Switched Zero Dynamics Attacks on Sampled-Data Systems with Non-Uniform Sampling Vulnerability and Countermeasures

Wolleswinkel, Bart; Mazo, Manuel; Ferrari, Riccardo

DOI
10.1145/3746643

Publication date
2025

Document Version
Final published version

Published in
ACM Transactions on Cyber-Physical Systems

Switched Zero Dynamics Attacks on Sampled-Data Systems with Non-Uniform Sampling: Vulnerability and Countermeasures

BART WOLLESWINKEL, MANUEL MAZO, JR., and RICCARDO FERRARI, Delft Center for Systems and Control (DCSC), Delft University of Technology, Delft, The Netherlands

We describe a new variant of zero dynamics attack (ZDA), what we call a *switched* ZDA, targeting linear time-invariant (LTI) sampled-data systems with non-uniform sampling. Specifically, we consider continuous-time systems and construct attacks that exploit the unstable sampling zeros resulting from a zero-order hold (ZOH) mechanism. These attacks can be constructed by strong adversaries who have knowledge of the plant dynamics, with the additional requirement that they can determine the next sampling instant. We provide sufficient conditions when cyber-physical systems are vulnerable to switched ZDAs, and prove that these attacks can be disruptive while remaining stealthy. We also provide two possible countermeasures that make switched ZDAs ineffective. The first countermeasure revolves around creating a mismatch between the next sampling instant as predicted by the adversary and the true one, which makes the switched ZDAs no longer stealthy. The second countermeasure relies on increasing the inter-sample times such that the system no longer contains unstable sampling zeros, making the switched ZDA no longer disruptive. We demonstrate the vulnerability of sampled-data systems with non-uniform sampling to switched ZDAs in several illustrative examples, and exemplify the effectiveness of the proposed countermeasures.

CCS Concepts: • **Security and privacy** → **Embedded systems security**; *Intrusion detection systems*; • **Computer systems organization** → *Embedded software*;

Additional Key Words and Phrases: Networked Control System (NCS), Secure Control, Zero Dynamics Attack (ZDA), Sampled-Data System, Aperiodic Sampling, Event-Triggered Control (ETC)

ACM Reference format:
Bart Wolleswinkel, Manuel Mazo, Jr., and Riccardo Ferrari. 2025. Switched Zero Dynamics Attacks on Sampled-Data Systems with Non-Uniform Sampling: Vulnerability and Countermeasures. *ACM Trans. Cyber-Phys. Syst.* 9, 3, Article 32 (August 2025), 23 pages.
https://doi.org/10.1145/3746643

1 Introduction

Over the past decades, there has been an increase in the interaction between digital technologies and physical processes. Systems in which the physical layer is tightly interconnected with digital

This work has been partially supported by the EU Horizon program through the project TWAIN, grant id 101122194.
Authors' Contact Information: Bart Wolleswinkel (corresponding author), Delft Center for Systems and Control (DCSC), Delft University of Technology, Delft, The Netherlands; e-mail: b.wolleswinkel@tudelft.nl; Manuel Mazo, Jr., Delft Center for Systems and Control (DCSC), Delft University of Technology, Delft, The Netherlands; e-mail: m.mazo@tudelft.nl; Riccardo Ferrari, Delft Center for Systems and Control (DCSC), Delft University of Technology, Delft, The Netherlands; e-mail: r.ferrari@tudelft.nl.

ACM 2378-9638/2025/8-ART32
https://doi.org/10.1145/3746643

platforms, such as computation, have been named **cyber-physical systems (CPSs)**. These CPSs require a merger of knowledge from domains such as computer science, information technology, and process engineering. Ongoing advances in science and engineering improve the link between computational and physical elements, increasing the adaptability, efficiency, functionality, reliability, and safety of CPSs [1].

One instance where CPSs occur is in a control system architecture where a digital controller interacts with a physical plant. Examples include chemical plants, manufacturing facilities, and power grids, all of which are categorized as I**ndustrial Control Systems (ICS)**. For these ICSs, arguably, the most straightforward choice for measuring the process output is by sampling periodically. However, in recent years, non-uniform sampling (also called aperiodic sampling [32, 41] or nonequidistant sampling [79]) has received increased attention.

Disregarding inter-sample behavior, non-uniformly sampled-data systems can be modeled as **switched linear (SL)** systems when considering the dynamics from one sampling instant to another. As such, this formulation arises naturally in the study of, for instance, multi-rate sampled-data systems [25]. Recent results on the stability of SL systems can be found in [41], while reachability and controllability of SL systems are discussed in [25]; of particular interest for our work is [16], which discusses zeros and zero dynamics of switching systems.

Increasingly often, CPSs make use of a (wireless) communication network between the controller and plant, leading to so-called **networked control systems (NCSs)**. In an NCS, non-uniform sampling of a continuous-time physical process can be used to reduce the number of transmissions over a (possibly shared) band-limited communications network. Another reason for using non-uniform sampling is that switching among different sampling rates may avoid singularities caused by an inappropriate choice of sampling rates [25]. Prominent examples of non-uniform sampling schemes include, but are not limited to, **event-triggered control (ETC)** [6, 39, 40, 68, 72], **self-triggered control (STC)** [2, 37, 55, 80], and multi-rate sampling [53, 58, 87]. Even when a periodic sampler is used, the sampling intervals between two consecutive sampling instants in an NCS are usually time-varying rather than constant, due to, for instance, communication delays [35]. Another reason for the former is that NCSs subject to packet dropouts can be modeled as sampled-data systems with non-uniform sampling [88].

While NCSs are advantageous in many aspects, the use of a communication channel between the plant and controller also makes NCSs vulnerable to cyberattacks. There is a relative abundance of literature regarding secure control of discrete-time and sampled-data systems. However, it is evident that the literature on attacks on non-uniformly sampled-data systems has not yet gained the same traction. The study of the former is important, as critical infrastructure, such as ICSs, is a high-value target at risk of cyberattacks [31]. Over the past decades, more and more ICSs have also become NCSs, using a communication network to exchange information between controller and plant [35]. These NCSs themselves, however, are also at greater risk of falling victim to cyberattacks, due to the use of a communication network, which is often wireless [11]. In these NCSs, bandwidth is usually very limited [55], and as such, proposals for non-uniform sampling policies are gaining in popularity [39]. Combining the former developments, it is important to study the effects and limitations of cyberattacks on non-uniformly sampled-data systems. While denial-of-service attacks have received considerable attention in the ETC literature [18, 20], other types of attacks are still an area ripe for novel development. In particular, deception attacks have received rather little attention, and relatively few resilient ETC mechanisms against deception attacks have been reported [88]. A type of deception attack that has received sporadic attention is replay attacks [9, 23, 81], while other deception attacks, such as covert attacks [24, 42], false data injection attacks [8, 66], and **zero dynamics attacks (ZDAs)**, have not been considered in frameworks with non-uniform sampling.

Of the former, ZDAs have been studied in relative detail in the past decades. ZDAs on discrete-time systems were first discussed in [74], where the authors provide countermeasures in the form of changing either the system dynamics, input matrix, or measurement matrix. The construction of ZDAs using a different methodology was outlined in [75], and a survey of variations of ZDAs can be found in [69]. Recently, the effect of quantization on ZDAs has been studied [47, 51]. As a countermeasure to make ZDAs detectable, the authors of [57] propose the use of dual-rate control scheme. In [49], the authors propose **generalized hold (GH)** (in contrast to **zero-order hold (ZOH)**) as a countermeasure to remove all unstable zeros, whereas the effect of triangle hold on the stability of sampling zeros is discussed in [61].

Conventional ZDAs rely on model knowledge to construct them. However, the authors of [63] show that even adversaries with imperfect model knowledge can be capable of constructing ZDAs. A fully data-driven approach for constructing ZDAs is discussed in [12], and in [59], the threat of ZDAs on systems with nonlinear dynamics is discussed. In [33], a method for the construction of ZDA on nonlinear systems using only input-output data is provided. Finally, in [50, 83], a related attack named a *masking attack* is outlined, which relies on either input redundancy (more inputs than outputs) or an actuator that can refresh more often than the sensor sample.

In this manuscript, we generalize the construction of ZDAs to continuous-time systems with non-uniform sampling, for which sampled-data systems with uniform sampling can be seen as a special case. Unlike periodic sampled-data systems, the notion of zeros for non-uniformly sampled-data systems is ambiguous [16]. As such, conventional methods for constructing ZDAs cannot be straightforwardly extended to non-uniformly sampled-data systems. Here, we leverage tools from geometric control for switched systems [16, 78], including a particular notion of zeros for these systems, to construct *switched* ZDAs, which share similar stealthiness properties with conventional ZDAs. We highlight a key difference from conventional ZDAs on periodic sampled-data systems, which are open-loop attacks and can therefore be constructed offline. On the contrary, *switched* ZDAs require knowledge of the next sampling instant, which might only be known at runtime, and thus require additional disclosure resources from the adversary. We also demonstrate that the former can be used as a basis for countermeasures when the next sampling instant is unavailable to the adversary (and, for that matter, the control system).

The remainder of this article is structured as follows. The considered NCS architecture, incorporating the sampling mechanism, is formulated in Section 2. We present the adversary model and define its objectives, constraints, and assumptions on the disclosure capabilities and disruption resources. In Section 3, we discuss how sampling the continuous-time plant might introduce sampling zeros, and we discuss criteria regarding their stability. The main result is presented in Section 4, where we introduce the notion of a *switched* ZDA, and provide the conditions for stealthiness and disruptiveness. We discuss how this new variant of ZDA relates to conventional ZDAs, and comment on how an adversary might acquire the next sample instant for specific sampling mechanisms. In Section 5, we propose two countermeasures such that certain systems with non-uniform sampling are resilient to switched ZDAs. Then, in Section 6, we provide several illustrative examples on models of real-world CPSs, including a secure control benchmark, namely the quadruple tank system. Finally, in Section 7, conclusions and relevant extensions for future work are discussed.

Notation. Let $\mathbb{R}$ denote the set of real number, $\mathbb{R}_{\geq a}$ ($\mathbb{R}_{>a}$) the set of real numbers greater or equal then (strictly greater than) a, $\mathbb{N}$ the set of natural numbers excluding zero, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ the set of natural numbers including zero, and $\mathbb{N}_{a:b} = [a, b] \cap \mathbb{N}$ the set of all natural numbers between, and including, a and b. For two sets $\mathbb{A}$ and $\mathbb{B}$, let $\mathbb{A} \subseteq \mathbb{B}$ denote that $\mathbb{A}$ is a subset of $\mathbb{B}$, and let $\mathbb{A} \subset \mathbb{B}$ denote that $\mathbb{A}$ is a *proper* subset of $\mathbb{B}$ (i.e., there exists a $b \in \mathbb{B}$ such that $b \notin \mathbb{A}$). Given a set $\mathbb{A} \subseteq \mathbb{R}^n$, let $\#\mathbb{A}$ denote its cardinality (i.e., the number of elements), and let $|\mathbb{A}|$ denote the Lebesgue measure (i.e., its n-dimensional volume). For a subspace $V \subseteq \mathbb{R}^n$ and a matrix $\mathbf{A}$,

let $\mathbf{A}V = \{\mathbf{A}\mathbf{v} \mid \mathbf{v} \in V\}$ denote the resulting subspace when applying the transformation $\mathbf{A}$ to all elements of V. Given two subspaces V and $W \subseteq \mathbb{R}^n$ (a subspace $V \subseteq \mathbb{R}^n$ and vector $\mathbf{x} \in \mathbb{R}^n$), let $V + W$ ($V + \mathbf{x}$) denote the sum resulting in the subspace $U = V + W = \{\mathbf{v} + \mathbf{w} \mid \mathbf{v} \in V, \mathbf{w} \in W\}$ (the affine subset $\mathbb{U} = V + \mathbf{x} = \{\mathbf{v} + \mathbf{x} \mid \mathbf{v} \in V\}$). Given a vector space X and a subspace $V \subseteq X$, let $X/V = \{\mathbf{x} + V \mid \mathbf{x} \in X\}$ denote the quotient space. In general, we use an underaccent tilde $\underset{\sim}{\mathcal{P}}$ and Greek $\boldsymbol{\chi}$ to denote continuous-time systems and their respective states, and $\mathcal{P}$ and Roman $\mathbf{x}$ to denote their discrete-time (i.e., discretized) counterparts.

2 Problem Definition

Consider the following continuous-time **linear time-invariant (LTI)** plant:

$$\underset{\sim}{\mathcal{P}} : \quad \begin{aligned} \dot{\boldsymbol{\chi}}(t) &= \underset{\sim}{\mathbf{A}}\boldsymbol{\chi}(t) + \underset{\sim}{\mathbf{B}}\boldsymbol{\upsilon}(t), && \text{(1a)} \\ \boldsymbol{\gamma}(t) &= \mathbf{C}\boldsymbol{\chi}(t), && \text{(1b)} \end{aligned}$$

with state vector $\boldsymbol{\chi}(t) \in \mathbb{R}^{n_\mathrm{x}}$, actuation vector $\boldsymbol{\upsilon}(t) \in \mathbb{R}^{n_\mathrm{u}}$, measurement vector $\boldsymbol{\gamma}(t) \in \mathbb{R}^{n_\mathrm{y}}$, and matrices $\underset{\sim}{\mathbf{A}}$, $\underset{\sim}{\mathbf{B}}$, and $\mathbf{C}$ all of appropriate dimensions. Without loss of generality, we assume $t \in \mathbb{R}_{\geq 0}$. We make the following standard assumptions:

Assumption 1. *The pair $(\underset{\sim}{\mathbf{A}}, \underset{\sim}{\mathbf{B}})$ is controllable and the pair $(\underset{\sim}{\mathbf{A}}, \mathbf{C})$ is observable, i.e., the realization $\underset{\sim}{\mathcal{P}}$ is minimal.* ◊

The physical process $\underset{\sim}{\mathcal{P}}$ is controlled by a (possibly dynamic) digital discrete-time LTI controller C, given by:

$$C : \quad \begin{aligned} \mathbf{c}_{k+1} &= \mathbf{A}_\mathrm{c}\mathbf{c}_k + \mathbf{B}_\mathrm{c}\mathbf{y}_i, && \text{(2a)} \\ \mathbf{u}_{\mathrm{c},i} &= \mathbf{C}_\mathrm{c}\mathbf{c}_k + \mathbf{D}_\mathrm{c}\mathbf{y}_i, && \text{(2b)} \end{aligned}$$

where $\mathbf{u}_{\mathrm{c},i} \in \mathbb{R}^{n_\mathrm{u}}$ is the actuation input, $\mathbf{y}_i = \boldsymbol{\gamma}(t_i)$ is the ith sampled output, and all matrices $\mathbf{A}_\mathrm{c}, \mathbf{B}_\mathrm{c}, \mathbf{C}_\mathrm{c}$, and $\mathbf{D}_\mathrm{c}$ (some of which can be zero) are of appropriate dimensions. Furthermore, we assume a ZOH mechanism at the plant side resulting in $\boldsymbol{\upsilon}(t) = \mathbf{u}_{\mathrm{c},i} + \mathbf{a}_i$ for all $t \in [t_i, t_{i+1})$, meaning the input remains constant between sampling instants. The input $\mathbf{a}_i$ is a malicious attack vector, as will be discussed in Section 2.1. Depending on the specific controller C, the controller state dynamics as in (2a) are updated periodically, meaning $i \leq k, k+1, \ldots, k+\kappa_i - 1 < i+1$ [17, 27], or whenever a new measurement becomes available, meaning $k = i$ [2, 39].

