Resilient Strategies Against Cyberattacks in Network Control Systems

by

Amin Nazarzadeh Oghaz

A thesis submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Control Systems

Department of Electrical and Computer Engineering

University of Alberta

Abstract

Large scale modern control systems involve the interconnection of system components using a communication network. The presence of a network can make these systems vulnerable to cyber attacks, thus compromising overall system's performance and stability. Cyber attacks in control systems has been a constant topic of research for over a decade, with concentration on three main issues; namely, attack detection, resiliency of the control system, and state estimation under cyber attacks. In this study, we address real-world challenges within this field and aim to enhance the current state of resiliency strategies in network control systems.

In the first part, we study input-to-state stability of nonlinear systems under DoS attack. More specifically, our goal is to obtain a relationship between ISS and DoS attack parameters. We propose a novel model-based dual-mode sampling approach which, depending on the attack intervals, intermittently switches between event-triggered and periodic sampling. We show that the combined model-based state prediction, packetized data transmission, and event-triggered sampling can attenuate the effects of DoS attack on stability.

In the next part of this research, our interest is in the study of one of the most critical forms of deception attacks, known as zero-dynamics attacks (ZDAs) in sampled-data systems. This type of attack excites the internal dynamics of the system resulting in unobservable, stealthy, deviation of the states when the internal system dynamics is non-minimum phase. In this part, our interest is in mitigating the effect of ZDAs in nonlinear sampled-data systems using the multi-rate approach. Our approach consists of analyzing the dissipativity property in the zero-dynamics part of the system and finding conditions on the sampling rate that neutralize the attack. We show that, under some

mild conditions, using a multi-rate approach provides a secure nonlinear system against ZDAs by preserving the minimum-phase property.

Then, we consider the practical limitation of the network control system and design a secure control framework that takes advantage of the asynchronous sampling in event-triggered schemes and embeds a sense of sampling zeros dynamics into the triggering threshold. Therefore, the triggering instants happen in such a way that stabilize the zero-dynamics of the sampled-data system. In this way, the event-based controller not only addresses the stability problem and network limitation but also provides a solution to the unstable sampling zeros issue. Thus, aside from all the aforementioned benefits, our proposed method also serves as a self-defence mechanism that confronts ZDAs whenever the system is targeted by an adversary.

Finally, we propose a new method that aims to compensate for the performance loss observed with the previous approach. We develop a model-based event-triggered control setup consisting of a novel triggering condition with an inference-based control rule using a nonlinear model. The key point is to exploit the concept of asynchronous (nonuniform) sampling inherent in the event-triggered mechanism as the main solution. We employ the multiple Lyapunov functional method and determine conditions on the switching signal that produce the desired result. Finally, we analyze the stability of the overall system using Lyapunov theory and discover conditions on the event-triggered parameters and inference-based control law that satisfy the stability criteria and render the zero-dynamics minimum-phase. As a result, ZDAs become ineffective and not a viable option to a malicious attacker.

Preface

Chapter 3 has been published in the article: A. Nazarzadeh, M. Ghodrat, and H. J. Marquez, "Stability Analysis for Model-Based Event-Triggered Nonlinear Control Systems under DoS Attacks", IEEE Transactions on Control of Network System in April, 2023. I was responsible for the main idea, analysis, design, mathematical derivations, simulation part and also the work drafting. Mohsen Ghodrat was involved with the paper composition and drafting. Dr. Marquez contributed to the main idea and also had the supervision role throughout the work. He was also involved with the paper composition and drafting.

Chapter 4 has been published in the article: A. Nazarzadeh and H. J. Marquez, "Secure Nonlinear Sampled-Data Control System Against Stealthy Attack: Multi-Rate Approach", IEEE Transactions on Automatic Control in March, 2023. I was responsible for the main idea, analysis, design, mathematical derivations, simulation part and also the work drafting. Dr. Marquez contributed to the main idea and also had the supervision role throughout the work. He was also involved with the paper composition and drafting.

Chapter 5 has been conditionally accepted for publication in the article: A. Nazarzadeh and H. J. Marquez, "Event-Based Self-Defence Strategy in Networked Control Systems Against ZDAs", IEEE Transactions on Control of Network Systems in November, 2023. I was responsible for the main idea, analysis, design, mathematical derivations, simulation part and also the work drafting. Dr. Marquez contributed to the main idea and also had the supervision role throughout the work. He was also involved with the paper composition and drafting.

Chapter 6 has been submitted for publication in the article: A. Nazarzadeh and H. J. Marquez, "On the Resiliency of Model-Based Event-Triggered Control Systems Against Stealthy Attacks", IEEE Transactions on Automatic Control on March, 2023. I was responsible for the main idea, analysis, design, mathematical derivations, simulation part and also the work drafting. Dr. Marquez contributed to the main idea and also had the supervision role throughout the work. He was also involved with the paper composition and drafting

To my beloved parents, supportive sister, loving wife
and the newest joy in our lives, Ariana

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my supervisor, Professor Horacio J. Marquez, for the guidance and support provided throughout my graduate education. His expertise in control theory and his willingness to assist have greatly contributed to the success of this research. Working with him has been a truly fortunate and enjoyable experience.

I extend my heartfelt appreciation to all the friends I made during my Ph.D. program, especially my dear friend Mohsen, who contributed to parts of this work and has always been there to help me in challenging situations. My sincere thanks go to my wife, Roya, for her unwavering love and encouragement.

Last but not least, I express my deepest gratitude to my parents and sister for their unconditional support and patience throughout this journey.

