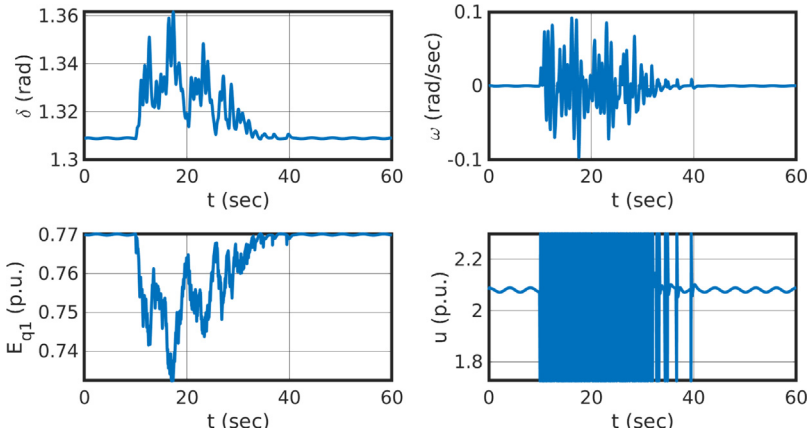

Fig. 13. Simulation of closed-loop system for Example 2 with ARS ($N = 8$) with adversarial modification of controllers 2, 4, 6, and 7 from $T_{adv} = 10$ s.

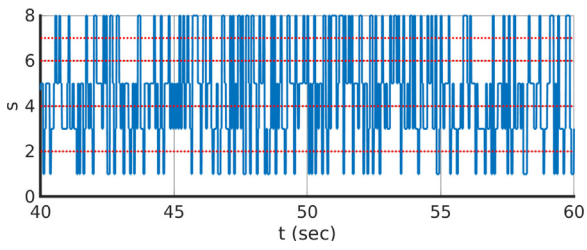

Fig. 14. Controller switching state ($s(t)$) for simulation with ARS in Fig. 13. Attacked nodes (2, 4, 6, 7) are denoted with horizontal red dotted lines.

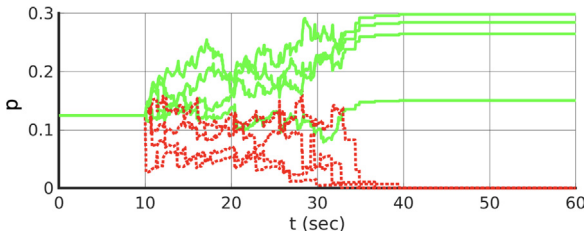

Fig. 15. Controller switching probabilities ($p_i(t), i = 1, \ldots, N$) for simulation with ARS in Fig. 13. As in Fig. 4, attacked and unattacked controllers are denoted with red dotted and green solid lines, respectively.

CRediT authorship contribution statement

Prashanth Krishnamurthy: Conceptualization, Methodology, Software, Investigation, Writing – original draft, Writing – review & editing. **Farshad Khorrami:** Conceptualization, Methodology, Software, Investigation, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] P. Krishnamurthy, F. Khorrami, Adaptive randomized controller switching for resilient cyber-physical systems, in: Proc. of the IEEE Conference on Control Technology and Applications, Montreal, Canada, 2020, pp. 738–743.

[2] R. Kisner, W. Manges, L. Macintyre, J. Nutaro, J. Munro Jr., P. Ewing, M. Howlader, T. Kuruganti, R. Wallace, M. Olama, Cybersecurity through Real-Time Distributed Control Systems, Oak Ridge National Laboratory, 2010.

[3] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, Guide to Industrial Control Systems (ICS) Security, NIST, 2015, NIST Special Publication 800-82, rev. 2.

[4] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadeghi, M. Maniatakos, R. Karri, The cybersecurity landscape in industrial control systems, Proc. IEEE 104 (5) (2016) 1039–1057.

[5] D. Bodeau, R. Graubart, Cyber Resiliency Design Principles, MITRE Technical Report 17-0103, MITRE, 2017.