Let t_i denote the time at which the ith sample is transmitted, with $i \in \mathbb{N}_0$, which might be only known at execution time. At those time instants, the sensors send a measurement $\mathbf{y}_i = \boldsymbol{\gamma}(t_i)$ to the controller, which then computes an updated input $\mathbf{u}_{\mathrm{c},i}$ and transmits this to the actuators. Without loss of generality, we assume $t_0 = 0$.

The plant $\underset{\sim}{\mathcal{P}}$ and digital controller C are physically non-collocated, and transmission over the communication channel is based on a (non-uniform) sampling policy $\mathcal{S}$. Examples of sampling policies that adhere to this architecture can be seen in Figure 1. The first examples highlight ETC, which can be further subdivided into **periodic event-triggered control (PETC)** and continuous event-triggered control. In ETC, a triggering condition $\phi : \mathbb{R}^{n_\mathrm{y}} \times \mathbb{R}^{n_\mathrm{y}} \to \{\texttt{transmit}, \texttt{idle}\}$ is monitored at the sensors, and a new measurement $\mathbf{y}_i$ is transmitted to the controller over a sensors-to-controller channel when a triggering condition is satisfied. In STC, the next sampling instant t_{i+1} is instead decided at the controller side by a prediction function $\Gamma : \mathbb{R}^{n_\mathrm{x}} \times \mathbb{R}^{n_\mathrm{u}} \to \mathbb{R}_{>0}$, and at each sampling instant t_i, the next sampling instant t_{i+1} is calculated and transmitted to both the sensors and actuators over a **controller-to-sensors (C2S)** and **controller-to-actuators (C2A)** channel, respectively. Lastly, there also exist non-uniform but periodic sampling schemes, where a periodic schedule $\vec{\tau}_1, \vec{\tau}_2, \ldots, \vec{\tau}_m$ of length m, with different inter-sample times, follow each other

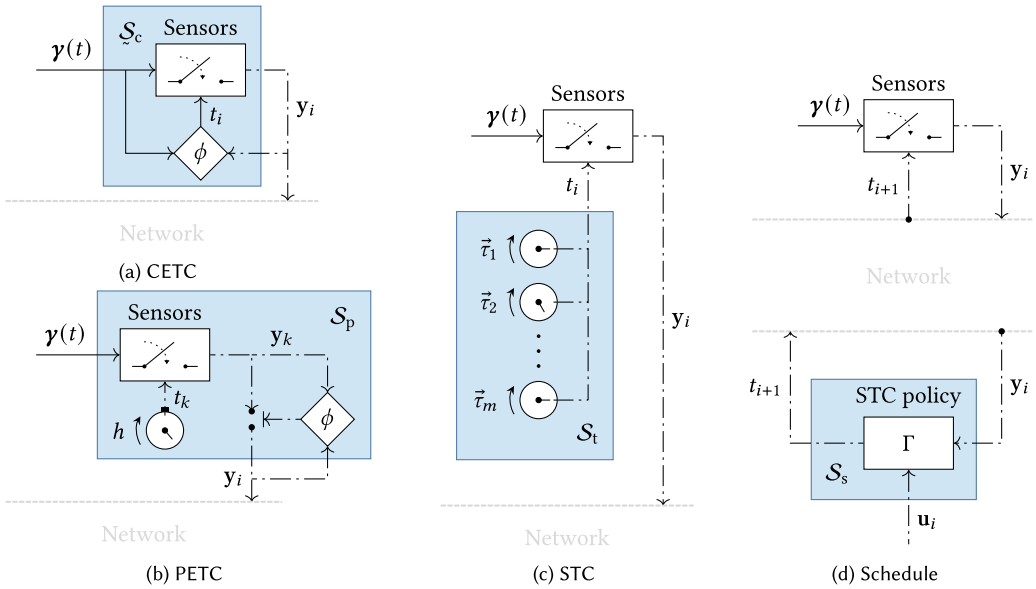


Fig. 1. Architecture of various aperiodic sampling schemes.

sequentially and periodically repeat. The overhead arrow notation "$\vec{\cdot}$" indicates that there exists an i such that periodicity holds, which in the case of a periodic schedule is trivially $i = 0$.

The dynamics between sampling instants, resulting from the plant $\underset{\sim}{\mathcal{P}}$ with the non-uniform feedback due to the sampling policy $\mathcal{S}$, can be modeled as an SL system as follows:

$$\mathcal{P}_{\text{sl}}: \quad \mathbf{x}_{i+1} = \mathbf{A}_{\tau_{i+1}}\mathbf{x}_i + \mathbf{B}_{\tau_{i+1}}\mathbf{u}_i, \tag{3a}$$

$$\mathbf{y}_i = \mathbf{C}\mathbf{x}_i, \tag{3b}$$

where the next inter-sample time $\tau_{i+1} = t_{i+1} - t_i$, and the matrices $\mathbf{A}_\tau$, $\mathbf{B}_\tau$ (under a ZOH mechanism) are given by

$$\mathbf{A}_\tau = e^{\underset{\sim}{\mathbf{A}}\cdot\tau}, \qquad \mathbf{B}_\tau = \int_0^\tau e^{\underset{\sim}{\mathbf{A}}\cdot s}\, \mathrm{d}s \underset{\sim}{\mathbf{B}}, \tag{4}$$

with $\mathbf{x}_i = \boldsymbol{\chi}(t_i)$, $\mathbf{u}_i = \boldsymbol{\upsilon}(t_i)$, and $\mathbf{y}_i = \boldsymbol{\gamma}(t_i)$. Given a sampling policy $\mathcal{S}$, this gives rises to a set of possible sample times $\mathbb{H} \subset \mathbb{R}_{>0}$, such that $\tau_i \in \mathbb{H}$ for all $i \in \mathbb{N}_0$. Note that, given some initial condition $\mathbf{x}_0 = \boldsymbol{\chi}(0)$ and controller design C, the choice of sampling policy $\mathcal{S}$ also generates the set of sample instants $\mathbb{T}(\mathbf{x}_0)$, with $t_i \in \mathbb{T}(\mathbf{x}_0)$. As $t_{i+1} > t_i$, this set permits a naturally ordered sequence $(t_i \mid \mathbf{x}_0)_{i\in\mathbb{N}}$. Note that it can be the case that $\mathbb{T}(\mathbf{x}_0)$ is only known at runtime and not in advance: such is, for example, the case when the sampling policy $\mathcal{S}$ itself incorporates feedback (as is the case for, e.g., ETC and STC). Based on how $\mathbb{T}(\mathbf{x}_0)$ is implicitly constructed, we make the following assumption:

Assumption 2. *Considering the dynamics $\underset{\sim}{\mathcal{P}}$ as in (1), the sampling policy $\mathcal{S}$ and controller C are designed such that for all $\mathbf{x}_0 \in \mathbb{R}^{n_x}$, the sampling times $\mathbb{T}(\mathbf{x}_0)$ guarantee asymptotic stability of the origin. That is,* $\lim_{t\to\infty} \|\boldsymbol{\chi}(t)\| = 0$. ◊

Remark 1. In case the controller C is a full-state feedback controller of the form $\mathbf{u}_{\text{c},i} = \mathbf{K}\hat{\mathbf{x}}_i$, with $\underset{\sim}{\mathbf{A}} + \underset{\sim}{\mathbf{B}}\mathbf{K}$ Hurwitz, one can design an ETC policy $\mathcal{S}$ using an *emulation approach* as described in [37]

such that Assumption 2 is satisfied. Similar sequential design procedures for PETC and STC are outlined in [38, 71] and [5, 55], respectively, to name a few examples. A co-design method for ETC is outlined in [64].

Remark 2. We might have that $\mathbb{H}_{\mathcal{P}} = \bigcup_{\mathbf{x}_0 \in \mathbb{R}^{n_\mathrm{x}}} \mathbb{T}(\mathbf{x}_0) \subset \mathbb{H}$, i.e., not all possible inter-sample times are actually exhibited in the implementation. Note that $\mathbb{H}$ is an (indirect) design choice, while $\mathbb{H}_{\mathcal{P}}$ is a consequence of, among other things, the specific dynamics $\mathcal{P}$ and choice of controller C. For instance, in STC, $\mathbb{H}$ can be considered as the codomain of Γ, which might not equal the image of Γ.

To make sure Assumption 1 also holds for the discretized sample dynamics $\mathcal{P}_{\mathrm{sl}}$ for all $\tau \in \mathbb{H}$, we require that the sampling times τ are *non-pathological*, which we define as follows:

Definition 2.1 (Pathological Sampling [13, Definition 3.2.1]). Suppose $\tau \in \mathbb{R}_{>0}$ is such that there exists $\lambda, \lambda' \in \sigma(\underset{\sim}{\mathbf{A}})$ and a $k \in \mathbb{Z}$, with $\mathfrak{R}\{\lambda\} = \mathfrak{R}\{\lambda'\}$, such that $\mathfrak{I}\{\lambda\} = \mathfrak{I}\{\lambda'\} \cdot (2\pi \cdot k/\tau)$ (i.e., the eigenvalues λ and λ' are *rationally related*). Then, the sample time τ is *pathological*.

Whenever a sampling time τ is non-pathological, this guarantees that $(\underset{\sim}{\mathbf{A}}, \underset{\sim}{\mathbf{B}})$ being controllable implies the discretized pair $(\mathbf{A}_\tau, \mathbf{B}_\tau)$ is controllable as well [54]. Therefore, we make the following assumption:

Assumption 3. *Let $\mathbb{H}_{\mathrm{p}} \subset \mathbb{R}_{>0}$ denote the set of all*[1] *sampling times τ that are pathological. Then, $\mathbb{H} \cap \mathbb{H}_{\mathrm{p}} = \varnothing$.* ◊

Note that periodic sampling, implying $\mathbb{H} = \{h\}$ with $h \in \mathbb{R}_{>0}$, is a special case of the more general framework we consider here.

2.1 Adversary Model

Next, we introduce an adversary $\mathcal{A}$ and define its goals and objectives, as well as its capabilities. The attack framework follows that of [75], while the adversary model will be that as described in [67]. We consider a *strong adversary*, which is an adversary that has full knowledge of the system dynamics [75]. The adversary is also assumed to have disruption resources of the C2A channel, and as such

$$\boldsymbol{\upsilon}(t) = \mathbf{u}_{\mathrm{c},i} + \mathbf{a}_i, \quad \text{for all } t \in [t_i, t_{i+1}), \tag{5}$$

with $\mathbf{u}_{\mathrm{c},i} \in \mathbb{R}^{n_\mathrm{u}}$ being the controller actuation, and $\mathbf{a}_i \in \mathbb{R}^{n_\mathrm{u}}$ the malicious attack vector. We define the information available to the adversary, which is the combination of system knowledge and disclosure resources at the sampling instant t_i, as the set $\mathbb{I}_{\mathrm{a}}(t_i)$. We assume the adversary satisfies the following:

Assumption 4. *The information available to the adversary $\mathcal{A}$ satisfies $\mathbb{I}_{\mathrm{a}}(t_i) \supseteq \{t_{i+1} \wedge \underset{\sim}{\mathcal{P}}, C, \mathcal{S}\}$ for all $t_i \geq t_{i_\mathrm{a}}$, where t_{i_a} denotes the first attacked time instant.* ◊

Remark 3. The assumption of model knowledge of the adversary is a strong requirement on the capabilities of the adversary, but standard in the literature on ZDAs [49, 63, 74]. It is motivated by the existence of resourceful and sophisticated adversaries, such as those backed by nation-states (who could acquire the above information through industrial espionage [15]), or those from insider attacks [70].

Assumption 4 is the main assumption of this work. It is slightly stronger than the assumption needed for an adversary to craft a conventional ZDA, as it assumes $t_{i+1} \in \mathbb{I}_{\mathrm{a}}(t_i)$.

[1] Note that the set $\mathbb{H}_{\mathrm{p}}$ is countable [4], which implies $|\mathbb{H}_{\mathrm{p}}| = 0$.

Remark 4. A conventional (periodic) ZDA is an *open-loop* attack, meaning the attack vectors $\mathbf{a}_i$ can be computed offline for all i. A switched ZDA, however, relies on disclosure of t_{i+1}, and therefore, in general, needs to be constructed online. Furthermore, note that the adversary adheres to the inter-sample time as determined by the sampling policy $\mathcal{S}$, meaning $\dot{\boldsymbol{\upsilon}}(t) = \mathbf{0}$ for all $t \in (t_i, t_{i+1})$.[2] The justification of the former is that sending additional packets whenever $t \neq t_i$ might lead to detection via other means focused on traffic conformity, due to the increased traffic over the network [84]. Furthermore, for sampling policies such as an STC policy $\mathcal{S}_\mathrm{s}$ or a periodic schedule $\mathcal{S}_\mathrm{t}$, where the next sampling instant t_{i+1} is known in advance, the actuators do not accept new commands whenever $t \in (t_i, t_{i+1})$.

Next, we state two properties an attack $(\mathbf{a}_i)_{i\in\mathbb{N}_0}$ can exhibit.

Definition 2.2 (ϵ-Stealthy Attack, Adapted from [52]). Given an $\epsilon \in \mathbb{R}_{>0}$, an attack $(\mathbf{a}_i)_{i\in\mathbb{N}_0}$ is *ϵ-stealthy* if $\|\mathring{\mathbf{y}}_i - \mathbf{y}_i\| < \epsilon$ for all i. Here, $\mathring{\mathbf{y}}_i$ is the nominal output trajectory given an identical initial condition $\mathbf{x}_0$ but with $\mathbf{a}_i = \mathbf{0}$ for all i.

Definition 2.3 (Disruptive Attack). An attack $(\mathbf{a}_i)_{i\in\mathbb{N}_0}$ is *disruptive* if $\lim_{t\to\infty} \|\boldsymbol{\chi}(t)\| = \infty$.