Amin Nazarzadeh Oghaz
Edmonton, Alberta
Canada

Notation

$\mathbb{R}, \mathbb{N}, \mathbb{Z}^+$	set of real, natural, and positive integers number
$\mathbb{N}^0$	set$\mathbb{N} \cup 0$.
$\mathbb{R}^n$	n-dimensional vectors with components in$\mathbb{R}$.
$x \in X$	$x$is an element of set X
$X \subset Y$	X is a subset of Y
$A^\top$	Transpose of matrix or vector A
A^{H}	Conjugate transpose of matrix A
A^{-1}	Inverse of matrix A
$\lambda_i(A)$	Eigenvalues of matrix $A$with $\lambda_1(A) \geq \ldots \geq \lambda_n(A)$ when all are real
I	Identity matrix of appropriate dimension
$\|x\|$	The Euclidean norm of a vector$x \in \mathbb{R}^n$
$\mathbb{R}_{>r}(\mathbb{R}_{\geq r})$	set of reals greater than (greater than or equal) to$r$.
$\alpha \in \text{class} - \mathcal{K}$	$\alpha : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$is strictly increasing and$\alpha(0)=0$
$\alpha \in \text{class} - \mathcal{K}_\infty$	$\alpha(s) \to \infty \text{as} s \to \infty$
$\alpha \in \text{class} - \mathcal{KL}$	$\alpha : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ for each fixed$t \geq 0, \zeta(., t)$belongs to class $- \mathcal{K}$ and for each fixed $s \geq 0, \zeta(s, t)$ decreases to zero as $t \to \infty$.
M=diag(V_i)	block matrix M includes square matrices V_i in the main diagonal and zeroes in the off-diagonal entries.
$\delta x_k = \frac{1}{T}(x_{k+1} - x_k)$	$\delta-$operator on discrete-time state x_k with sampling time T.

Abbreviations

FDI	False Data Injection
DoS	Denial of Service
ZDA	Zero-Dynamics Attack
ETM	Event-Triggered Mechanism
TC	Triggering Condition
ISS	Input-to-State Stability
ZOH	Zero-Order Hold
A/D	Analog to Digital
D/A	Digital to Analog
LTI	Linear Time-Invariant
LQR	linear Quadratic Regulator
LQG	Linear Quadratic Gaussian
LMI	Linear Matrix Inequality
PID	Proportional Integral Derivative
RHS	Right Hand Side
LHS	Left Hand Side

Contents

Abstract **ii**

Preface **iv**

Acknowledgements **vi**

Notation **vii**

Abbreviation **viii**

List of Figures **xii**

1 Introduction **1**

1.1 Background 1

1.2 Literature Survey 1

1.3 Research Motivation and Contributions 8

2 Mathematical Background **11**

2.1 Consistency of Discrete-Time Approximate Models 11

2.2 Zero-Dynamics 12

2.3 Zero-Dynamics Attacks 13

3 Model-Based Event-Triggered Control Against DoS Attacks **15**

3.1 Problem Statement 15

3.1.1 Event-Triggered Mechanism 17

3.1.2 Main Problem . . . 19
3.2 Preliminary Results . . . 19
3.2.1 Stability over $\theta_i^{(1)}$ . . . 21
3.3 Main Result . . . 24
3.3.1 Zeno Exclusion . . . 24
3.3.2 Stability Analysis . . . 24
3.4 Case Study . . . 30
3.5 Summary . . . 33

4 Multi-Rate Sampled-Data Control Against Zero-Dynamics Attack 35
4.1 Problem Statement . . . 35
4.1.1 Multi-Rate Sampling . . . 37
4.1.2 Main Problem . . . 37
4.2 Preliminary Results . . . 38
4.3 Main Results . . . 41
4.3.1 Lifting . . . 41
4.3.2 Zero-Dynamics of the Lifted System . . . 42
4.3.3 Stability of the Zero-Dynamics . . . 44
4.4 Case Study . . . 47
4.5 Summary . . . 50

5 Event-Triggered Control Against Zero-Dynamics Attacks 51
5.1 Problem Statement . . . 52
5.1.1 Event-Triggered Mechanism . . . 55
5.1.2 Main Problem . . . 55
5.2 Preliminary Results . . . 56
5.3 Main Results . . . 58
5.4 Case Study . . . 66
5.5 Summary . . . 69

6 Model-Based Event-Triggered Control Against ZDAs **70**

6.1 Problem Statement 70

6.1.1 Event-Based Inferential Control Setup 72

6.1.2 Sampling zeros dynamical system 73

6.1.3 Zero-Dynainter-samplemics Attacks 73

6.1.4 Main Problem 74

6.2 Preliminary Results 74

6.2.1 Event-Triggering Condition 77

6.3 Main Results 78

6.4 Case Study 83

6.5 Summary 89

7 Summary and Conclusion **90**

7.1 Directions for Future work 92

References **94**

List of Figures

3.1 Block diagram of the closed-loop control system under DoS attack 16

3.2 Diagram of data transmission time relationship under DoS attack. 19

3.3 (a): Nonlinear system state response under a DoS attack. (b): Inter-sampling time. . 31

3.4 (a): Nonlinear system state response under a periodic DoS attack. (b): Inter-sampling time. 33

4.1 Block diagram of the control system under ZDAs 36

4.2 Trajectories of the original (a) and normal form (b) states. 49

4.3 Trajectory of the normal form states (a) and details (b). 49

4.4 Trajectory of the dual-rate control system under ZDA. 50

5.1 Block diagram of the closed-loop control system equipped with an event-triggered mechanism under ZDAs 52

5.2 The shape of trajectories $\hat{\eta}$ and $\widetilde{\eta}$ at constant time t with respect to $\tau_k \in [t_k, t)$ for different values of θ. 62

5.3 A schematic of $\widetilde{\eta}$'s trajectory under two triggering conditions (5.34) 63

5.4 A schematic of $\widetilde{\eta}$'s trajectory under the proposed method 63

5.5 (a): States responses. (b): Trajectory of the sampling zero $\widetilde{\eta}$. (c): Events instants t_k under (5.6). 67

5.6 Trajectory of the states (a) and details (b). 68

5.7 (a): Trajectory of the sampling zero $\hat{\eta}$. (b): Events instants t_k under (5.39). 68

6.1 Block diagram of the closed-loop control system equipped with an event-triggered mechanism under ZDAs. 71

6.2 Schematic of single trailer articulated vehicle in (X, Y)-plane. 83
6.3 Time response of the states with fixed sampling time T. 85
6.4 Time response of the system under ETM (6.13) and without ZDA. 86
6.5 Time response of the system under ETM (6.13) and active ZDA. 87
6.6 Time response of the system under ETM (6.39) and without ZDA. 87
6.7 Time response of the system under ETM (6.39) and active ZDA. 88

Chapter 1

Introduction

1.1 Background

Large-scale modern control systems involve the interconnection of system components using a communication network and have been widely applied in large-scale fields due to their advantages in flexibility and mobility compared to traditional structures. The presence of a network, however, brings new challenges, such as security issues which can make these systems vulnerable to cyber attacks. Indeed, although standard transmission protocols enhance the modularity of network control systems, they also pose a weakness in terms of cybersecurity, providing potential access points for attackers and thus compromising the overall system performance and stability. Cyber attacks in control systems have been a constant topic of research for over a decade, with concentration on three main issues; namely, attack detection, resiliency of the control system, and state estimation under cyber attacks. See for example [1, 2, 3]. A review of numerous security incidents in critical systems over the past decade, such as nuclear power stations, railway networks, power electric grids, and water networks, emphasizes the importance of studying cybersecurity in control systems. Many countries have initiated efforts to enhance the security of industrial control systems, opening a new chapter in cybersecurity research, [4].