[6] F. Khorrami, P. Krishnamurthy, R. Karri, Cybersecurity for control systems: A process-aware perspective, IEEE Des. Test Mag. 33 (5) (2016) 75–83.
[7] D. Serpanos, Secure and resilient industrial control systems, IEEE Des. Test 35 (1) (2018) 90–94.
[8] D. Serpanos, M.T. Khan, H. Shrobe, Designing safe and secure industrial control systems: A tutorial review, IEEE Des. Test 35 (3) (2018) 73–88.
[9] P. Krishnamurthy, F. Khorrami, R. Karri, D. Paul-Pena, H. Salehghaffari, Process-aware covert channels using physical instrumentation in cyber-physical systems, IEEE Trans. Inf. Forensics Secur. 13 (11) (2018) 2761–2771.
[10] H. Salehghaffari, F. Khorrami, Resilient power grid state estimation under false data injection attacks, in: Proc. of the IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, 2018, pp. 1–5.
[11] P. Krishnamurthy, H. Salehghaffari, S. Duraisamy, R. Karri, F. Khorrami, Stealthy rootkits in smart grid controllers, in: Proc. of IEEE Intl. Conf. on Computer Design, Abu Dhabi, UAE, 2019.
[12] N. Patel, P. Krishnamurthy, S. Garg, F. Khorrami, Adaptive adversarial videos on roadside billboards: Dynamically modifying trajectories of autonomous vehicles, in: Proc. of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Macau, China, 2019, pp. 5916–5921.
[13] C. Bakker, A. Bhattacharya, S. Chatterjee, D.L. Vrabie, Hypergames and cyber-physical security for control systems, ACM Trans. Cyber-Phys. Syst. 4 (4) (2020).
[14] A. Keliris, H. Salehghaffari, B. Cairl, P. Krishnamurthy, M. Maniatakos, F. Khorrami, Machine learning-based defense against process-aware attacks on industrial control systems, in: Proc. of the IEEE Intl. Test Conf., Fort Worth, TX, 2016, pp. 1–10.
[15] S.Z. Yong, M. Zhu, E. Frazzoli, Switching and data injection attacks on stochastic cyber-physical systems: Modeling, resilient estimation, and attack mitigation, ACM Trans. Cyber-Phys. Syst. 2 (2) (2018).
[16] Y. Shoukry, M. Chong, M. Wakaiki, P. Nuzzo, A. Sangiovanni-Vincentelli, S.A. Seshia, J.A.P. Hespanha, P. Tabuada, SMT-based observer design for cyber-physical systems under sensor attacks, ACM Trans. Cyber-Phys. Syst. 2 (1) (2018).
[17] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N.O. Tippenhauer, H. Sandberg, R. Candell, A survey of physics-based attack detection in cyber-physical systems, ACM Comput. Surv. 51 (4) (2018) 76:1–76:36.
[18] N. Patel, A.N. Saridena, A. Choromanska, P. Krishnamurthy, F. Khorrami, Adversarial learning-based on-line anomaly monitoring for assured autonomy, in: Proc. of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Madrid, Spain, 2018, pp. 6149–6154.
[19] P. Krishnamurthy, R. Karri, F. Khorrami, Anomaly detection in real-time multi-threaded processes using hardware performance counters, IEEE Trans. Inf. Forensics Secur. 15 (2020) 666–680.
[20] N. Patel, A.N. Saridena, A. Choromanska, P. Krishnamurthy, F. Khorrami, Learning-based real-time process-aware anomaly monitoring for assured autonomy, IEEE Trans. Intell. Veh. 5 (4) (2020) 659–669.
[21] N.K. Patel, P. Krishnamurthy, H. Amrouch, J. Henkel, M. Shamouilian, R. Karri, F. Khorrami, Towards a new thermal monitoring based framework for embedded CPS device security, IEEE Trans. Dependable Secure Comput. (2020) (in press). Early access version online on IEEE, Feb. 2020.
[22] V. Lesi, I. Jovanov, M. Pajic, Integrating security in resource-constrained cyber-physical systems, ACM Trans. Cyber-Phys. Syst. 4 (3) (2020).
[23] M.T. Khan, M. Pinzger, D. Serpanos, H. Shrobe, Runtime protection of real-time critical control applications against known threats, IEEE Des. Test 37 (6) (2020) 88–95.
[24] D.M. Blough, G.F. Sullivan, A comparison of voting strategies for fault-tolerant distributed systems, in: Proc. of the IEEE Symp. on Reliable Distributed Systems, Huntsville, AL, USA, 1990, pp. 136–145.
[25] E.P. Kim, N.R. Shanbhag, Soft N-modular redundancy, IEEE Trans. Comput. 61 (3) (2012) 323–336.
[26] P. Ulbrich, M. Hoffmann, R. Kapitza, D. Lohmann, W. Schroder-Preikschat, R. Schmid, Eliminating single points of failure in software-based redundancy, in: Proc. of the European Dependable Computing Conf., Sibiu, Romania, 2012, pp. 49–60.