Note that $\lim_{t\to\infty} \|\boldsymbol{\chi}(t)\| = \infty$ implies $\lim_{i\to\infty} \|\mathbf{x}_i\| = \infty$, meaning it suffices to look solely at the dynamics $\mathcal{P}_\mathrm{sl}$ between sample instants. To conclude, we can state the objective and constraints of the adversary as follows:

Problem 1. *Given an $\epsilon \in \mathbb{R}_{>0}$, create an attack $(\mathbf{a}_i)_{i\in\mathbb{N}_0}$ for the sampled-data system $\mathcal{P}_\mathrm{sl}$ as in (3) that is both ϵ-stealthy and disruptive.*

Recall that a *conventional* ZDA is a sequence $\mathbf{a}_k = \mathbf{u}_0 z^k$, where we use k to denote that the attack is constructed for a periodic system. Here, $z \in \mathbb{C}$ is an (unstable) zero of the triple $\mathbf{A}_h$, $\mathbf{B}_h$, $\mathbf{C}$, and $\mathbf{u}_0 \neq \mathbf{0}$ is the input-zero direction [77], which is the solution to the output-zeroing problem given by the Rosenbrock system matrix

$$\begin{bmatrix} z\cdot\mathbf{I} - \mathbf{A}_h & -\mathbf{B}_h \\ \mathbf{C} & \mathbf{0} \end{bmatrix} \begin{bmatrix} \mathbf{x}_0 \\ \mathbf{u}_0 \end{bmatrix} = \mathbf{0}. \tag{6}$$

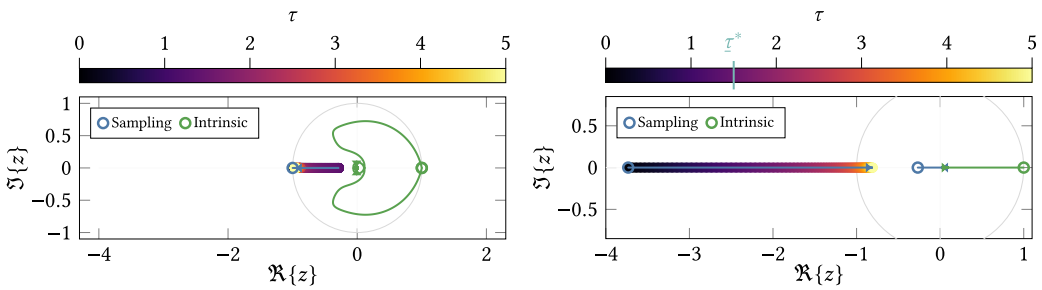
The former definition cannot be straightforwardly extended to non-uniform sampling policies, as the definition of the zero $z \in \mathbb{C}$ for the switched system $\mathcal{P}_\mathrm{sl}$ is ambiguous [16]. This brings us to an alternative design method for *switched* ZDAs as outlined in Section 4. In the next section, we discuss a vulnerability of sampled-data systems the adversary could potentially exploit.

3 Sampling Zeros

In order to construct an attack $(\mathbf{a}_i)_{i\in\mathbb{N}_0}$ that satisfies Problem 1, we shift our attention to *output-nulling* inputs [74]. These input sequences are related to the zeros of the system, i.e., the inputs $\mathbf{u}_i \neq \mathbf{0}$ for all t, for which $\mathbf{y}_i = \mathbf{0}$ for all t, for some initial condition $\mathbf{x}_0$. While the continuous-time plant $\underset{\sim}{\mathcal{P}}$ might not contain any unstable zeros, the individual modes of the discretized dynamics $\mathcal{P}_\mathrm{sl}$ might contain (unstable) *sampling zeros*.

For a **single-input and single-output (SISO)** system (i.e., $n_\mathrm{u} = n_\mathrm{y} = 1$), the *relative degree* n_ν of the continuous-time plant $\underset{\sim}{\mathcal{P}}$ is defined as $n_\nu = n_\mathrm{p} - \underset{\sim}{n}_\mathrm{z}$, where n_p denotes the number of poles (i.e., the number of states n_x) and $\underset{\sim}{n}_\mathrm{z}$ the number of zeros of the continuous-time system. Regardless of the relative degree n_ν of the continuous-time plant $\underset{\sim}{\mathcal{P}}$, the individual modes of the discretized

[2] Note that whenever an adversary does not adhere to keeping the attack vector constant between sampling instants, then a ZDA might be possible regardless of the countermeasures as proposed in Section 5. In fact, similar reasoning still holds for periodic control, as updating the actuators at a sufficiently small sampling time $\tau_\mathrm{a} < \inf \mathbb{H}$ could still yield unstable sampling zeros (see Section 3).



(a) $n_x = 4, n_\nu = 2$ [32] (b) $n_x = 4, n_\nu = 3$ [51]

Fig. 2. Root loci of two SISO systems. Unstable sampling zeros appear for $n_\nu > 2$ (which are stable for sufficiently large τ).

dynamics $\mathcal{P}_{\text{sl}}$ as in (3) contain $n_x - 1$ zeros for almost all[3] inter-sample times τ [69]. While for the $\underset{\sim}{n}_z$ zeros $s \in \mathbb{C}$ of $\underset{\sim}{\mathcal{P}}$, called *intrinsic zeros*, it holds[4] that $z \approx e^{s \cdot \tau}$ (similar to the poles) for sufficiently small τ, for the $n_x - \underset{\sim}{n}_z - 1$ *sampling zeros* that do not have a continuous-time counterpart, there is no simple relationship. Furthermore, if the sampling period τ is small enough, at least one of these sampling zeros is unstable, captured in the following theorem:

Theorem 3.1 (Unstable sampling zeros [13, Lemma 3.3.3]). *Suppose $\underset{\sim}{\mathcal{P}}$ is SISO with relative degree $n_\nu > 2$. Then, as $\tau \to 0$, the discretized dynamics corresponding to $\mathbf{A}_\tau$, $\mathbf{B}_\tau$, $\mathbf{C}$ will contain at least one unstable sampling zero.*

Note that in many engineering applications and ICSs, sufficiently fast sample rates and a relative degree n_ν strictly greater than two are common [86]. This may happen for quite reasonable sampling periods, and therefore, sampled-data systems with unstable inverses are ubiquitous [89]. Furthermore, as $\tau \to 0$, it is known that these sampling zeros approach the roots of the Euler–Frobenius polynomial [49, 85], meaning that the output-zeroing input corresponding to the sampling zero should have alternating signs [69]. If the open-loop system $\underset{\sim}{\mathcal{P}}$ is stable, then as $\tau \to \infty$, the discretization contains only stable zeros, captured in the following lemma:

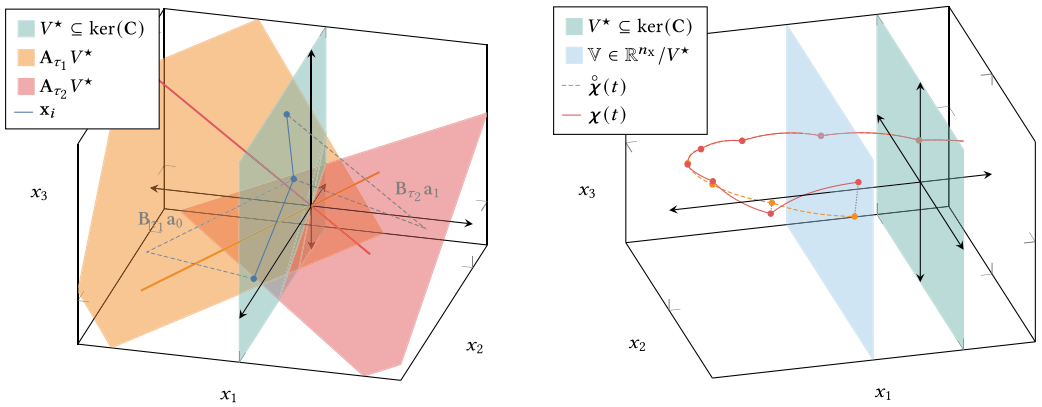
Lemma 3.2 ([89, Theorem 2]). *Suppose $\underset{\sim}{\mathcal{P}}$ is SISO, stable, has relative degree $n_\nu \geq 1$, and has no zeros at the origin. Then, as $\tau \to \infty$, the individual modes of the discretized dynamics $\mathcal{P}_{\text{sl}}$ contain only stable zeros.*

Two illustrative examples can be seen in Figure 2. For these systems, there exists a critical sampling period τ^* for which sampling with $\tau > \tau^*$ leads to stable zeros. Furthermore, a lower bound $\underline{\tau}^*$ on the sampling period $\tau \in \mathbb{R}_{>0}$ such that Lemma 3.2 does not hold (here stated only for simple poles and zeros) is known:

Lemma 3.3 ([56, Theorem 1]). *A lower bound $\underline{\tau}^* \in \mathbb{R}_{>0}$ such that Lemma 3.2 is guaranteed not to hold (i.e., for any $\tau < \underline{\tau}^*$, there is at least one unstable sampling zero) is given by*

$$\underline{\tau}^* = \frac{\log\left(2 \cdot \alpha \cdot (n_x + 1)\right)}{|\min \Re\{\sigma(\underset{\sim}{\mathbf{A}})\}|}, \tag{7}$$

[3]For particular values of the sampling period, some zeros may go to infinity, or they may be cancelled by poles, i.e., hidden modes [89].
[4]In particular, it holds that $z \leftrightarrow e^{\tau \cdot z}$ as $\tau \to 0$ [36].



(a) A robust controlled invariant subspace $V^\star \subseteq \ker(\mathbf{C})$ (b) Nominal and attacked trajectories $\mathring{\boldsymbol{\chi}}(t)$ and $\boldsymbol{\chi}(t)$

Fig. 3. Illustration of concepts from geometric control relevant to switched ZDAs.

where $\alpha = \max_j |a_j / \underset{\sim}{P}(0)|$ *and* $\underset{\sim}{P}(s) = \mathbf{C}(s \cdot \mathbf{I} - \underset{\sim}{\mathbf{A}})^{-1}\underset{\sim}{\mathbf{B}}$ *is the transfer function of* $\underset{\sim}{\mathcal{P}}$*, which can be written (by means of partial fraction decomposition) as*

$$\frac{1}{s} \cdot \underset{\sim}{P}(s) = \frac{\underset{\sim}{P}(0)}{s} + \sum_{j=1}^{n_\mathbf{x}} \frac{a_j}{s - b_j}, \qquad a_j, b_j \in \mathbb{R}. \tag{8}$$

4 Switched Zero Dynamic Attacks

In this section, we discuss the construction of a new variant of ZDA, called a switched ZDA. First, we recall some relevant notions from geometric control.

Definition 4.1 (Invariant Subspace [10]*).* A subspace $V \subseteq \mathbb{R}^{n_\mathbf{x}}$ is an $\mathbf{A}$*-invariant subspace* if $\mathbf{A}V \subseteq V$.

Definition 4.2 (Controlled Invariant Subspace [10]*).* A subspace $V \subseteq \mathbb{R}^{n_\mathbf{x}}$ is an $(\mathbf{A}, \mathbf{B})$*-controlled invariant subspace* if $\mathbf{A}V \subseteq V + \mathrm{Im}(\mathbf{B})$, or equivalently, if there exists a matrix $\mathbf{F}$, called a *friend* of V, such that V is an $(\mathbf{A} + \mathbf{BF})$-invariant subspace.

Of particular interest are the controlled invariant subspaces that are contained in the kernel of $\mathbf{C}$. Intuitively, an $(\mathbf{A}, \mathbf{B})$-controlled invariant subspace V is a subspace for which, after applying the transformation $\mathbf{A}$ to V, there exists some input $\mathbf{u}$ that "pushes" the mapped states back onto V (see Figure 3(a)). Since we are dealing with linear systems, this necessarily implies the existence of a feedback gain $\mathbf{F}$ achieving the former, which, in general, is not unique. We denote by $\mathbb{F}(V) = \{\mathbf{F} \in \mathbb{R}^{n_\mathbf{u} \times n_\mathbf{x}} \mid (\mathbf{A} + \mathbf{BF})V \subseteq V\}$ the set of friends of V.

Furthermore, since the dynamics $\mathcal{P}_{\mathrm{sl}}$ are an SL system, we need an equivalent notion of zeros of SL systems. For our purposes, we focus on the zeros of the individual modes of the system, related to the following definition:

Definition 4.3 (Robust Controlled Invariant Subspace [16]*).* A subspace V is a *robust controlled invariant subspace* for the dynamics $\mathcal{P}_{\mathrm{sl}}$ if, for all $\tau \in \mathbb{H}$, V is an $(\mathbf{A}_\tau, \mathbf{B}_\tau)$-controlled invariant subspace.

Note that in (3), the matrix $\mathbf{C}$ is constant for all sampling periods τ. Therefore, if V is a robust-controlled invariant subspace, then the maximal controlled invariant subspace $V^\star \subseteq \ker(\mathbf{C})$ is constant for all sampling instants. A sufficient condition for when this is the case is provided next:

Lemma 4.4. *Suppose $\mathbb{H} \subset h \cdot \mathbb{N}$ and $\mathcal{P}$ is SISO. Then, almost always,*[5] *if V is an $(\mathbf{A}_h, \mathbf{B}_h)$-controlled invariant subspace, V is a robust controlled invariant subspace for all $\tau \in \mathbb{H}$.*

Proof. Note that the individual modes of the sampling dynamics $\mathcal{P}_{\text{sl}}$ *almost always* have $n_{\text{x}} - 1$ invariant zeros [69]. This implies $\dim(V) = n_{\text{x}} - 1$. As $\mathbb{H} \subseteq h \cdot \mathbb{N}$, this means $\tau = n \cdot h$ for some $n \in \mathbb{N}$. We can write $\mathbf{A}_\tau = \mathbf{A}_{n \cdot h}$, and $\mathbf{B}_\tau = \mathbf{B}_{n \cdot h}$, which are explicitly given by

$$\mathbf{A}_{n \cdot h} = \mathbf{A}_h^n, \qquad \mathbf{B}_{n \cdot h} = \sum_{k=0}^{n-1} \mathbf{A}_h^k \mathbf{B}_h = \mathbf{A}_h^{n-1}\mathbf{B}_h + \mathbf{A}_h^{n-2}\mathbf{B}_h + \ldots + \mathbf{A}_h\mathbf{B}_h + \mathbf{B}_h. \tag{9}$$

As a shorthand, we introduce $\mathbf{\Phi}_n = \mathbf{A}_h^{n-1} + \mathbf{A}_h^{n-2} + \ldots + \mathbf{A}_h + \mathbf{I}$ and proof Lemma 4.4 by induction. Suppose for some $n \in \mathbb{N}$, the subspace V is an $(\mathbf{A}_{n \cdot h}, \mathbf{B}_{n \cdot h})$-controlled invariant subspace, which implies

$$\mathbf{A}_{n \cdot h} = \mathbf{A}_h^n \subseteq V + \text{Im}(\mathbf{B}_{n \cdot h}) = V + \text{Im}(\mathbf{\Phi}_n \mathbf{B}_h). \tag{10}$$

Multiplying (10) with $\mathbf{A}_h$ from the left results in

$$\mathbf{A}_h \mathbf{A}_h^n = \mathbf{A}_h^{n+1} \subseteq \mathbf{A}_h V + \mathbf{A}_h \text{Im}(\mathbf{\Phi}_n \mathbf{B}_h) = \mathbf{A}_h V + \text{Im}(\mathbf{A}_h \mathbf{\Phi}_n \mathbf{B}_h). \tag{11}$$