In networked control systems, cyber-attacks predominantly target the integrity and availability of data flow. The latter is known as a Denial of Service attack, which disrupts data flow through the network. The former is referred to as deception attacks, where malicious signals are injected into sensor-to-controller or controller-to-actuator channels, [1]. DoS attacks, however, are much easier to implement by a malicious agent and therefore occur much more often in networked control systems. DoS attacks are manifested as the interruption of data flow through the network and can be intentionally accomplished by an attacker by propagating a random jamming signal through the network. Therefore, DoS attacks do not require any sort of information about the

system structure and/or interconnections, [5]. In general, DoS attacks result in data packet losses. There are, however, some fundamental differences between packet dropouts induced by DoS attacks and those induced by the behaviour of an unreliable network. In fact, the latter is usually modelled as a random process whose characteristics can be extracted by examining the system, [6]. DoS attacks, on the other hand, are manipulated by the attacker, and therefore, predicting an attack scenario using typical process characteristics is, in general, not possible. Several models have been developed to address this issue, including the time-delay approach, the switched system approach, the game-theoretic approach, and probabilistic approaches using stochastic processes like Bernoulli or Markov processes. While these models are useful for specific problems, they lack comprehensiveness. A deterministic approach, limiting the duration and frequency of attacks, is more applicable when attackers have limited resources, [7]. Methods to address systems under DoS attacks fall into two categories: robust control and inferential control. While the former approach focuses on finding the maximum tolerable attack interval and keep preserving acceptable performance levels, the later tries to compensate for the control system, typically by using models to predict outputs during attacks. On the other hand, deception attacks act as exogenous inputs to components, compromising trustworthy information flow. Although the impact of attacks may resemble faults in control systems, technical differences exist. Simultaneous faults are assumed to be rare and lack intent, while attacks can be coordinated across multiple points with malicious intent, [8]. The complexity of deception attacks depends on the attacker's available resources, categorized as disclosure, disruption, and model knowledge. Different types of deception attacks can be constructed based on these resource levels, such as eavesdropping attacks, replay attacks, and ZDAs targeting internal dynamics, [9]. Among all type of deception attacks, the ZDA is the most critical forms of deception attacks. We focus on ZDAs because they can target the system while remaining stealthy, [5]. In non-minimum phase systems, these attacks stimulate internal dynamics without showing signs in the output, especially in sampled-data systems where additional non-minimum phase zero-dynamics are induced during the discretization process, [10]. Studies in this regard address three main problems: performance degradation, attack detection, and attack mitigation.

To combat the cyber attacks and implement defence strategies in network control systems, utilizing advanced control system theory is crucial. among them, the concept of multi-rate sampling and generalized hold functions approach has been attract the attention of researcher and recently has been used as the core of ideas in this field, enabling the mitigation of attack effects and ensuring the security of the system. Multirate systems come into play when signals in a system are sampled at different speeds. This happens when different parts of the system have different behaviours and limitations related to input and output channels. Indeed, the concept of multirate systems was first introduced in [11], and later these systems found practical applications in various areas such as estimating values, identifying and fixing faults in control systems, communication, and sensor networks, as well as digital signal processing, [12]. In the field of cybersecurity and

resilient control design, the multirate approach has been employed not only to compensate for the lack of reliable data during attacks but also to detect strictly stealthy attacks in feedback control systems. Another tools that have been a focal point of research in the past decade is event-triggered approach. This method is developed as an alternative for time-driven systems where a new control action occurs only when changes in the measured outputs exceed a predetermined threshold. These controllers stand out for their ability to deliver performance akin to traditional control methods while minimizing the need for continuous updates specially when there is limited source of energy and communication recourses. The primary benefit of event-based schemes in network control is that they can achieve a similar performance to time-triggered systems while reducing unnecessary transmission of information between components, thus alleviating network congestion. See for example [13] and the references therein.

1.2 Literature Survey

Providing a rather comprehensive model for DoS attacks has taken an important place in the literature during the last decade, dealing with how to formulate the attack in a way that is integrable with the control system equations. As a consequence, several methods have been emerged offering solutions for the aforementioned trend. In [14, 15, 16] a time-delay model is employed to describe a system subject to the DoS attack. Reference [17] studies the system both in the presence of attacks as well as in the absence of attack as an augmented system and provides a unified formulation using the dwell-time concept, the resting time between two switching instant, borrowed from the switched system theory. Reference [18] offers pulse-width-modulation (PWM) approach to deal with periodic attacks with unknown on/off intervals. Reference [19] considers a game-theoretic approach with the control system acting as a defender.

A number of references consider the attack as an exogenous signal with stochastic behaviour. Examples include [20] and [21], to mention a few, in which the attack signal is modelled as a Bernoulli and Markov process, respectively. Although this approach provides important contributions in the literature, they however suffer from the lack of reality due to the unpredictable attacker's plan. A rather general framework was introduced in reference [7] and employed in references [22, 23, 24, 25, 26, 27, 28]. In this model, DoS attacks are defined by imposing a limit on the total length and the number of attacks. This approach is sensible, for example, when the attacker has a limited source of power. Moreover, network control systems are usually equipped with data protection layers and most cyber-attacks are eventually detected and repelled, thus justifying the limit on the number of attacks.

Analysis and design of control systems under DoS attacks has been studied from two main perspectives, namely, robust control and model-based control [5]. In the robust control approach,

a robust controller is designed to tolerate the maximum possible length of consecutive data losses induced by a DoS attack. Reference [25] defines a new measure of robustness against DoS attack. This measure is used to design a maximally robust controllers. Reference [26] studies the robustness of a linear time-invariant system under DoS attacks when there is a bandwidth limitation and obtain sufficient conditions on the communication bit-rate that guarantee exponential stability. Reference [24] considers robustness of a class of nonlinear event-triggered control systems, using the framework of hybrid dynamical systems. In [29] a linear system under DoS attack is modelled as an aperiodic sampled-data system. A procedure is then provided to design a resilient state-feedback control according to the min and max interval of attacks.