[27] R.I. Williams, Hardware configuration of redundant safety integrated systems, Control Eng. (2013).
[28] J.P.G. Sterbenz, D. Hutchison, E.K. Çetinkaya, A. Jabbar, J.P. Rohrer, M. Schöller, P. Smith, Redundancy, diversity, and connectivity to achieve multilevel network resilience, survivability, and disruption tolerance, Telecommun. Syst. 56 (1) (2014) 17–31.
[29] K. Austin, Applying network best practices via ethernet network redundancy, Control Eng. (2016).
[30] J. Park, R. Ivanov, J. Weimer, M. Pajic, S.H. Son, I. Lee, Security of cyber-physical systems in the presence of transient sensor faults, ACM Trans. Cyber-Phys. Syst. 1 (3) (2017).
[31] Y. Xu, I. Koren, C.M. Krishna, AdaFT: A framework for adaptive fault tolerance for cyber-physical systems, ACM Trans. Embedded Comput. Syst. 16 (3) (2017).
[32] K.S. Son, D.H. Kim, G.Y. Park, H.G. Kang, Availability analysis of safety grade multiple redundant controller used in advanced nuclear safety systems, Ann. Nucl. Energy 111 (2018) 73–81.
[33] A. Laszka, W. Abbas, Y. Vorobeychik, X. Koutsoukos, Synergistic security for the industrial internet of things: Integrating redundancy, diversity, and hardening, in: Proc. of the IEEE Intl. Conf. on Industrial Internet, Seattle, WA, USA, 2018, pp. 153–158.
[34] G. Gualandi, E. Casalicchio, Use of redundancy in the design of a secure software defined industrial control application, in: Proc. of the Intl. Conf. on Software Defined Systems, Rome, Italy, 2019, pp. 102–109.
[35] R. Ma, P. Cheng, Z. Zhang, W. Liu, Q. Wang, Q. Wei, Stealthy attack against redundant controller architecture of industrial cyber-physical system, IEEE Internet Things J. 6 (6) (2019) 9783–9793.
[36] ControlLogix Redundancy System, Allen-Bradley, 2006, https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um523_-en-p.pdf.
[37] CODESYS redundancy toolkit: Two Industrial IEC 61131-3 controllers for one single application make the application fail safe, https://www.codesys.com/products/codesys-runtime/redundancy-toolkit.html.
[38] A. Kanellopoulos, K.G. Vamvoudakis, Switching for unpredictability: A proactive defense control approach, in: Proc. of the American Control Conference, Philadelphia, PA, USA, 2019, pp. 4338–4343.
[39] A. Kanellopoulos, K.G. Vamvoudakis, A moving target defense control framework for cyber-physical systems, IEEE Trans. Automat. Control 65 (3) (2020) 1029–1043.
[40] L. Zhai, K.G. Vamvoudakis, Data-based and secure switched cyber–physical systems, Systems Control Lett. 148 (2021) 104826.
[41] Y. Li, Z. Lin, A switching anti-windup design based on partitioning of the input space, Systems Control Lett. 88 (2016) 39–46.
[42] Y. Xie, Z. Lin, Global stabilization of a chain of integrators by a switching event-triggered bounded control, in: Proc. of the American Control Conference, Seattle, WA, USA, 2017, pp. 3688–3693.
[43] S. Su, Y. Wei, Z. Lin, Stabilization of discrete-time linear systems with an unknown time-varying delay by switched low-gain feedback, IEEE Trans. Automat. Control 64 (5) (2019) 2069–2076.
[44] L. An, G.-H. Yang, Secure state estimation against sparse sensor attacks with adaptive switching mechanism, IEEE Trans. Automat. Control 63 (8) (2018) 2596–2603.
[45] M. Porfiri, D.G. Roberson, D.J. Stilwell, Fast switching analysis of linear switched systems using exponential splitting, SIAM J. Control Optim. 47 (5) (2008) 2582–2597.
[46] W. Wang, D. Nesic, Input-to-state stability and averaging of linear fast switching systems, IEEE Trans. Automat. Control 55 (5) (2010) 1274–1279.
[47] C. Pedicini, L. Iannelli, F. Vasca, The averaging method for control design and stability analysis of practical switched systems, in: Proc. of the IEEE Intl. Conf. on Control Applications, Dubrovnik, Croatia, 2012, pp. 1285–1290.
[48] Y. Wang, D.J. Hill, R.H. Middleton, L. Gao, Transient stability enhancement and voltage regulation of power systems, IEEE Trans. Power Syst. 8 (2) (1993) 620–627.
[49] S. Jain, F. Khorrami, B. Fardanesh, Adaptive nonlinear excitation control of power systems with unknown interconnections, IEEE Trans. Control Syst. Technol. 2 (4) (1994) 436–446.