By assumption, it holds that V is an $(\mathbf{A}_h, \mathbf{B}_h)$-controlled invariant subspace (the base case, $n = 1$), which means that

$$\mathbf{A}_h V \subseteq V + \text{Im}(\mathbf{B}_h). \tag{12}$$

As the sum of subspaces is non-decreasing (i.e., $W + Z \subseteq V \implies W \subseteq V, Z \subseteq V$), we can substitute (12) into (11), resulting in

$$\mathbf{A}_h^{n+1} \subseteq V + \text{Im}(\mathbf{A}_h \mathbf{\Phi}_n \mathbf{B}_h) + \text{Im}(\mathbf{B}_h). \tag{13}$$

We end up with the inequality

$$\mathbf{A}_h^{n+1} \subseteq V + \text{Im}(\mathbf{A}_h \mathbf{\Phi}_n \mathbf{B}_h) + \text{Im}(\mathbf{B}_h) \stackrel{?}{=} V + \text{Im}(\mathbf{A}_h \mathbf{\Phi}_n \mathbf{B}_h + \mathbf{B}_h) = V + \text{Im}(\mathbf{\Phi}_{n+1} \mathbf{B}_h), \tag{14}$$

where the middle equality is the one needed to show that V is an $(\mathbf{A}_{(n+1) \cdot h}, \mathbf{B}_{(n+1) \cdot h})$-controlled invariant subspace. As $\dim(V) = n_{\text{x}} - 1$, and $\text{rank}(\mathbf{B}_h) = 1$ (the system is controllable due to Assumptions 1 and 3), a sufficient condition for the equality in (14) to hold is that

$$(\mathbf{A}_h \mathbf{\Phi}_n + \mathbf{I}) \text{Im}(\mathbf{B}_h) \not\subset V, \tag{15}$$

as then the right-hand side of (14) will equal $\mathbb{R}^{n_{\text{x}}}$. Note that (15) holds *almost always*, and as such

$$\mathbf{A}_{(n+1) \cdot h} \subseteq V + \text{Im}(\mathbf{A}_h \mathbf{\Phi}_n \mathbf{B}_h + \mathbf{B}_h) = V + \text{Im}(\mathbf{B}_{(n+1) \cdot h}), \tag{16}$$

proving V is an $(\mathbf{A}_{(n+1) \cdot h}, \mathbf{B}_{(n+1) \cdot h})$-controlled invariant subspace. As the base case $n = 1$ holds by assumption, this completes the proof. ∎

Conclusively, the maximal robust controlled invariant subspace $V^\star \subseteq \ker(\mathbf{C})$ is identical for all pairs of matrices $(\mathbf{A}_\tau, \mathbf{B}_\tau)$ with $\tau \in \mathbb{H}$. The eigenvalues of the matrix $\mathbf{A}_\tau + \mathbf{B}_\tau \mathbf{F}_\tau$ are directly related to the zeros of the individual modes of the system $\mathcal{P}_{\text{sl}}$, as indicated in the next lemma:

Lemma 4.5 ([43, Theorem 4.7]). *For a triple $(\mathbf{A}_\tau, \mathbf{B}_\tau, \mathbf{C})$ and $V^\star \subseteq \ker(\mathbf{C})$, we have that $\sigma(\mathbf{A}_\tau + \mathbf{B}_\tau \mathbf{F}_\tau \mid V^\star)$, i.e., the eigenvalues of the matrix whose eigenspace is contained in $V^\star$, are precisely the zeros of the triple $(\mathbf{A}_\tau, \mathbf{B}_\tau, \mathbf{C})$ for all $\mathbf{F}_\tau \in \mathbb{F}(V^\star)$.*

[5] Almost always indicates that the property holds generically and that the set of matrices $\mathbf{A}_h, \mathbf{B}_h$, and $\mathbf{C}$ for which the condition does not hold has measure zero.

Next, we are ready to provide the main results of the article. We define a *switched* ZDA as follows:

Definition 4.6 (Switched ZDA). A *switched ZDA* $(\mathbf{a}_i)_{i\in\mathbb{N}_0}$ can be constructed by iterating the dynamical system:

$$\mathcal{A}: \quad \mathbf{f}_{i+1} = (\mathbf{A}_{\tau_{i+1}} + \mathbf{B}_{\tau_{i+1}}\mathbf{F}_{\tau_{i+1}})\mathbf{f}_i, \tag{17a}$$

$$\mathbf{a}_i = \mathbf{F}_{\tau_{i+1}}\mathbf{f}_i, \tag{17b}$$

for some non-zero initial condition $\mathbf{f}_0 \in V^\star \setminus \{\mathbf{0}\}$, where $\mathbf{F}_\tau \in \mathbb{F}(V^\star)$, and $V^\star \subseteq \ker(\mathbf{C})$ is a robust controlled invariant subspace for the dynamics $\mathcal{P}_{\text{sl}}$.

From (17), it is evident that the next sampling instance τ_{i+1} needs to be know to the adversary, i.e., $\tau_{i+1} \in \mathbb{I}_{\text{a}}(t_i)$. Note that here we assume that the adversary can either predict τ_{i+1} ahead of time (which is the case for, e.g., $\mathcal{S}_{\text{p}}$ and $\mathcal{S}_{\text{t}}$), such that it has ample to compute $\mathbf{a}_i$, or that the adversary can immediately compute the attack vector $\mathbf{a}_i$ as soon as the next sampling instant t_{i+1} becomes available (which is the case for, e.g., $\mathcal{S}_{\text{s}}$). For the latter, this leads to another idealized assumption:

Assumption 5 (Zero processing time [37, 64]). *Both the computation of* (17) *as well as the transmission according to* (5) *can be done instantaneously.* ◊

Remark 5. While Assumption 5 is inconceivable in practice, it might be reasonable to assume that the computation of (17) can be done sufficiently fast after receiving t_{i+1} (as it only requires a single matrix multiplication), and therefore the delay in transmission (5) is negligible (and therefore undetectable).

Proposition 4.7. *Suppose* $\mathbf{x}_0 = \mathring{\mathbf{x}}_0$. *Then, given an* $\epsilon \in \mathbb{R}_{>0}$, *the switched ZDA as in Definition 4.6 is* ϵ*-stealthy.*

Proof. The proof follows by induction similar to [74]. Let $\mathcal{K}$ be the mapping of the output $\mathbf{y}$ to the control input $\mathbf{u}_{\text{c}}$ by the controller C. Suppose for some $i \geq 1$, the state is given by

$$\mathbf{x}_i = \mathring{\mathbf{x}}_i + \mathbf{f}_i + \Delta\mathbf{x}_i, \tag{18}$$

with $\mathbf{f}_i$ as constructed from (17), and with $\mathring{\mathbf{x}}_i$ the nominal trajectory whenever $\mathbf{a}_i = \mathbf{0}$ for all i. Then, $\mathbf{x}_{i+1}$ is given by

$$\mathbf{x}_{i+1} = \mathbf{A}_{\tau_{i+1}}(\mathring{\mathbf{x}}_i + \mathbf{f}_i + \Delta\mathbf{x}_i) + \mathbf{B}_{\tau_{i+1}}(\mathcal{K}(\mathbf{C}\mathring{\mathbf{x}}_i) + \mathcal{K}(\mathbf{C}\Delta\mathbf{x}_i) + \mathbf{F}_{\tau_{i+1}})\mathbf{f}_i \tag{19a}$$

$$= \underbrace{\mathbf{A}_{\tau_{i+1}}\mathring{\mathbf{x}}_i + \mathbf{B}_{\tau_{i+1}}\mathcal{K}(\mathbf{C}\mathring{\mathbf{x}}_i)}_{\mathring{\mathbf{x}}_{i+1}} + \underbrace{(\mathbf{A}_{\tau_{i+1}} + \mathbf{B}_{\tau_{i+1}}\mathbf{F}_{\tau_{i+1}})\mathbf{f}_i}_{\mathbf{f}_{i+1}} + \underbrace{\mathbf{A}_{\tau_{i+1}}\Delta\mathbf{x}_i + \mathbf{B}_{\tau_{i+1}}\mathcal{K}(\mathbf{C}\Delta\mathbf{x}_i)}_{\Delta\mathbf{x}_{i+1}}, \tag{19b}$$

where we have made use of the fact that the controller C is linear and that $\mathbf{C}\mathbf{f}_i = \mathbf{0}$ for all i, as $\mathbf{f}_i \in \ker(\mathbf{C})$. As a base case, we have $\mathbf{x}_1 = \mathbf{A}_{\tau_1}\mathring{\mathbf{x}}_0 + \mathbf{B}_{\tau_1}\mathcal{K}(\mathbf{C}\mathring{\mathbf{x}}_0) + (\mathbf{A}_{\tau_1} + \mathbf{F}_{\tau_1}\mathbf{B}_{\tau_1})\mathbf{f}_0 - \mathbf{A}_{\tau_1}\mathbf{f}_0$, and as such, we can recursively write

$$\Delta\mathbf{x}_i = -\Big(\sum_{\ell=2}^{i-1}\mathbf{A}_{\tau_\ell}\mathbf{A}_{\tau_1}\mathbf{f}_0 + \sum_{\ell=3}^{i-1}\mathbf{A}_{\tau_\ell}\mathbf{B}_{\tau_2}\mathcal{K}(\mathbf{C}\Delta\mathbf{x}_1) + \ldots + \mathbf{B}_{\tau_{i-1}}\mathcal{K}(\mathbf{C}\Delta\mathbf{x}_{i-1})\Big), \tag{20}$$

where $\|\mathbf{C}\Delta\mathbf{x}_i\| = \|\mathring{\mathbf{y}}_i - \mathbf{y}_i\|$ is the part of the attack trajectory detectable from the output. Note that (20) is identical to the trajectory as caused by the initial condition $\mathbf{A}_{\tau_1}\mathbf{f}_0$, which by Assumption 2 is bounded (i.e., $\|\Delta\mathbf{x}_i\| < M$, for all i) as $\lim_{i\to\infty}\Delta\mathbf{x}_i = \mathbf{0}$. Furthermore, from (20), we see that $\mathbf{f}_0 \to \mathbf{0}$ (and by extension, $\Delta\mathbf{x}_1, \Delta\mathbf{x}_2, \ldots$) implies $\Delta\mathbf{x}_i \to \mathbf{0}$, which implies that for any $\epsilon \in \mathbb{R}_{>0}$, there exists an $\mathbf{f}_0 \neq \mathbf{0}$ such that $\|\mathbf{C}\Delta\mathbf{x}_i\| < \epsilon$ for all i. ■

The exact bound $\|\mathbf{C}\Delta\mathbf{x}_i\| < \epsilon$ is hard to capture and depends on the controller C and sampling policy $\mathcal{S}$. For many non-uniform sampling policies [17, 27, 34, 38], linear matrix inequality-based conditions for asymptotic stability exist, which give a bound by means of a Lyapunov function. Choosing a vector $\mathbf{f}_0$ sufficiently small often suffices for practical stealthiness. By Assumption 4, we have that $\{\underset{\sim}{\mathcal{P}}, C, \mathcal{S}\} \in \mathbb{I}_{\mathrm{a}}(t)$, meaning the adversary could simulate (20) and iteratively decrease the magnitude of $\mathbf{f}_0$ until a suitable ϵ-stealthiness is reached.

Note that according to (18), we have that $\mathbf{x}_i = \mathring{\mathbf{x}}_i + \Delta\mathbf{x}_i + \mathbf{f}_i$, and combined with $\mathbf{f}_i \in V^\star$, we have that $\mathbf{x}_i \in (\mathring{\mathbf{x}}_i + \Delta\mathbf{x}_i) + V^\star \in \mathbb{R}^{n_{\mathrm{x}}}/V^\star$, as visualized in Figure 3(b). This result shows that, in contrast to previous suggestions [62], ZDAs can remain stealthy even if the system is not in steady state. The former exploits the linearity of the systems [7], such that the influence of the nominal trajectory and the additive attack can be decoupled.

While $\tau_i \in \mathbb{H}$ might not be known in advance by the adversary (and, for that matter, neither by the control system), one often has that $\#\mathbb{H} < \infty$. As $\mathcal{S} \in \mathbb{I}_{\mathrm{a}}(t)$ and therefore, by extension, $\mathbb{H} \in \mathbb{I}_{\mathrm{a}}(t)$, in many scenarios, the design of the set of friends $\{\mathbf{F}_\tau\}_{\tau\in\mathbb{H}}$ can be pre-computed offline before the attack is initiated. Given the sampling dynamics $\mathcal{P}_{\mathrm{sl}}$, one can find a friend $\mathbf{F}_\tau$ for each $\tau \in \mathbb{H}$. In general, it holds that $\mathbb{F}(V^\star) = \{-\mathbf{U}(\mathbf{V}^{\mathsf{T}}\mathbf{V})^{-1}\mathbf{V}^{\mathsf{T}} + \mathbf{G}\mathbf{H} \,|\, \ker(\mathbf{H}) = V^\star\}$, where $\mathrm{Im}(\mathbf{V}) = V^\star$ and $\mathbf{U} \in \mathbb{R}^{n_{\mathrm{u}}\times\dim(V^\star)}$ is the solution to $\mathbf{A}_\tau V^\star = V^\star + \mathbf{B}_\tau\mathbf{U}$ [60], meaning $\mathbb{F}(V^\star)$ forms an affine space. Concluding, this brings us to the following result:

Proposition 4.8. *Suppose $\underset{\sim}{\mathcal{P}}$ is SISO, has relative degree $n_\nu > 2$, and furthermore $\sup\mathbb{H} < \underline{\tau}^*$, with $\underline{\tau}^*$ as in Lemma 3.3. Then, for all $\epsilon \in \mathbb{R}_{>0}$, there exists an initial condition $\mathbf{f}_0 \in V^\star \setminus \{\mathbf{0}\}$ such that the switched ZDA satisfies Problem 1.*

Proof. The ϵ-stealthiness of the switched ZDA was established in Proposition 4.7. Since $\sup\mathbb{H} < \underline{\tau}^*$, according to Lemma 3.3, the largest inter-sample time is strictly smaller than the one needed for stable sampling zeros. Since $n_\nu > 2$, according to Theorem 3.1, the individual modes of the inter-sample dynamics $\mathcal{P}_{\mathrm{sl}}$ have at least one unstable sampling zero for all $\tau \in \mathbb{H}$. Then, according to Lemma 4.5, the matrix $\mathbf{A}_\tau + \mathbf{B}_\tau\mathbf{F}_\tau$ will have at least one unstable eigenvector contained in $V^\star$. Therefore, we have that $\lim_{i\to\infty}\|\mathbf{f}_i\| = \infty$. Recalling that $\mathbf{x}_i = \mathring{\mathbf{x}}_i + \mathbf{f}_i + \Delta\mathbf{x}$, we have that $\lim_{t\to\infty}\|\boldsymbol{\chi}(t)\| = \infty$. ∎

4.1 Attack Space

As evident from (17), Assumption 4 is crucial, meaning the adversary is not only a strong adversary but is also able to determine the next sampling instant, as $\tau_{i+1} \in \mathbb{I}_{\mathrm{a}}(t_i)$. The relationship with a conventional ZDA (on a periodically sampled plant) can be seen in Figure 4. Here, we describe how the adversary might acquire τ_{i+1} for different sampling policies $\mathcal{S}$:

- *STC Policy $\mathcal{S}_{\mathrm{s}}$.* In STC, the next sampling instant t_{i+1} is transmitted from the controller to the sensors. Therefore, if the adversary is able to eavesdrop on this message, the adversary can determine $\tau_{i+1} = t_{i+1} - t_i$.
- *ETC Policy $\underset{\sim}{\mathcal{S}}_{\mathrm{c}}$ or $\mathcal{S}_{\mathrm{p}}$.* In ETC, although the next sampling instant is not known beforehand by the control system and therefore neither by the adversary, these systems sometimes reach a periodic regime after a finite transient [29, 65]. Therefore, with sufficient patience and disclosure resources on when the ith measurement is transmitted, the adversary can eventually predict the next sampling instant.
- *Periodic Schedule $\mathcal{S}_{\mathrm{t}}$:* The schedule of length m inter-sample times (i.e., $\#\mathbb{H} \leq m$) is known in advance. As by Assumption 4, $\mathcal{S}_{\mathrm{t}} \in \mathbb{I}_{\mathrm{a}}(t)$, the adversary can determine the next inter-sample time $\tau_{i+1} = \vec{\tau}_{(i+1) \bmod m}$, where a mod b denotes the remainder of a when divided by b.