In the model-based approach, the controller employs the plant model to generate a prediction of the plant's future output to be used during attack intervals. The controller then uses the predicted output to generate the actuator signal and hence stabilizes the system during attacks. Reference [20] follows this idea and proposes an optimal controller for linear systems under constraints on the state and input in an expected and probabilistic sense. Reference [27] proposes a model-based event-triggered sampling scheme where a predictor is designed to predict states in the interval between events, thus, saving communication resources and increasing the tolerable DoS attack intervals. Reference [22] employs a model-based observer and quantized output controller to obtained sufficient conditions on the DoS duration and frequency bounds for exponential convergence and Lyapunov stability. In [28] an LQG optimal controller is designed using the packetized model predictive approach for a system in the presence of DoS attack, in which a slack vector of predicted input is sent to the actuator at any sample time corresponding to the unreliable network induced by attacks.

While DoS attack can be summarized as an unpredictable communication loss, deception attack, however, is much more intelligent and can be propagated in a way that not only the attack remains stealthy but also targets the trustable information flow in the control system loop. Studies on control systems subject to deception attacks can be categorized according to the attack's different forms and types. Indeed, the level of defence strategy's complexity relies on the level of model knowledge, disruption, and disclosure resources on the attacker's side, [30]. In this regard, Examples include replay attack, false data injection attack, eavesdropping attack, and ZDA. In particular, [31] seeks asymptotical stability of the attacked system using a robust dynamic compensator. In this approach, an unknown dynamical system with finite L_2-gain is considered as a rather general attack's model and a robust dynamic compensation scheme, driven by two virtual dynamical systems, is proposed corresponding to the insecure situation. In [32] the replay attack is considered in which the feedback signal is infected by an imposed shifted output coming from the attacker and resulting an artificial sense of time delay in the control loop. The attack is then revealed using rewriting Kalman filter estimation from fixed gain to stochastic. In [33] a form of deception attack so-called false data injection is modelled as a Bernoulli process. Then, by using

recursive linear matrix inequalities, a time-varying controller gain is obtained to deal with any abnormally induced by the attacker.

Besides the mentioned topics, attack detection and identification is another trend in this field. In this regard, reference [34] investigates the problem of false data injection using tools from controlled invariant sets. The method is then formulated based on reachability problems to find a set of admissible control sequences such that the current state is reachable, otherwise, an attack has occurred. In [35] an energy-based solution is offered to monitor the system and provide a detectability property in such a way that any unbalance effect on the amount of system's energy is counted as a sign of attack. Reference [36] provides a new approach based on side initial state information for integrity attack detection. Indeed, the initial state firstly is derived from the system's physical description and then employed to evaluate the reachability of the measured output in a bounded time interval and reveal the presence of an attack. Reference [37] presents a watermarking setup as a detecting method for the replay attack. In this manner, an unobservable artificial signal is injected into the system. This signal has no impact on the system performance, but causes the detectable residual if the attack is activated in the control loop.

The critical impact of cyber-attacks in control systems has lead researchers to investigate a systematic approach to deal with different attacker's scenarios. Beginning with [38], some structural properties of attacks including stealthiness, detectability, and identifiability were taken into account in the analysis and design of resilient control systems. Following that, several works have studied the stealthiness property of deception attacks and developed methods to generate strictly undetectable attacks. In the study presented in [39], the problem of designing a stealthy false data injection attack was explored in a switched system. This type of attack is usually not stealthy and can be detected by a χ^2-detector. However, in this paper, a strictly stealthy FDI attack was designed using a joint attack strategy, targeting both sensors and the switching signal. Reference [40] developed a process for generating stealthy false data injection attacks based on controlled invariant subspaces and geometric control theory. The stealthiness of the attack was evaluated using the incremental stability of the control system and the incremental input-to-state stability of the detector. Finally, a sufficient condition was obtained based on the initial condition of the attack model to preserve its stealthiness. In [41], the problem of generating stealthy attacks with limited resources was investigated. To maximally degrade the estimation performance of the control system, a partially multi-sensor false data injection attack was proposed. The selection of targeted sensors was formulated as a constrained optimization problem. In [42], a new local stealthy covert attack was proposed by combining covert attacks and ZDAs. In this method, access to all control inputs is not necessary to keep the attack stealthy. The proposed approach demonstrated that the attack could remain stealthy even if it partially targeted sensors and actuators, but only if the mismatch between the actual plant and its model was small enough to be negligible.

The problem of designing stealthy attacks involves the cost of accessing the critical resources of the plant. Indeed, attackers not only need model knowledge but also require disclosure and disruption resources to successfully remain stealthy. As a consequence, multiple studies have turned their attention to the so-called ZDA, which has the property of remaining stealthy under certain conditions for non-minimum phase systems, without the attacker needing any feedback from disclosure resources. ZDA stimulates the internal dynamic of the system resulting in unobservable deviation, making any non-minimum phase mode of the system unbounded over time [43]. Research in this area has mainly focussed on three problems. The first approach focus on studying the effect of the ZDA on performance degradation. In this regard, the problem is formulated using reachability analysis to approximate the maximum reachable set in which the attacker may deviate states. Reference [44] considers a stochastic control system equipped with χ^2 detector. The so-called reachable set in which the stealthy attack can compromise the states is then predicted using an ellipsoidal approximation method. In [45] two security metrics are proposed based on geometric's properties of the reachable set. Reachability analysis is then formulated by using LMI techniques for a linear system equipped with a general dynamic output controller, resulting in an optimum controller in a way that the reachable set getting shrunk as much as possible. Reference [46] addressed the problem of risk assessment for stealthy attacks in systems with a level of uncertainty. It introduced a new metric known as output-to-output gain and derived necessary and sufficient conditions for the risk to be bounded. The problem was formulated as an infinite non-convex optimization problem, approximated as a sampled non-convex optimization problem, and finally transformed into an equivalent convex semi-definite program using the concepts of dissipativity and s-procedure. In the second approach, the main objective is to detect the attack. This approach typically assumes that the control system is equipped with an abnormal detector, such as a χ^2 detector. Such a strategy can be seen in [47, 48] and [49]. In [47] a new idea called the moving target approach is considered against stealthy attack, including changes in the system's parameters, adding an authenticating dynamics, and employing nonlinear sensors, all in a time-varying fashion. As a consequence, the attacker cannot follow the system model which results in revealing the stealthy attack by the detector. Reference [48] explores the impact of changes of a linear system's parameters, more precisely, regarding the number of measurements, presence of perturbation, and effect of actuators gain on the attack detection and made a connection between stealthiness property of attacks and geometric control characterization of the system's zero-dynamic. Reference [49] firstly provides a systematic approach to determine whether or not a stealthy attack can occur in a control system. Then, if there is a vulnerable spot, the minimum number of protected redundant measurements, which is needed to avoid stealthy attacks, is counted as a solution to have a secure system. In [50], the existence condition of a kernel attack, which is the superset of all stealthy attacks, was provided. It was proven that the kernel attack is detectable if both the observer-based residual and the control input-based residual are available. Two different schemes were provided for stealthy attack

detection based on the moving target approach and the encrypted transmission approach in the feedback control system. The ultimate goal was to limit the attacker's knowledge of the system model. The third approach's consists of modifying the control law in such a way that the ZDA becomes neutral whenever propagated in the control system. In this approach, the ZDA is considered as an unavoidable exogenous input and the main goal is to firstly identify and then re-construct the vulnerable spots in a control system such that the attack is no more taken into account as a threat. In [51] the stability degradation under ZDA in sampled-data systems is investigated in which induced sampling zeros appears according to the sample and hold process. A generalized hold function as an alternative of zero-order-hold is then proposed to neutralize the attack. Reference [52] introduces a multi-rate sampling and uses the property that multi-rate sampling permits removing certain non-minimum phase zeros in a linear system. Some conditions are then obtained using a multi-rate setup to construct a secured control system subject to ZDA.

As it is shown in [51] and [52] the problem of ZDA is much more critical in sampled-data systems because of the sampling and hold process. Indeed, the discretization process adds a new zero-dynamics to the system, known as *sampling zeros*, which have no counterpart in the original continuous-time system, and surprisingly the newly induced zero-dynamics is non-minimum phase if the relative degree is more than two in a system with a fast sampling rate, [10, 53]. Using the multi-rate strategy proposed in [52] is a novel way to neutralize the ZDA in sampled-data systems. Compared to other methods such as [47, 51] modifying the software part instead of the hardware of the control system, is the main benefit of this method.

The basic idea of the multi-rate approach is to predict fast rate states between any two slow rate actual ones using a discrete-time model of the continuous-time system, and feed the actuator with a combination of predicted and actual data in the faster rate fashion. As a consequence, the sampling and hold components are managed with different sampling times, making it possible to relocate sampling zeros induced by the discretization. Multi rate sampled-data system has been an active area of research, starting with earlier work of Kranc [15], with multiple applications, including estimation and control, fault detection and isolation, communications and sensor networks, and digital signal processing. Extensive research on the development and analysis of linear multi-rate control systems has been carried out (see for example [1, 34, 35] and the references therein). For instance, Longhi [36] analyzes some structural properties such as reachability, controllability, and stabilizability of linear multi-rate sampled-data plants. Linear multi-rate controllers for a given multi-rate sampled-data system are parameterized in [37]. After earlier works developed by Chen and Qiu [34] on multi-rate H_2/H_∞ control, many researchers try to solve this problem using various methodologies, [35] and [38]. Performance comparison of the linear single-rate and multi-rate sampled-data systems was accomplished in [33]. In a nonlinear system, however, using the multi-rate setup is much more challenging than the linear case and has received comparatively much less attention. This is mainly due to the lack of a general theory for the multi-rate design

of nonlinear plants and intrinsic complexity accompanied with nonlinear equations which make the problem non-trivial. In particular, multi-rate nonlinear control systems has been studied by [54, 55, 56, 57, 58, 59, 60, 61] when the output is measured at a slow rate compared to the control input. More explicitly, [54] formulates the basic idea of multi-rate approach in nonlinear systems, and investigates the existence of fast sampling for practical asymptotic stability of time-delay system based on an approximate model in a disturbance-free environment. In [55] and [56] the multi-rate idea is extended for input to state stability of nonlinear systems subject to a disturbance in continuous-time and discrete-time design, respectively. In [57] dissipativity of multi-rate control systems is studied using emulation method with emphasis on designing L_2 gain nonlinear controllers for multi-rate sampled-data systems. The aforementioned work considers the full-information case where all state-variables are available for feedback, to overcome this difficulty, In [58] multi-rate output feedback control for nonlinear systems is proposed and [59] provides a more general result when network induced constraints are taken into account as norm-bounded uncertainties. Reference [60] employs a discrete-time high-gain observer and proposes a multi-rate observer-based controller for a class of nonlinear systems where, unlike the previous works, the measurement sampling rate is faster than the control update rate. To deal with uncertainties in the sampling times, [61] studies observer design in a multi-rate nonlinear system according to perturbations in the sampling schedule, which is a more realistic situation compared to the previous works.

One important aspect in the study of networked control systems under cyber attacks is the implementation of the results using the event-triggered framework. The benefits of this approach stem from the flexibility offered by the event-based scheme when deciding when to transfer information between system components. Rather than enforcing a fixed sampling rate, the event-based approach enables the use of low data transfers during active attack intervals, and higher rates after the attack. The idea of event-triggered sampling firstly began with the work reported in [62], which considers a first-order stochastic system and shows that event-triggered sampling dominates the regular time-triggered control with respect to closed-loop variance and sampling rate. Following this work, stability analysis and performance evaluation of control systems equipped with event-triggered sampling became a constant topic of research. Reference [63], presents a clever and rather general solution to the stability problem of event-triggered systems. In this reference, the author assumes the existence of a pre-designed continuous-time control law that results in the input-to-state stability of a nonlinear plant. Reference [63] has inspired much work and several event-based strategies have been proposed that extend this work (see [64] and the references therein). Following novelties in this field, the application of event-triggered sampling in control systems under cyber-attacks has seen much attention from the research community in recent years. To mention but a few, reference [7] as a pioneer work in DoS attack, studies the implementation of event-triggered and self-triggered sampling in a linear system in the presence of attacks. Reference [23] analyzes the nonlinear control system which is equipped with event-triggered setup, proposed in [63], sub-