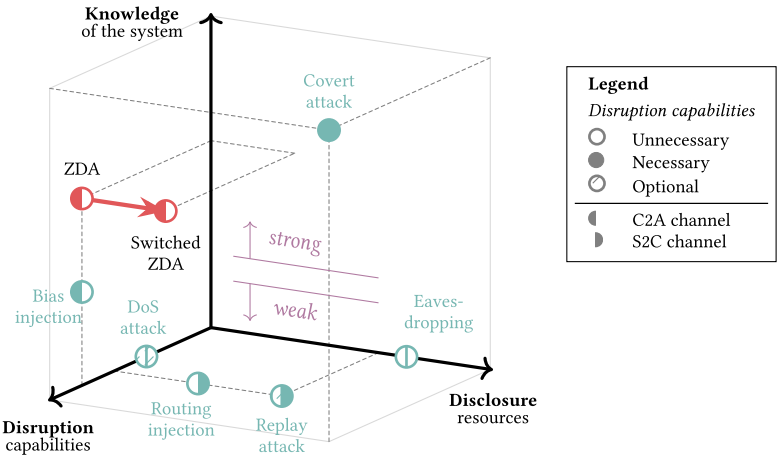


Fig. 4. Cyber-physical attack space, adapted from [76, Figure 1]. Switched ZDAs require additional disclosure resources.

5 Resilience to Switched Zero Dynamic Attacks

As outlined in Problem 1, in order for the attack to be successful, the attack needs to be both disruptive and ϵ-stealthy. In this section, we explain two possible countermeasures to switched ZDAs based on violating either one of the former conditions.

5.1 Existing Countermeasures

Several countermeasures against conventional ZDAs on periodic sampled-data systems have been proposed in the literature [49, 57, 74], such as a GH device at the actuators [49] or multi-rate sampling [57].

The aforementioned countermeasures have only been considered for periodic sampled-data systems. As such, we have extended the proposed GH scheme in [49] to accommodate for non-uniform sampling, by precomputing and storing the different hold patterns (for different inter-sample times) at the actuators. Note that for GH, the next inter-sample time τ_{i+1} needs to be known at the sampling instant t_i, and as such, this countermeasure can only be used for a schedule policy $\mathcal{S}_\mathrm{t}$ or STC policy $\mathcal{S}_\mathrm{s}$. A disadvantage of GH is that the digital controller C often needs to be reconfigured to mitigate some of the performance loss [49].

Dual-rate control as proposed in [57], where the sensors sample more often than that the hold device refreshes, can also be extended to non-uniformly sampled-data systems. Here, we consider updating the control input based on the sensor policy $\mathcal{S}$, but sending measurement updates periodically at a faster rate, leading to a dual-rate control scheme. Note that this does come at the expense of more redundant communications over the bandwidth-limited communication network. Both countermeasures are compared in Section 6.

5.2 Extending Inter-Sample Times

In some cases, ETC and STC sampling policies can eventually reach a periodic regime. Therefore, if the inter-sample times τ_i in this periodic regime are large enough, the sampling zeros are stable according to Lemma 3.2, and the switched ZDA will no longer be disruptive.

Proposition 5.1. *Suppose the sampling policy $\mathcal{S}$ is such that there exists an $i' \in \mathbb{N}$, such that for all $i \geq i'$, $\tau_{i+m} = \tau_i$ with $m \in \mathbb{N}$, yielding the sequence $(\vec{\tau}_k)_{k=1}^m$. Furthermore, define*

$$\vec{\mathbf{M}} = (\mathbf{A}_{\vec{\tau}_1} + \mathbf{F}_{\vec{\tau}_1}\mathbf{B}_{\vec{\tau}_1})(\mathbf{A}_{\vec{\tau}_2} + \mathbf{F}_{\vec{\tau}_2}\mathbf{B}_{\vec{\tau}_2}) \cdots (\mathbf{A}_{\vec{\tau}_m} + \mathbf{F}_{\vec{\tau}_m}\mathbf{B}_{\vec{\tau}_m}). \tag{21}$$

If $\lambda_{\max}(\vec{\mathbf{M}} \mid V^\star) < 1$, then the attack $(\mathbf{a}_i)_{i\in\mathbb{N}_0}$ defined in Definition 4.6 is no longer disruptive.

Proof. Combining (21) with (17), we can write

$$\lim_{i\to\infty} \mathbf{f}_i = \lim_{i\to\infty} \sum_{\ell=1}^{i} (\mathbf{A}_{\tau_\ell} + \mathbf{B}_{\tau_\ell}\mathbf{F}_{\tau_\ell})\mathbf{f}_0 = \lim_{i\to\infty} \vec{\mathbf{M}}^i \underbrace{\sum_{\ell=1}^{i'-1} (\mathbf{A}_{\tau_\ell} + \mathbf{B}_{\tau_\ell}\mathbf{F}_{\tau_\ell})}_{\mathbf{M}} \mathbf{f}_0 = \lim_{i\to\infty} \vec{\mathbf{M}}^i \mathbf{M}\mathbf{f}_0. \tag{22}$$

As $i' \in \mathbb{N}$ is finite, we have that the $\mathbf{M}$ as in (22) is bounded, i.e., $\|\mathbf{M}\| < \infty$. Note that $\mathbf{f}_i \in V^\star$ for all i, and as such, $\mathbf{M}\mathbf{f}_i = \mathbf{f}_{i'-1} \in V^\star$. With $\lambda_{\max}(\vec{\mathbf{M}} \mid V^\star) < 1$, we have that $\|\mathbf{f}_{i'-1}\| > \|\mathbf{f}_{i'}\| > \|\mathbf{f}_{i'+1}\| > \ldots$, which implies $\lim_{i\to\infty} \mathbf{f}_i = \lim_{i\to\infty} \vec{\mathbf{M}}^i \mathbf{M}\mathbf{f}_0 = \mathbf{0}$. Finally, from (18), we have that $\mathbf{x}_i = \mathring{\mathbf{x}}_i + \mathbf{f}_i + \Delta\mathbf{x}_i$, where $\lim_{i\to\infty} \mathring{\mathbf{x}}_i = \lim_{i\to\infty} \Delta\mathbf{x}_i = \mathbf{0}$ by Assumption 2. As such, $\lim_{i\to\infty} \|\mathbf{x}_i\| = \lim_{i\to\infty} \|\mathring{\mathbf{x}}_i + \mathbf{f}_i + \Delta\mathbf{x}_i\| \leq \lim_{i\to\infty} \|\mathring{\mathbf{x}}_i\| + \|\mathbf{f}_i\| + \|\Delta\mathbf{x}_i\| = 0$, proving the attack is not disruptive. ∎

For a periodic scheduling policy $\mathcal{S}_\mathrm{t}$, one trivially has that such an i' exists, with $i' = 0$. Note that for STC and ETC, the sequence of inter-sample times $\vec{\tau}_1, \ldots, \vec{\tau}_m$, provided they exist, can be obtained using ETCetera [19] for a linear PETC system with full-state feedback quadratic triggering condition (some STC implementations are equivalent to PETC implementations in the noise-free case, see for instance [55, 71] and [21, 27]). Guarantees for when the traffic automaton contains a minimizing cycle are given in [30, Proposition 13]. Note that while we are dealing with output feedback and, furthermore, the observation error $\tilde{\mathbf{x}}_i = \hat{\mathbf{x}}_i - \mathbf{x}_i$ might be very large, an abstraction can still be constructed as the next sampling time is based solely on the estimated state vector $\hat{\mathbf{x}}_i$.

Remark 6. It must be noted that there is a qualitative difference between using a periodic schedule $\mathcal{S}_\mathrm{t}$, with sequence $(\vec{\tau}_k)_{k=1}^m$, compared to an STC or ETC policy $\mathcal{S}$ which eventually reaches the same periodic sequence. Namely, STC and ETC can sample faster (or slower) whenever need be, having the advantage of "feedback" in determining the transmission times [32]. This often provides better guarantees on control performance. In that same spirit, one can use periodic control $\mathbb{H} = \{h\}$ and increase the sampling period $h \in \mathbb{R}_{>0}$ such that the discretized plant $\mathcal{P}_\mathrm{sl}$ no longer contains unstable sampling zeros. However, choosing such a sampling period is based fundamentally on a worst-case analysis across the state-space of the system [28].

5.3 Inter-Sample Time Mismatch

Clearly, one big assumption for the adversary to succeed is that the adversary knows the next inter-sample time τ_{i+1}. In Section 4.1, we described how an adversary might come about this knowledge. It can be, however, that this knowledge is actually much harder to obtain, meaning Assumption 4 is (partially) violated, i.e., $\tau_{i+1} \notin \mathbb{I}_\mathrm{a}(t_i)$. Instead, the adversary might only have access to an estimate $\hat{\tau}_{i+1} \in \mathbb{I}_\mathrm{a}(t_i)$, and for some i, we might have $\hat{\tau}_{i+1} \neq \tau_{i+1}$, i.e., the inter-sample time as predicted by the adversary does not match the actual inter-sample time.

A scenario where this can occur is ETC, where the next sampling instant t_{i+1} is not known in advance, neither to the adversary nor the control system. As discussed in Section 4.1, for some implementations, the inter-sample times settle on a periodic regime. However, for a given design of $\mathcal{S}$, it might also happen that the sequence of inter-sample times $(\tau_i)_{i\in\mathbb{N}}$ is chaotic [29]. This can

make it increasingly challenging for the adversary to reliably predict the next inter-sample time, as there is no discernible pattern in previous inter-sample times on which the adversary can rely. Inspired hereby, we have the following proposition:

Proposition 5.2. *Consider a switched ZDA* $(\hat{\mathbf{a}}_i)_{i\in\mathbb{N}_0}$*, and suppose the attack is disruptive. Furthermore, suppose* $\tau_{i+1} \notin \mathbb{I}_a(t_i)$*, and instead, only an estimate* $\hat{\tau}_{i+1} \in \mathbb{I}_a(t_i)$ *is known, which replaces* τ_{i+1} *in (17). Then, given an* $\epsilon \in \mathbb{R}_{>0}$*, if for all* i*, there exists an* $i' \geq i$ *such that* $\hat{\tau}_{i'+1} \neq \tau_{i'+1}$*, the switched ZDA will no longer be* ϵ*-stealthy.*

Proof. The proof follows by contradiction. Suppose there exist an $i' \geq i$ such that $\hat{\tau}_{i'+1} \neq \tau_{i'+1}$ for all i and that the *switched* ZDA is ϵ-stealthy for some $\epsilon \in \mathbb{R}_{>0}$. As the attack is disruptive, we have that $\lim_{i\to\infty} \|\mathbf{x}_i\| = \infty$. From (18), it follows that $\mathbf{x}_i = \mathring{\mathbf{x}}_i + \hat{\mathbf{f}}_i + \Delta\mathbf{x}_i$, where $\hat{\mathbf{f}}_i$ can be rewritten from (17), with the estimate of the next inter-sample time $\hat{\tau}_{i+1}$, as

$$\mathcal{A}: \qquad \hat{\mathbf{f}}_{i+1} = (\mathbf{A}_{\hat{\tau}_{i+1}} + \mathbf{B}_{\hat{\tau}_{i+1}}\mathbf{F}_{\hat{\tau}_{i+1}})\hat{\mathbf{f}}_i, \tag{23a}$$

$$\hat{\mathbf{a}}_i = \mathbf{F}_{\hat{\tau}_{i+1}}\hat{\mathbf{f}}_i. \tag{23b}$$

As by Assumption 2 we have that $\lim_{i\to\infty} \mathring{\mathbf{x}}_i = \lim_{i\to\infty} \Delta\mathbf{x}_i = \mathbf{0}$, it follows that $\lim_{i\to\infty} \|\hat{\mathbf{f}}_i\| = \infty$. For ϵ-stealthiness, it must hold that $\|\mathring{\mathbf{y}}_i - \mathbf{y}_i\| < \epsilon$ for all i. Suppose that up until i' the former is satisfied, and without loss of generality we assume $\hat{\tau}_{i+1} = \tau_{i+1}$ for all $i \leq i'$, implying $\hat{\mathbf{f}}_{i'} = \mathbf{f}_i$, with $\mathbf{f}_i$ as in (17a). Under an inter-sample time mismatch $\hat{\tau}_{i'+1} \neq \tau_{i'+1}$, using (18), we have

$$\begin{aligned}\mathbf{x}_{i'+1} &= \mathbf{A}_{\tau_{i'+1}}\mathring{\mathbf{x}}_{i'} + \mathbf{B}_{\tau_{i'+1}}\mathbf{u}_{\mathrm{c},i'} + (\mathbf{A}_{\tau_{i'+1}} + \mathbf{B}_{\tau_{i'+1}}\mathbf{F}_{\hat{\tau}_{i'+1}})\mathbf{f}_{i'} + \mathbf{A}_{\tau_{i'+1}}\Delta\mathbf{x}_{i'} \\ &= \mathring{\mathbf{x}}_{i'+1} + (\mathbf{A}_{\tau_{i'+1}} + \mathbf{B}_{\tau_{i'+1}}\mathbf{F}_{\hat{\tau}_{i'+1}})\mathbf{f}_{i'} + \Delta\mathbf{x}_{i'+1},\end{aligned} \tag{24}$$

where $\mathbf{x}_{i'+1} \neq \mathring{\mathbf{x}}_{i'+1} + \mathbf{f}_{i'+1} + \Delta\mathbf{x}_{i'+1}$, as $\mathbf{f}_{i'+1} = (\mathbf{A}_{\tau_{i'+1}} + \mathbf{B}_{\tau_{i'+1}}\mathbf{F}_{\tau_{i'+1}})\mathbf{f}_{i'}$ and $\hat{\tau}_{i'+1} \neq \tau_{i'+1}$. As such, the residual difference becomes $\|\mathring{\mathbf{y}}_{i'+1} - \mathbf{y}_{i'+1}\| = \left\|\mathbf{C}(\mathbf{B}_{\tau_{i'+1}}(\mathbf{F}_{\tau_{i'+1}} - \mathbf{F}_{\hat{\tau}_{i'+1}})\mathbf{f}_{i'} + \Delta\mathbf{x}_{i'+1})\right\|$, where $\mathbf{B}_{\tau_{i'+1}}(\mathbf{F}_{\tau_{i'+1}} - \mathbf{F}_{\hat{\tau}_{i'+1}})\mathbf{f}_{i'} \notin \ker(\mathbf{C})$, as from (4) the matrices $\mathbf{F}_{\tau_{i'+1}}$ and $\mathbf{F}_{\hat{\tau}_{i'+1}}$ are distinct whenever $\hat{\tau}_{i+1} \neq \tau_{i+1}$. For ϵ-stealthiness, we require that $\left\|\mathbf{C}(\mathbf{B}_{\tau_{i'+1}}(\mathbf{F}_{\tau_{i'+1}} - \mathbf{F}_{\hat{\tau}_{i'+1}})\mathbf{f}_{i'} + \Delta\mathbf{x}_{i'+1})\right\| < \epsilon$, but as $\mathbf{f}_{i'}$ can be arbitrarily large for a sufficiency large i', which by assumption can be arbitrarily large as there exists an $i' \geq i$ for all i, this leads to a contradiction. ∎