ject to DoS attacks. In [24] a nonlinear output-based event-triggered system under the DoS attack is formulated using a hybrid model, and conditions to have stability and performance criteria in terms of induced L_∞-gain is then extracted. Reference [26] focuses on bandwidth limitation as a practical constraint in a networked control system targeted by DoS attacks, and employs the event-triggered approach as a key idea to cope with this problem. In [27] the aperiodic property of event-triggered sampling is taken into account as a defence strategy against periodic DoS attacks on the sensor-to-controller network channel. The aforementioned result is then firstly extended by [65] to a system under asynchronous attacks on both sides of the communication network (sensor-to controller and controller-to-actuator channels) using static triggering conditions. Afterward, [66] contributes earlier mentioned toward dynamic triggering conditions. Reference [66] encapsulates an event-triggered system under periodic DoS using switching manner in a time-varying delay fashion to study exponential stability of the resulting switched system. In [33] a state-dependent event-triggered strategy together with a time-varying controller gain law are offered for a multi-agent system to overcome the cyber threat generated by false data injection attack besides the presence of disturbance and time-varying uncertainties. Reference [67] offered a resilient event-triggered control for a system in the presence of stochastic deception attack modelled as a Bernoulli process. Output controller law and the event-triggering threshold are then co-designed using LMIs based solution in a way that asymptotic stability is obtained. Reference [68] presented sufficient conditions according to input-to-state stability for a dynamic event-triggered PID-based control system subject to deception attack. Reference [69] employed an event-triggered mechanism as a tool for designing a covert attack that could target the system. Then, a defence strategy based on a self-triggered approach was provided to combat the proposed attack in which it utilized pseudo-random numbers unknown to the attacker. Reference [70] proposed a dynamic event-triggered H-infinity filtering method to ensure stability and H-infinity performance for a system under both DoS attacks and deception attacks. Although effective, the approach was deemed conservative and in need of further improvement, especially concerning common integral inequalities. In[71], a new approach based on a dynamic event-triggered scheme was introduced to identify secure time intervals for a system under stealthy attacks. To guarantee l^2 performance, the system was modelled as a linear parameter-varying system. Observers and event-triggered mechanisms were designed simultaneously to ensure input-to-state stability for the overall system where The system, under a stealthy attack, was also affected by process disturbances, measurement noise, and nonlinearities. In [72], a novel approach based on event-triggered sampling was designed to bypass attacks and secure the system under sparse FDI attacks. The main idea was to reconstruct the state from an approximate model of the nonlinear system initiated by event-triggered samples, instead of using periodically sampled data. This method increased the chances of exact estimation and decreased the negative influence of attacks on control decisions. The estimations were utilized to implement output-tracking control using the back-stepping method. Reference [73] addressed the problem of

performance degradation for a system under DoS attacks. It proposed a co-design approach for output-feedback control gains and event-triggered parameters using bilinear matrix inequalities, which were solved by a successive convex optimization approach. The results provided a trade-off between control performance and communication cost, while maintaining the system's exponential stability under attacks. In [74], a resilient control approach was proposed for a self-triggered system under false data injection attacks, based on control signal reconstruction. The idea was to keep the event interval as long as possible and send the critical control input in a protected way to the actuator side. This approach allowed the continuous control signal to be reconstructed using a first-order hold mechanism.

1.3 Research Motivation and Contributions

In this section, we delve into the driving forces behind our research and provide an overview of the key contributions presented in this thesis. While we discussed different aspects of cybersecurity in control systems in the previous section, there are still important unresolved problems that need careful attention, despite the progress made in recent years.

In chapter 3, our interest is in the study of the stability of nonlinear systems under DoS attack. More specifically, our goal is to obtain a relationship between asymptotic stability and DoS attack parameters. Introducing a novel event-triggering strategy for sensor measurements and control, we modify the model-based framework [75, 76, 77]. Our approach includes unique triggering rules with adjusted thresholds and error equations, distinguishing it from previous methods. While discrete-time models of nonlinear systems often lack closed-form solutions, our formulation aligns with sampled-data nonlinear control theory [78, 79]. We show that the triggering rule, designed using an approximate model, is effective for the true system under mild conditions. We also propose an innovative inference-based control method to address sensor data loss during DoS attacks, filling a gap in existing research on nonlinear systems [23, 24, 7, 80, 81]. By predicting future states using plant models, our approach compensates for missing sensor data. While inference-based methods are not new, this application to mitigate DoS attack effects on closed-loop stability is novel. We also implement a buffer system for efficient data transmission, drawing on techniques from [82, 83, 84]. Finally, We integrate a model-based controller and event-triggered sampling to optimize network traffic during data transmission, distinguishing our work from previous methods [23, 24, 7, 27]. Unlike prior studies, we relax constraints on attack synchronicity, channel targeting, and packet dropout assumptions, enhancing the flexibility and robustness of our approach.

In chapter 4 we turn our attention to another critical attacks in network control system known as ZDA. As shown in [51], [52], the problem of ZDAs is much more critical in sampled-data systems because of the sampling and hold process. In fact, discretization adds new zero-dynamics

to the system, known as *sampling zeros*, which have no counterpart in the original continuous-time system. Unfortunately, the newly induced zero-dynamics is non-minimum phase whenever the relative degree is more than two in a system with a fast sampling rate, [10, 53]. Although using the multi-rate strategy proposed in [52] is a novel way to neutralize the ZDAs in linear systems, nonlinear systems present a challenge due to the lack of exact discrete-time models. In this chapter, our interest is in mitigating the effect of ZDAs in nonlinear sampled-data systems using the multi-rate approach. We firstly study the effect of ZDAs on the stability of nonlinear systems using the concept of dissipativity. To the best of the authors' knowledge, this is the first study of nonlinear sampled-data systems under stealthy attacks. Previous works in [51, 52, 48] consider LTI systems. Recent work in [47] adds an artificial time-varying nonlinearity in the sensor part to limit the information available to an attacker, assuming that the closed-loop system remains stable. We extend the idea of using multi-rate sampling as a defence strategy against ZDAs initiated in [52] for linear systems, to the nonlinear case. Our framework is novel and constitutes the first attempt to implement the multi-rate approach in ZDAs in nonlinear control. Inspired in the nonlinear sampled-data theory initiated by [78] and [79], as well as [54, 59, 57] in the multi-rate case, our approach consists of using approximate models and provides a model-based solution that is applicable to nonlinear systems under ZDAs. Finally, using the concept of lifting, [85, 86], we formulate our solution in the lifted-domain and analyze the dissipativity property of the internal dynamics of a multi-rate nonlinear sampled-data system.

In chapter 5 our interest is in mitigating the effect of ZDAs by employing the event-triggered sampling schedule in a nonlinear system. The multi-rate sampling solution provided by [52], [51], and what we have proposed in chapter 4, although effective, requires significant communication resources that may be prohibitive in networked control with limited energy resources, limited bandwidth, or both. Therefore, in this chapter we focus on nonlinear systems and consider an entirely different approach, based on the use of event-triggering sampling. In this approach, the event-triggering mechanism produces asynchronous (*i..e* nonuniform) sampling and inter-sample times and can be designed to ensure that the system's zero-dynamics of the feedback system is minimum-phase, thus eliminating the possible existence of a harmful ZDA. Our approach is inspired by the theory of switched systems and the average dwell time introduced in [87], as well as the geometric approach in [53]. In this work we address practical limitations in networked control systems and propose a new event-triggered formalism in which the triggering decision depends not only on the plant output but also on the deviation of extrinsic zero-dynamics. The event-triggered approach was introduced and is primarily used to limit the transfer of information between system components to what is necessary, thus reducing network congestion in bandwidth-limited systems. See for example [13] and the references therein. Our proposed triggering method is cast in the dynamic event-based framework [88] and we utilize it as a secure solution to counteract ZDAs and ensure system resilience. The adjustable interval time between events serves as a key parameter

that effectively safeguards against these attacks. Moreover, as in the classical event-triggering approach, our scheme also reduces unnecessary communication demands when compared to traditional triggering conditions such as [63] under ZDAs. This feature becomes vital when a hybrid attack (for example, a combination of a ZDA and a denial of service attack) targets the system, forcing open loop operation for relatively long periods of time.

In chapter 6 we propose a new method that aims to compensate for the performance loss observed with the previous approach. The event-triggered method in chapter 5 has been shown to be effective in neutralizing the ZDA. Indeed, the core idea in is to increase the average inter-event time as much as possible to ensure boundedness of the extrinsic zero-dynamics while preserving the stability of the overall system. However, using this method comes at the cost of some performance degradation due to the relatively long time interval between events. To address this issue, we develop a model-based event-triggered control setup consisting of a novel triggering condition with an inference-based control rule using a nonlinear model. The proposed setup is non-trivial since it requires the use a model to generate predicted states and input signals for nonlinear differential equations that, in general, do not have a closed-form solution. As a result, we employ an approximate nonlinear model, which adds to the complexity of the solution due to model uncertainty. Our formulation draws on the theory of sampled-data nonlinear control introduced in [78, 79]. Notice that the majority of literature on resilience control under cyber attacks is limited to linear systems, and comparatively less attention has been given to the nonlinear case. Moreover, our proposed triggering scheme utilizes the model-based framework [75, 76] but incorporates changes, including the introduction of a new error equation and a new threshold criterion based on the stability of the zero-dynamics. This new structure differentiates our approach from the methods presented in references [75, 89] and chapter 5. We point out that in our previous chapter, our design achieves boundedness of the extrinsic zero-dynamics, thus limiting the impact of ZDAs. However, in this work, our solution is much for effective, achieving exponential stability for the extrinsic zero-dynamics, making the system immune to the effects of ZDAs. The solution presented here also removes the problems associated with extended inter-event sampling times encountered in the previous chapter. Moreover, the design procedure for the event-triggering condition in this work is entirely different, making it a unique and novel approach.

Chapter 2

Mathematical Background

In this section, essential technical terms and foundational concepts are introduced, forming the basis for the subsequent chapters of the thesis.

Consider the following system:

$$\dot{x}(t) = f(x(t)) + g(x(t))u(t), \quad y(t) = h(x(t)), \tag{2.1}$$

where $x \in \mathbb{R}^n$, $u, y \in \mathbb{R}$, and f, g, h are locally Lipschitz function, *i.e.*, $\exists\ \lambda_f$ such that for any x and $\widetilde{x}$ in a compact set X, $|f(x,u) - f(\widetilde{x},u)| \leq \lambda_f |(x - \widetilde{x})|$.

Assume now that the system (2.1) is controlled by

$$\dot{v}(t) = s(y(t), v(t)), \quad u^c(t) = U(y(t), v(t)),$$

where $v \in R^r$ is the state of the controller and s, U are continuous, locally Lipschitz functions and zero at zero.

Definition 2.1 ([57])**.** *The continuous-time system* (2.1) *with control input* $u(t)$ *is said to be differential dissipative with respect to the continuous supply rate* ω *if there exists a continuously differentiable storage function* $V(x, v)$ *such that for all* $x \in \mathbb{R}^n$, $u \in \mathbb{R}$

$$\dot{V}(t) = \frac{\partial V}{\partial x}\left(f(x) + g(x)u\right) + \frac{\partial V}{\partial v} s(y, v) \leq \omega(u, y). \tag{2.2}$$

2.1 Consistency of Discrete-Time Approximate Models

Definition 2.2 ([55])**.** *Approximate model* $F^a_{T,h}$ *is said to be one-step consistent with the exact model* F^e_T *if for any compact set* X *there exists a function* $\rho \in K_\infty$ *and sampling time* $T^* > 0$ *where*

for any $0<T\leq T^*$ there exist $h^*>0$ such that for all $0<h<h^*$ and $x\in X$, the following is satisfied:

$$|F_T^e(x,u_T)-F_{T,h}^a(x,u_T)|\leq T\rho(h). \tag{2.3}$$

Inequality (2.3) guarantees that the error between solutions initiated with the same initial condition is small over one integration (sampling) step, relative to the step size. This definition has its origins in the numerical analysis literature, and has been extensively used in the theory of nonlinear sampled-data systems. See references [78, 79, 55].