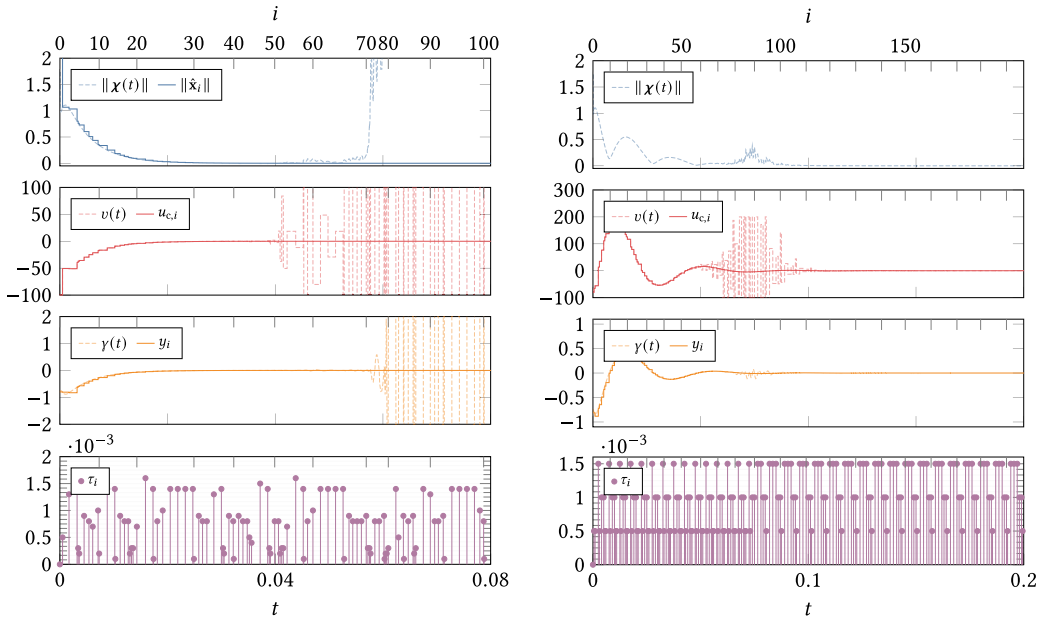
To conclude, either countermeasure as outlined above, or any of the existing countermeasures described in Section 5.1, extended to non-uniformly sampled-data systems, make it such that a switched ZDA $(\mathbf{a}_i)_{i\in\mathbb{N}}$ is no longer a solution to Problem 1.

6 Illustrative Example

Several CPSs that are SISO and have relative degree strictly larger than two have been previously considered in the literature. Examples include a worktable motion control system [22], an in-vehicle networked active suspension system [26], an automatic voltage regulator [58], and a DC-DC converter [48], the latter two of which are used in critical infrastructure such as power grids. We illustrate the vulnerability of sampled-data systems with non-uniform sampling to switched ZDAs, for different sampling policies $\mathcal{S}$, on the DC-DC converter [48]. The dynamics of the DC-DC converter are given by

$$\underset{\sim}{\mathbf{A}} = \begin{bmatrix} -6876.9 & 6605.9 & -6421.8 \\ -5123.1 & 5394.1 & -7578.2 \\ -4123.1 & 4394.1 & -5578.2 \end{bmatrix}, \qquad \underset{\sim}{\mathbf{B}} = \begin{bmatrix} -1 \\ 1 \\ 2 \end{bmatrix}, \qquad \mathbf{C} = \begin{bmatrix} 0 \\ -0.8 \\ 0.8 \end{bmatrix}^{\mathsf{T}}, \tag{25}$$

with relative degree $n_\nu = 3$. A full-state feedback controller $\mathbf{K} = [5861.4 \quad -5590.4 \quad 4406.3]$ has been designed such that $\underset{\sim}{\mathbf{A}} + \underset{\sim}{\mathbf{B}}\mathbf{K}$ is Hurwitz. First, we demonstrate a scenario where an adversary can



(a) Successful switched ZDA with STC policy $\mathcal{S}_s$

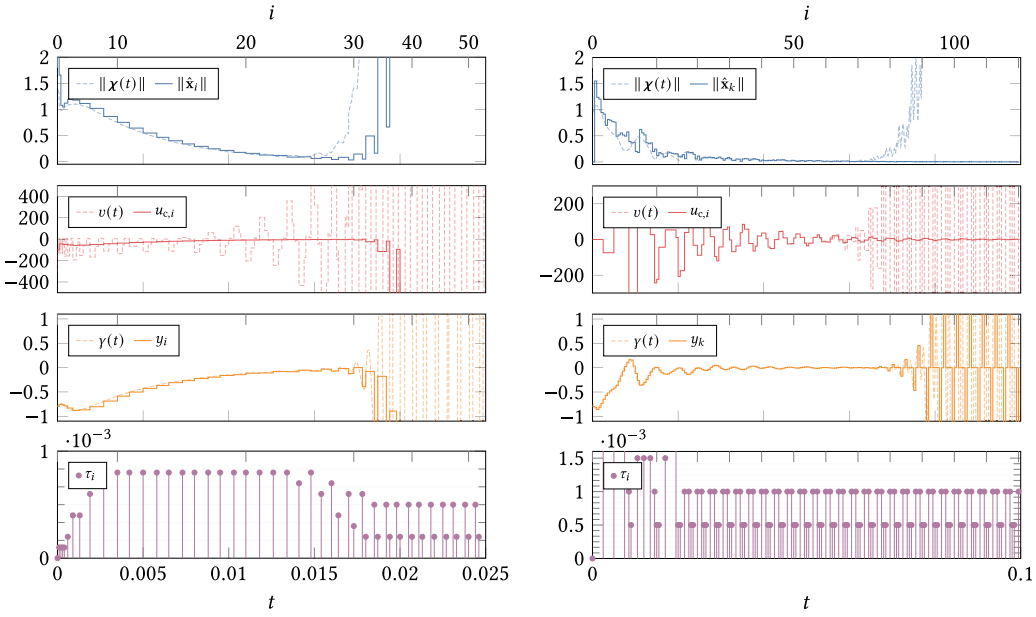
(b) Non-disruptive switched ZDA with schedule $\mathcal{S}_t$

Fig. 5. A switched ZDA on a sampled-data system with non-uniform sampling.

successfully construct a switched ZDA. Consider the STC policy $\mathcal{S}_s$ as in [55], with an observer O whose design is outlined in [3]. The parameters are selected such that $\mathbb{H} = h \cdot \mathbb{N}_{1:50}$, with $h = 2 \cdot 10^{-5}$, guarantees asymptotic stability, satisfying Assumption 2. Furthermore, $\sup \mathbb{H} = 1 \cdot 10^{-3} < \underline{\tau}^* = 1.13 \cdot 10^{-3}$, and therefore, according to Proposition 4.8, the system is vulnerable to a switched ZDA. As the STC policy $\mathcal{S}_s$ transmits the next sample instant t_{i+1} over the C2S channel, as outlined in Section 4.1, the adversary can eavesdrop on this transmission. With $\mathbf{x}_0 = \hat{\mathbf{x}}_0 = \mathbf{1}$, the resulting trajectories can be seen in Figure 5(a), where it becomes evident that the attack remains undetected while the state norm diverges.

Next, we demonstrate how increasing the inter-sample times can lead to the switched ZDA becoming ineffective. For the sake of demonstration, consider a periodic schedule S_t, consisting of $\mathbb{H} = 10^{-3} \cdot \{0.5, 0.5, 1.5, 0.5, 1, 1\}$ (such that the attack initially grows) and $\mathbb{H}' = 10^{-3} \cdot \{1.5, 1.5, 1, 1, 0.5, 1.5\}$ from $t = 0.08$ onward. For the latter, we can compute $\vec{\mathbf{M}}$ and find $\sigma(\vec{\mathbf{M}} \mid V^\star) = \{-0.505, -15.3 \cdot 10^{-2}\}$. Therefore, according to Proposition 5.1, the attack is no longer disruptive. This is illustrated in Figure 5(b), where we observe that under the latter periodic schedule $\mathbb{H}'$, the attack vector decays, making the switched ZDA ineffective.

Finally, we also demonstrate how existing countermeasures can be extended to non-uniform sampled-data systems. To this extent, we consider GH, where, as explained in Section 5.1, the next inter-sample time τ_{i+1} needs to be known in advance. As such, consider the STC policy $\mathcal{S}_s'$ as in [80], with the same observer O. The GH mechanism is designed as outlined in [49], such that the lifted system contains no zeros. The resulting simulation can be seen in Figure 6(a), where it is evident that the switched ZDA is no longer stealthy. Additionally, consider an observer-based PETC policy $\mathcal{S}_p$ as outlined in [34], where the design parameters are set such that $\mathbb{H} = h \cdot \mathbb{N}_{1:5}$, with $h = 5 \cdot 10^{-4}$. The output y_k is sampled and transmitted every h time units, but the input is held for longer based on the PETC policy $\mathcal{S}_p$, leading to the dual-rate scheme. The resulting trajectories



(a) GH countermeasure with STC policy $\mathcal{S}'_s$

(b) Dual-rate countermeasure with PETC policy $\mathcal{S}_p$

Fig. 6. Extension of two existing countermeasures to non-uniformly sampled-data systems.

can be seen in Figure 6(b), where the switched ZDA is detected due to the additional measurements y_k.

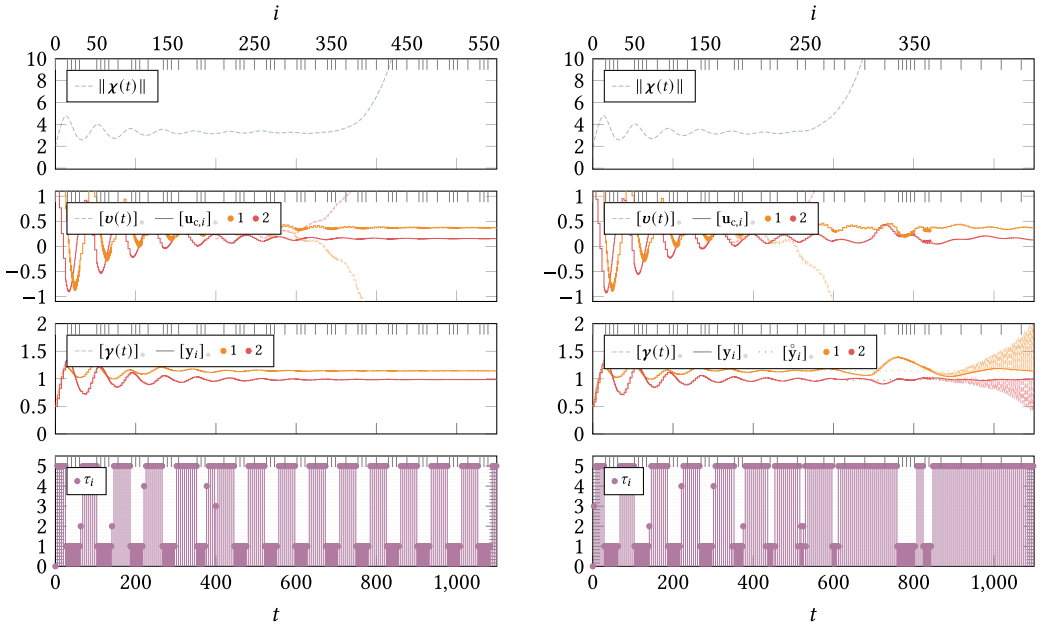
6.1 Quadruple Tank Benchmark

While we have discussed the sampling zeros of SISO systems, **multiple-input and multiple-output (MIMO)** systems can also be vulnerable to switched ZDAs. Unfortunately, the behavior of sampling zeros for MIMO systems is poorly understood. However, the behavior of an *intrinsic zeros* $s \in \mathbb{C}$ under (ZOH) sampling, that is, those zeros which are present in the continuous-time plant $\underset{\sim}{\mathcal{P}}$, is well-approximated by the mapping $z \mapsto e^{h \cdot s}$.[6] This implies that a plant $\underset{\sim}{\mathcal{P}}$ with unstable zeros will generally result in a plant $\mathcal{P}_{\text{sl}}$, whose individual modes have unstable zeros as well. To demonstrate, we take the quadruple tank system as an example [46], which is a commonly used benchmark in the secure control literature [33, 62, 74, 76]. The dynamics of the plant $\underset{\sim}{\mathcal{P}}$ are given by

$$\underset{\sim}{\mathbf{A}} = \begin{bmatrix} -0.016 & 0 & 0.026 & 0 \\ 0 & -0.011 & 0 & 0.018 \\ 0 & 0 & -0.026 & 0 \\ 0 & 0 & 0 & -0.018 \end{bmatrix}, \quad \underset{\sim}{\mathbf{B}} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0.001 \\ 0.001 & 0 \end{bmatrix}, \quad \mathbf{C} = \begin{bmatrix} 50 & 0 \\ 0 & 50 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}^{\mathsf{T}}. \tag{26}$$

We demonstrate the effectiveness of the switched ZDA by considering the two decentralized proportional–integral controllers as described in [46, Section VI] and the task of tracking a stationary reference $\mathbf{1}$. As we are dealing with a dynamic output-feedback controller C, we consider the PETC policy $\mathcal{S}'_p$ as outlined in [27], where the continuous-time controller is discretized with sampling period $h = 1$ using the bilinear transform. With these parameters, the inter-sample times eventually

[6] However, the mapping of a zero is not so simple that it is generally impossible to derive a closed-form expression of the zero z of $\mathcal{P}$ that corresponds to the zero s of $\underset{\sim}{\mathcal{P}}$ in terms of the parameters $\underset{\sim}{\mathbf{A}}$, $\underset{\sim}{\mathbf{B}}$, $\underset{\sim}{\mathbf{C}}$, and h [36].



(a) PETC policy with patient adversary

(b) The effect of inter-sample time mismatch

Fig. 7. A successful switched ZDA on the quadruple tank system and the effect of inter-sample time mismatch.

become periodic with period $m = 22$. Therefore, the adversary can wait, e.g., until $t = 500$, when it has reasonably confirmed the existence of the periodic pattern and commence the attack only then. With $\mathbf{x}_0 = \hat{\mathbf{x}}_0 = \mathbf{0}$, the resulting trajectories can be seen in Figure 7(a), where it becomes evident that the switched ZDA is successful.

Finally, we also demonstrate the effectiveness of inter-sample time mismatch. Considering the same controller C and sampling policy $\mathcal{S}'_{\mathrm{p}}$, we demonstrate what happens when the adversary disregards the non-uniform sampling behavior, and instead constructs a *conventional* ZDA as outlined in Section 2.1 with period $h = 1$. The result can be seen in Figure 7(b), where a clear and detectable deviation in the output can be seen at around $t = 700$. Note that for smaller t this deviation is not noticeable, as the attack vector $\mathbf{a}_i$ is still small.

These simulation results demonstrate, for one, the versatility of switched ZDAs, as they can be constructed mostly irrespective of the sampling policy $\mathcal{S}$ and for more intricate MIMO systems as well.

7 Conclusions and Future Work

In this article, we proposed a new variant of ZDA, named a switched ZDA, and indicated when sampled-data systems with non-uniform sampling are potentially vulnerable to these attacks. The construction of the attack relies on knowledge of the adversary of both the plant dynamics as well as the next inter-sample time. We also proposed two countermeasures that make switched ZDAs ineffective. In several numerical examples, we demonstrated the vulnerability of real-world systems to switched ZDAs and illustrated the effectiveness of the countermeasures.

In line with the work of [12, 63], it is interesting to consider how Assumption 4 can be relaxed, as it is more likely that the adversary (and for that matter, the control system) does not know the exact model dynamics. Extensions of our framework to data-driven approaches, and stealthiness in the

presence of model uncertainty, are considered future work. Investigating the effect of (time-varying) delays in NCSs, and how these affect ZDAs, also in the case of periodic sampling, could prove interesting future directions to research. Other extensions being researched include the effect of actuator saturation, due to limitations in the physical process, on the disruptiveness of (switched) ZDAs [82].

7.1 Extension to Nonlinear Systems and Real-World Experiments

In this article, we have described switched ZDAs and highlighted a key difference with conventional ZDAs. For future research, it will be interesting to investigate how our proposed methodology lends itself to nonlinear systems. Conventional ZDAs have been shown to be effective on both nonlinear systems [62] and real systems by means of experiment [45, 73]. The construction of these attacks often relies on the use of the Byrnes-Isidori normal form [44], originally developed for nonlinear systems. As an adaptation for non-uniform sampling, leading to switched system dynamics, an extension of the Byrnes-Isidori normal form to switched nonlinear systems [14] could provide a starting point, which is left to future work. Experimental validation on a real-world control system is also of future interest.

References

[1] Cesare Alippi. 2014. *Intelligence for Embedded Systems: A Methodological Approach* (1st. ed.). Springer International Publishing, Cham, Zug, Switzerland. DOI: https://doi.org/10.1007/978-3-319-05278-6

[2] João Almeida, Carlos Silvestre, and António Pascoal. 2011. Self-triggered observer based control of linear plants. *IFAC Proceedings Volumes* 44, 1 (Jan. 2011), 10074–10079. DOI: https://doi.org/10.3182/20110828-6-IT-1002.02235

[3] João Almeida, Carlos Silvestre, and Antonio M. Pascoal. 2012. Observer based self-triggered control of linear plants with unknown disturbances. In *Proceedings of the 2012 American Control Conference (ACC)*. IEEE, Montreal, Quebec, Canada, 5688–5693. DOI: https://doi.org/10.1109/ACC.2012.631504811

[4] João Almeida, Carlos Silvestre, and António M. Pascoal. 2014. Self-triggered output feedback control of linear plants in the presence of unknown disturbances. *IEEE Transactions on Automatic Control* 59, 11 (Nov. 2014), 3040–3045. DOI: https://doi.org/10.1109/TAC.2014.2318091

[5] Ross P. Anderson, Dejan Milutinović, and Dimos V. Dimarogonas. 2015. Self-triggered sampling for second-moment stability of state-feedback controlled SDE systems. *Automatica* 54 (Apr. 2015), 8–15. DOI: https://doi.org/10.1016/j.automatica.2015.01.020

[6] K. J. Astrom and B. M. Bernhardsson. 2002. Comparison of Riemann and Lebesgue sampling for first order stochastic systems. In *Proceedings of the 41st IEEE Conference on Decision and Control*. IEEE, Vol. 2, Las Vegas, Nevada, 2011–2016. DOI: https://doi.org/10.1109/CDC.2002.1184824

[7] Cheng-Zong Bai, Fabio Pasqualetti, and Vijay Gupta. 2015. Security in stochastic control systems: Fundamental limitations and performance bounds. In *Proceedings of the 2015 American Control Conference (ACC)*. IEEE, Chicago, Illinois, 195–200. DOI: https://doi.org/10.1109/ACC.2015.7170734

[8] Cheng-Zong Bai, Fabio Pasqualetti, and Vijay Gupta. 2017. Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs. *Automatica* 82 (Aug. 2017), 251–260. DOI: https://doi.org/10.1016/j.automatica.2017.04.047

[9] Angelo Barboni, Ahmad W. Al-Dabbagh, and Thomas Parisini. 2022. An event-triggered watermarking strategy for detection of replay attacks. *IFAC-PapersOnLine* 55, 6 (Jan. 2022), 317–322. DOI: https://doi.org/10.1016/j.ifacol.2022.07.148

[10] Giuseppe Basile and Giovanni Marro. 1992. *Controlled and Conditioned Invariants in Linear System Theory*. Prentice Hall, Englewood Cliffs, NJ.

[11] Alvaro A. Cardenas, Tanya Roosta, and Shankar Sastry. 2009. Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems. *Ad Hoc Networks* 7, 8 (Nov. 2009), 1434–1447. DOI: https://doi.org/10.1016/j.adhoc.2009.04.012

[12] Federico Celi and Fabio Pasqualetti. 2022. Data-Driven meets geometric control: Zero dynamics, subspace stabilization, and malicious attacks. *IEEE Control Systems Letters* 6 (2022), 2569–2574. DOI: https://doi.org/10.1109/LCSYS.2022.3170866

[13] Tongwen Chen and Bruce Allen Francis. 1995. *Optimal Sampled-Data Control Systems* (1st. ed.). Springer London, London, UK. DOI: https://doi.org/10.1007/978-1-4471-3037-6

[14] Daizhan Cheng, Gang Feng, and Zairong Xi. 2006. Stabilization of a class of switched nonlinear systems. *Journal of Control Theory and Applications* 4, 1 (Feb. 2006), 53–61. DOI: https://doi.org/10.1007/s11768-006-5259-0

[15] Michelle S. Chong, Henrik Sandberg, and André M. H. Teixeira. 2019. A tutorial introduction to security and privacy for cyber-physical systems. In *Proceedings of the 2019 18th European Control Conference (ECC)*. IEEE, Napoli, Italy, 968–978. DOI: https://doi.org/10.23919/ECC.2019.8795652

[16] Giuseppe Conte, Anna Maria Perdon, Elena Zattoni, and Bostwick Wyman. 2023. Zeros and zero dynamics of switching systems. *IFAC-PapersOnLine* 56, 2 (2023), 8147–8152. DOI: https://doi.org/10.1016/j.ifacol.2023.10.988

[17] Gabriel de Albuquerque Gleizer and Manuel Mazo. 2020. Self-triggered output-feedback control of LTI systems subject to disturbances and noise. *Automatica* 120 (Oct. 2020), 109129. DOI: https://doi.org/10.1016/j.automatica.2020.109129

[18] C. De Persis and P. Tesi. 2014. Resilient control under denial-of-service. *IFAC Proceedings Volumes* 47, 3 (Jan. 2014), 134–139. DOI: https://doi.org/10.3182/20140824-6-ZA-1003.02184

[19] Giannis Delimpaltadakis, Gabriel de Albuquerque Gleizer, Ivo van Straalen, and Manuel Mazo. Jr. 2022. ETCetera: beyond event-triggered control. In *Proceedings of the 25th ACM International Conference on Hybrid Systems: Computation and Control (HSCC '22)*. ACM, New York, New York, 1–11. DOI: https://doi.org/10.1145/3501710.3519523

[20] V. S. Dolk, P. Tesi, C. De Persis, and W. P. M. H. Heemels. 2017. Event-triggered control systems under denial-of-service attacks. *IEEE Transactions on Control of Network Systems* 4, 1 (Mar. 2017), 93–105. DOI: https://doi.org/10.1109/TCNS.2016.2613445

[21] M. C. F. Donkers. 2011. Networked and Event-Triggered Control Systems. Ph.D. Dissertation. Technische Universiteit Eindhoven, Eindhoven, North Brabant, The Netherlands. DOI: https://doi.org/10.6100/IR716705

[22] Richard C. Dorf and Robert H. Bishop. 2016. *Modern control systems*. (13th. ed.). Pearson, Hoboken. Retrieved from https://files.crazt.moe/temp/Modern%20Control%20Systems%2013th.pdf

[23] Dajun Du, Changda Zhang, Xue Li, Minrui Fei, and Huiyu Zhou. 2023. Attack detection for networked control systems using event-triggered dynamic watermarking. *IEEE Transactions on Industrial Informatics* 19, 1 (Jan. 2023), 351–361. DOI: https://doi.org/10.1109/TII.2022.3168868

[24] Alexander J. Gallo, Sribalaji C. Anand, André M. H. Teixeira, and Riccardo M. G. Ferrari. 2021. Design of multiplicative watermarking against covert attacks. In *Proceedings of the 2021 60th IEEE Conference on Decision and Control (CDC)*. IEEE, Austin, Texas, 4176–4181. DOI: https://doi.org/10.1109/CDC45484.2021.9683075

[25] S. S. Ge, Zhendong Sun, and T. H. Lee. 2001. Reachability and controllability of switched linear systems. In *Proceedings of the 2001 American Control Conference. (Cat. No.01CH37148)*. IEEE, Vol. 3, Arlington, Virginia, 1898–1903. DOI: https://doi.org/10.1109/ACC.2001.946016

[26] Xiaohua Ge, Qing-Long Han, Xian-Ming Zhang, and Derui Ding. 2021. Dynamic event-triggered control and estimation: A survey. *International Journal of Automation and Computing*. 18, 6 (Dec. 2021), 857–886. DOI: https://doi.org/10.1007/s11633-021-1306-z

[27] Gabriel de A. Gleizer and Manuel Mazo. 2018. Self-triggered output feedback control for perturbed linear systems. *IFAC-PapersOnLine* 51, 23 (Jan. 2018), 248–253. DOI: https://doi.org/10.1016/j.ifacol.2018.12.043

[28] Gabriel de A. Gleizer and Manuel Mazo. 2021. Computing the sampling performance of event-triggered control. In *Proceedings of the 24th International Conference on Hybrid Systems: Computation and Control (HSCC '21)*. ACM, New York, New York, 1–7. DOI: https://doi.org/10.1145/3447928.3456635

[29] Gabriel de Albuquerque Gleizer and Manuel Mazo. 2023. Chaos and order in event-triggered control. *IEEE Transactions on Automatic Control* 68, 11 (Nov. 2023), 6541–6556. DOI: https://doi.org/10.1109/TAC.2023.3242334

[30] Gabriel de Albuquerque Gleizer and Manuel Mazo Jr. 2022. Chaos and order in event-triggered control. arXiv:2201.04462. DOI: https://doi.org/10.48550/arXiv.2201.04462

[31] Eric Goetz and Sujeet Shenoi (Eds.). 2007. *Critical Infrastructure Protection*. IFIP International Federation for Information Processing, Vol. 253. Springer US, Boston, MA. DOI: https://doi.org/10.1007/978-0-387-75462-8

[32] Tom Gommans, Duarte Antunes, Tijs Donkers, Paulo Tabuada, and Maurice Heemels. 2014. Self-triggered linear quadratic control. *Automatica* 50, 4 (Apr. 2014), 1279–1287. DOI: https://doi.org/10.1016/j.automatica.2014.02.030

[33] W. Steven Gray, Luis A. Duffaut Espinosa, and M. Aminul Haq. 2022. Universal zero dynamics attacks using only input-output data. In *Proceedings of the 2022 American Control Conference (ACC)*. IEEE, Atlanta, Georgia, 4985–4991. DOI: https://doi.org/10.23919/ACC53348.2022.9867481

[34] L. B. Groff, L. G. Moreira, J. M. Gomes da Silva, and D. Sbarbaro. 2016. Observer-based event-triggered control: A discrete-time approach. In *Proceedings of the 2016 American Control Conference (ACC)*. IEEE, Boston, Massachusetts, 4245–4250. DOI: https://doi.org/10.1109/ACC.2016.7525589

[35] Rachana Ashok Gupta and Mo-Yuen Chow. 2010. Networked control system: Overview and research trends. *IEEE Transactions on Industrial Electronics* 57, 7 (Jul. 2010), 2527–2535. DOI: https://doi.org/10.1109/TIE.2009.2035462

[36] T. Hagiwara. 1996. Analytic study on the intrinsic zeros of sampled-data systems. *IEEE Transactions on Automatic Control* 41, 2 (Feb. 1996), 261–263. DOI: https://doi.org/10.1109/9.481531

[37] W. P. M. H. Heemels, K. H. Johansson, and P. Tabuada. 2012. An introduction to event-triggered and self-triggered control. In *Proceedings of the 012 IEEE 51st IEEE Conference on Decision and Control (CDC)*. IEEE, Maui, Hawaii, 3270–3285. DOI: https://doi.org/10.1109/CDC.2012.6425820

[38] W. P. M. H. Heemels and M. C. F. Donkers. 2013. Model-based periodic event-triggered control for linear systems. *Automatica* 49, 3 (Mar. 2013), 698–711. DOI: https://doi.org/10.1016/j.automatica.2012.11.025

[39] W. P. M. H. Heemels, M. C. F. Donkers, and Andrew R. Teel. 2013. Periodic event-triggered control for linear systems. *IEEE Transactions on Automatic Control* 58, 4 (Apr. 2013), 847–861. DOI: https://doi.org/10.1109/TAC.2012.2220443

[40] W. P. M. H. Heemels, J. H. Sandee, and P. P. J. Van Den Bosch. 2008. Analysis of event-driven controllers for linear systems. *International Journal of Control* 81, 4 (Apr. 2008), 571–590. DOI: https://doi.org/10.1080/00207170701506919

[41] Laurentiu Hetel, Christophe Fiter, Hassan Omran, Alexandre Seuret, Emilia Fridman, Jean-Pierre Richard, and Silviu Iulian Niculescu. 2017. Recent developments on the stability of systems with aperiodic sampling: An overview. *Automatica* 76 (Feb. 2017), 309–335. DOI: https://doi.org/10.1016/j.automatica.2016.10.023

[42] Fangyuan Hou and Jian Sun. 2017. Covert attacks against output tracking control of cyber-physical systems. In *Proceedings of the 43rd Annual Conference of the IEEE Industrial Electronics Society (IECON '17)*. IEEE, Beijing, China, 5743–5748. DOI: https://doi.org/10.1109/IECON.2017.8216996.

[43] Xiaoming Hu. 2012. Geometric Control Theory. Retrieved from https://www.math.kth.se/optsyst/grundutbildning/kurser/SF2842/Lecturenotes

[44] Alberto Isidori. 2013. The zero dynamics of a nonlinear system: From the origin to the latest progresses of a long successful story. *European Journal of Control* 19, 5 (Sep. 2013), 369–378. DOI: https://doi.org/10.1016/j.ejcon.2013.05.014

[45] Hamidreza Jafarnejadsani, Hanmin Lee, Naira Hovakimyan, and Petros Voulgaris. 2018. A multirate adaptive control for MIMO systems with application to cyber-physical security. In *Proceedings of the 2018 IEEE Conference on Decision and Control (CDC)*. IEEE, Miami, Florida, 6620–6625. DOI: https://doi.org/10.1109/CDC.2018.8619570

[46] K. H. Johansson. 2000. The quadruple-tank process: A multivariable laboratory process with an adjustable zero. *IEEE Transactions on Control Systems Technology* 8, 3 (May 2000), 456–465. DOI: https://doi.org/10.1109/87.845876.

[47] Xile Kang and Hideaki Ishii. 2023. Effects of quantization on zero-dynamics attacks to closed-loop sampled-data control systems. In *Proceedings of the 2023 62nd IEEE Conference on Decision and Control (CDC)*. IEEE, Marina Bay Sands, Singapore, 846–851. DOI: https://doi.org/10.1109/CDC49753.2023.10383573

[48] Bumsu Kim, Kunhee Ryu, and Juhoon Back. 2022. A generalized hold based countermeasure against zero-dynamics attack with application to DC-DC converter. *IEEE Access* 10 (2022), 44923–44933. DOI: https://doi.org/10.1109/ACCESS.2022.3168128

[49] Jihan Kim, Juhoon Back, Gyunghoon Park, Chanhwa Lee, Hyungbo Shim, and Petros G. Voulgaris. 2020. Neutralizing zero dynamics attack on sampled-data systems via generalized holds. *Automatica* 113 (Mar. 2020), 108778. DOI: https://doi.org/10.1016/j.automatica.2019.108778

[50] Jihan Kim, Gyunghoon Park, Hyungbo Shim, and Yongsoon Eun. 2019. Masking attack for sampled-data systems via input redundancy. *IET Control Theory & Applications* 13, 14 (2019), 2300–2308. DOI: https://doi.org/10.1049/iet-cta.2018.6075

[51] Kosuke Kimura and Hideaki Ishii. 2022. Quantized zero dynamics attacks against sampled-data control systems. In *Proceedings of the 2022 IEEE 61st Conference on Decision and Control (CDC)*. IEEE, Cancún, Quintana Roo, Mexico, 6140–6145. DOI: https://doi.org/10.1109/CDC51059.2022.9992601

[52] Kosuke Kimura and Hideaki Ishii. 2024. Quantized zero dynamics attacks against Sampled-Data control systems. *IEEE Transactions on Automatic Control* 69, 5 (Nov. 2024), 3418–3425. DOI: https://doi.org/10.1109/TAC.2023.3338051

[53] Seung-Hi Lee, Young-Hoon Kim, and Chung Choo Chung. 2002. Multirate digital control system design. In *Proceedings of the 2002 American Control Conference*, Vol. 3, IEEE, Anchorage, Alaska, 1861–1866. DOI: https://doi.org/10.1109/ACC.2002.1023903

[54] Steffen Linsenmayer, Dimos V. Dimarogonas, and Frank Allgöwer. 2019. Periodic event-triggered control for networked control systems based on non-monotonic Lyapunov functions. *Automatica* 106 (Aug. 2019), 35–46. DOI: https://doi.org/10.1016/j.automatica.2019.04.039

[55] Manuel Mazo, Adolfo Anta, and Paulo Tabuada. 2010. An ISS self-triggered implementation of linear controllers. *Automatica* 46, 8 (Aug. 2010), 1310–1314. DOI: https://doi.org/10.1016/j.automatica.2010.05.009

[56] Bengt Mårtensson. 1982. Zeros of Sampled Systems. Master's thesis. Lund University, Lund, Skåne, Sweden.

[57] Mohammad Naghnaeian, Nabil Hirzallah, and Petros G. Voulgaris. 2015. Dual rate control for security in cyber-physical systems. In *Proceedings of the 2015 54th IEEE Conference on Decision and Control (CDC)*. IEEE, Osaka, Honshu, Japan, 1415–1420. DOI: https://doi.org/10.1109/CDC.2015.7402409

[58] Mohammad Naghnaeian, Nabil H. Hirzallah, and Petros G. Voulgaris. 2019. Security via multirate control in cyber–physical systems. *Systems & Control Letters* 124 (Feb. 2019), 12–18. DOI: https://doi.org/10.1016/j.sysconle.2018.12.001

[59] Amir Norouzi Mobarakeh, Mohammad Ataei, and Rahmat-Allah Hooshmand. 2024. The threat of zero-dynamics attack on non-linear cyber-physical systems. *IET Cyber-Physical Systems: Theory & Applications* 9, 4 (Jun. 2024), 463–476. DOI: https://doi.org/10.1049/cps2.12099

[60] Lorenzo Ntogramatzidis, Thang Nguyen, and Robert Schmid. 2015. Repeated eigenstructure assignment for controlled invariant subspaces. *European Journal of Control* 26 (Nov. 2015), 1–11. DOI: https://doi.org/10.1016/j.ejcon.2015.07.003

[61] Minghui Ou, Zhiyong Yang, Zhenjie Yan, Mingkun Ou, Shuanghong Liu, Shan Liang, and Shengjiu Liu. 2022. Stability of zeros for Sampled-Data models with triangle sample and hold implemented by zero-order hold. *Machines* 10, 5 (2022), 386. DOI: https://doi.org/10.3390/machines10050386

[62] Gyunghoon Park, Chanhwa Lee, and Hyungbo Shim. 2018. On stealthiness of zero-dynamics attacks against uncertain nonlinear systems: A case study with quadruple-tank process (I). In *Proceedings of the 23rd International Symposium on Mathematical Theory of Networks and Systems*. Hong Kong University of Science and Technology, Hong Kong, China, 10–17. Retrieved from https://mtns2018.hkust.edu.hk/proceedings_online.html

[63] Gyunghoon Park, Chanhwa Lee, Hyungbo Shim, Yongsoon Eun, and Karl H. Johansson. 2019. Stealthy adversaries against uncertain cyber-Physical systems: Threat of robust zero-dynamics attack. *IEEE Transactions on Automatic Control* 64, 12 (Dec. 2019), 4907–4919. DOI: https://doi.org/10.1109/TAC.2019.2903429

[64] Chen Peng and Qing-Long Han. 2013. A novel event-triggered transmission scheme and $\mathcal{L}_2$ control co-design for sampled-data control systems. *IEEE Transactions on Automatic Control* 58, 10 (Oct. 2013), 2620–2626. DOI: https://doi.org/10.1109/TAC.2013.2256015

[65] Anusree Rajan and Pavankumar Tallapragada. 2020. Analysis of inter-event times for planar linear systems under a general class of event triggering rules. In *Proceedings of the 2020 59th IEEE Conference on Decision and Control (CDC)*. IEEE, Jeju Island, Republic of Korea, 5206–5211. DOI: https://doi.org/10.1109/CDC42340.2020.9304406

[66] Henrik Sandberg. 2020. Cyber-physical security. In *Encyclopedia of Systems and Control*, John Baillieul and Tariq Samad (Eds.), Springer, London, UK, 1–8. DOI: https://doi.org/10.1007/978-1-4471-5102-9_100112-1

[67] Henrik Sandberg, Vijay Gupta, and Karl H. Johansson. 2022. Secure networked control systems. *Annual Review of Control, Robotics, and Autonomous Systems* 5, 1 (May 2022), 445–464. DOI: https://doi.org/10.1146/annurev-control-072921-075953

[68] D. Sbarbaro, S. Tarbouriech, and J. M. Gomes da Silva. 2014. An event-triggered observer based control strategy for SISO systems. In *Proceedings of the 53rd IEEE Conference on Decision and Control*. IEEE, Los Angeles, California, 2789–2794. DOI: https://doi.org/10.1109/CDC.2014.7039817

[69] Hyungbo Shim, Juhoon Back, Yongsoon Eun, Gyunghoon Park, and Jihan Kim. 2022. Zero-dynamics attack, variations, and countermeasures. In *Security and Resilience of Control Systems: Theory and Applications*, Hideaki Ishii and Quanyan Zhu (Eds.), Springer International Publishing, Zurich, Zurich, Switzerland, 31–61. DOI: https://doi.org/10.1007/978-3-030-83236-0_2

[70] Jill Slay and Michael Miller. 2007. Lessons learned from the Maroochy water breach. In *Critical Infrastructure Protection*, Eric Goetz and Sujeet Shenoi (Eds.), Vol. 253, Springer US, Boston, MA, 73–82. DOI: https://doi.org/10.1007/978-0-387-75462-8_6

[71] Aleksandra Szymanek, Gabriel de A. Gleizer, and Manuel Mazo. 2019. Periodic event-triggered control with a relaxed triggering condition. In *Proceedings of the 2019 IEEE 58th Conference on Decision and Control (CDC)*. IEEE, Nice, Alpes-Maritimes, France, 1656–1661. DOI: https://doi.org/10.1109/CDC40024.2019.90298231

[72] Paulo Tabuada. 2007. Event-triggered real-time scheduling of stabilizing control tasks. *IEEE Transactions on Automatic Control* 52, 9 (Sep. 2007), 1680–1685. DOI: https://doi.org/10.1109/TAC.2007.904277

[73] André Teixeira, Daniel Pérez, Henrik Sandberg, and Karl Henrik Johansson. 2012. Attack models and scenarios for networked control systems. In *Proceedings of the 1st International Conference on High Confidence Networked Systems (HiCoNS '12)*. ACM, New York, 55–64. DOI: https://doi.org/10.1145/2185505.2185515

[74] André Teixeira, Iman Shames, Henrik Sandberg, and Karl H. Johansson. 2012. Revealing stealthy attacks in control systems. In *Proceedings of the 2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, Liverpool, Merseyside, UK, 1806–1813. DOI: https://doi.org/10.1109/Allerton.2012.6483441

[75] André Teixeira, Iman Shames, Henrik Sandberg, and Karl Henrik Johansson. 2015. A secure control framework for resource-limited adversaries. *Automatica* 51 (Jan. 2015), 135–148. DOI: https://doi.org/10.1016/j.automatica.2014.10.067

[76] Andre Teixeira, Kin Cheong Sou, Henrik Sandberg, and Karl Henrik Johansson.2015. Secure control systems: A quantitative risk management approach. *IEEE Control Systems Magazine* 35, 1 (Feb. 2015), 24–45. DOI: https://doi.org/10.1109/MCS.2014.2364709

[77] J. Tokarzewski. 2000. Zeros in discrete-time Mimo Lti systems and the output-zeroing problem. *International Journal of Applied Mathematics and Computer Science* 10, 3 (2000), 537–557.

[78] Harry L. Trentelman, Anton A. Stoorvogel, Malo Hautus, E. D. Sontag, and M. Thoma. 2001. *Control Theory for Linear Systems* (1st. ed.). Springer London, London, UK.

[79] Jurgen van Zundert and Tom Oomen. 2019. Beyond equidistant sampling for performance and cost: A loop-shaping approach applied to a motion system. *International Journal of Robust and Nonlinear Control* 29, 2 (2019), 408–432. DOI: https://doi.org/10.1002/rnc.4399

[80] Xiaofeng Wang and Michael D. Lemmon. 2010. Self-triggering under state-independent disturbances. *IEEE Transactions on Automatic Control* 55, 6 (Jun. 2010), 1494–1500. DOI: https://doi.org/10.1109/TAC.2010.2045697

[81] Bart Wolleswinkel, Riccardo Ferrari, and Manuel Mazo. 2024. A self-triggered control watermarking scheme for detecting replay attacks. In *Proceedings of the 2024 IEEE 63rd Conference on Decision and Control (CDC)*. IEEE, Milan, Lombardy, Italy, 4568–4573. DOI: https://doi.org/10.1109/CDC56724.2024.10886758

[82] Bart Wolleswinkel, Manuel Mazo, and Riccardo Ferrari. 2025. Zero dynamics attacks subject to actuator saturation: A constrained optimization approach. In *Proceedings of the 2025 IEEE 23rd European Control Conference (ECC)*. IEEE, Thessaloniki, Greece.

[83] Bart Wolleswinkel, Ivo Van Straalen, Luca Ballotta, Alexander J. Gallo, and Riccardo M. G. Ferrari. 2025. Periodic sparse control to prevent undetectable attacks on over-actuated systems. *IEEE Control Systems Letters*. DOI: https://doi.org/10.1109/LCSYS.2025.3581865

[84] Wenyuan Xu, Ke Ma, W. Trappe, and Yanyong Zhang. 2006. Jamming sensor networks: Attack and defense strategies. *IEEE Network* 20, 3 (May 2006), 41–47. DOI: https://doi.org/10.1109/MNET.2006.1637931

[85] Juan I. Yuz and Graham C. Goodwin. 2014. *Sampled-Data Models for Linear and Nonlinear Systems* (1st. ed.). Springer London, London, UK. DOI: https://doi.org/10.1007/978-1-4471-5562-1

[86] Cheng Zeng, Shan Liang, Yuzhe Zhang, Jiaqi Zhong, and Yingying Su. 2014. Improving the stability of discretization zeros with the Taylor method using a generalization of the fractional-order hold. *International Journal of Applied Mathematics and Computer Science* 24, 4 (2014), 745–757. DOI: 10.2478/amcs-2014-0055

[87] Cheng Zeng, Yingying Su, and Shan Liang. 2017. A sufficient and necessary condition for stabilization of zeros in discrete-time multirate sampled systems. *Automatic Control and Computer Sciences* 51, 1 (Jan. 2017), 42–49. DOI: https://doi.org/10.3103/S0146411617010084

[88] Xian-Ming Zhang, Qing-Long Han, Xiaohua Ge, Boda Ning, and Bao-Lin Zhang. 2023. Sampled-data control systems with non-uniform sampling: A survey of methods and trends. *Annual Reviews in Control* 55 (Jan. 2023), 70–91. DOI: https://doi.org/10.1016/j.arcontrol.2023.03.004

[89] K. J. Åström, P. Hagander, and J. Sternby. 1984. Zeros of sampled systems. *Automatica* 20, 1 (Jan. 1984), 31–38. DOI: https://doi.org/10.1016/0005-1098(84)90062-1

Received 15 September 2024; revised 25 April 2025; accepted 11 June 2025