Sufficient conditions for one-step consistency were obtained in [78, Lemma 1], and can be stated as follows. If $F_{T,h}^a$ is one step consistent with the Euler approximation, and $F_{T,h}^a$ is locally Lipschitz uniformly in u_T, *i.e.*, for any x and $\widetilde{x}$ in a compact set X, $|F_{T,h}^a(x,u_T)-F_{T,h}^a(\widetilde{x},u_T)|\leq\lambda_F|x-\widetilde{x}|$ where λ_F is Lipschitz constant. then $F_{T,h}^a$ is one-step consistent with F_T^e.

Definition 2.3 ([78, 59])**.** *$F_{T,h}^a$ is said to be multi-step consistent with F_T^e if given $L,\hat{\eta}\in\mathbb{R}_{>0}$, for any compact set X there exist T^* and a class-$\mathcal{KL}$ function α such that for each $0<T\leq T^*$ we can find h^* such that for $x,z\in X$ if $|x-z|\leq\delta$, where $\delta>0$, then $|F_T^e(x,u_T(x))-F_{T,h}^a(z,u_T(z))|\leq\alpha(\delta,T)$ for all $0<h\leq h^*$. Moreover, for $k\leq\frac{L}{T}$ we have $\alpha^k(0,T):=\underbrace{\alpha(\cdots\alpha(\alpha}_{k}(0,T),T)\cdots,T)\leq\hat{\eta}$.*

2.2 Zero-Dynamics

Definition 2.4. *Consider the system of the form 2.1 with relative degree r. Define the following transformation:*

$$\begin{aligned} z_k &= H_{nf}(x_k):=[\xi_k|\eta_k]^\intercal \\ &= [\phi_1(x_k),\cdots,\phi_r(x_k)|\phi_{r+1}(x_k),\cdots,\phi_n(x_k)]^\intercal, \end{aligned}$$

where $x=\phi^{-1}(z)$ and $\phi(.)=[\phi_1(.),\cdots,\phi_n(.)]$ such that $\phi_1=h(x),\phi_2=L_fh(x),...,\phi_r=L_f^{r-1}h(x)$ and $\Theta:=[\phi_{r+1},...,\phi_n]^\intercal$ is chosen in a way that $H_{nf}(x)$ is a diffeomorphism on a compact set X. Moreover, for any $x\in X$, $L_g\phi_i(x)=0$, $i=r+1,...,n$, where $L_fh(x)$ is the Lie derivative of $h(x)$ over the vector field $f(x)$, i.e., $L_fh(x)=\frac{\partial h(x)}{\partial x}f(x)$.

H_{nf} is called the normal form transformation and transfers the original system (4.3) into the following form, constructed using Taylor's formula with remainder, [53]:

$$F_T^g:\{\ \delta z_k=\hat{S}_T(z_k)+\hat{B}_T(\beta_{z_k}+\alpha_{z_k}u_k),\quad y_k=z_k^1\}, \tag{2.4}$$

$$\hat{S}_T(z_k)=\begin{bmatrix} S_T & 0 \\ 0 & 0 \end{bmatrix} z_k+\begin{bmatrix} 0 \\ \psi(z_k) \end{bmatrix}, \hat{B}_T=\begin{bmatrix} B_T \\ 0 \end{bmatrix}$$

$$S_T=\begin{bmatrix} 0 & 1 & \frac{T}{2} & \cdots & \frac{T^{r-2}}{(r-1)!} \\ 0 & 0 & 1 & \cdots & \frac{T^{r-3}}{(r-2)!} \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix}, B_T=\begin{bmatrix} \frac{T^{r-1}}{r!} \\ \frac{T^{r-2}}{(r-1)!} \\ \vdots \\ \frac{T}{2} \\ 1 \end{bmatrix}$$

$$\beta_{z_k}=L_f^r h(x)_{|x=x_k}, \quad \alpha_{z_k}=L_g L_f^{r-1} h(x)_{|x=x_k}$$

$$\psi_{z_k}=L_f \Theta(x)_{|x=x_k}=[L_f\phi_{r+1}(x_k), \cdots, L_f\phi_n(x_k)]^\top.$$

Assumption 2.1. *The function $\Theta=[\phi_{r+1}, ..., \phi_n]^\intercal$ is chosen such that it is continuously differentiable at every $x\in X$.*

The zero-dynamics of the system (2.1) is defined as the internal dynamics when the input and initial conditions are chosen such that y_k is zero for all k, [90, 53]. The aforementioned dynamics are given by the following two subsystems

$$\delta\eta_k = \psi(0, \hat{\xi}_k^{2:r}, \eta_k) \tag{2.5}$$

$$\delta\hat{\xi}_k^{2:r} = Q_{22}\hat{\xi}_k^{2:r}, \tag{2.6}$$

where $\hat{\xi}=\hat{H}\xi$, $\hat{H}=\left[\begin{array}{c|c} 1 & 0 \\ \hline H_{21} & I_{r-1} \end{array}\right]$, $H_{21}=-\left[\frac{r}{T}, \cdots, \frac{r!}{T^{r-1}}\right]^\intercal$, $\hat{\xi}_k^{2:r}:=[\hat{\xi}_k^2, ..., \hat{\xi}_k^r]$ and $Q=\hat{H}S_T=\left[\begin{array}{c|c} Q_{11} & Q_{12} \\ \hline Q_{21} & Q_{22} \end{array}\right]$.

The subsystem (2.5) is the sampled counterpart of the continuous-time zero dynamics known as the intrinsic part, and (2.6) is a linear subsystem so-called extrinsic zero-dynamics.

2.3 Zero-Dynamics Attacks

Consider the system (2.1) and suppose $u = u_c + u_a$. The following provides the definition of the ZDA.

Definition 2.5 ([30])**.** *The exogenous input u_a is a stealthy ZDA if it causes undamped internal oscillations that are not detectable at the output when injected into a non-minimum phase system. This results in $y = 0$ for the closed-loop system* (2.1)*, despite internal dynamics divergence.*

The following example demonstrates the malicious effect of ZDAs in a sampled-data system, using a constant sampling rate. Consider a system with $r\geq 2$ sampled using a small and constant sampling period h, *i.e.* $h\to 0$. Since the system's relative degree is $r\geq 2$, the use of a fast sampling

rate invariably results in non-minimum phase sampling zeros. Thus, the attacker utilizes the unstable Q_{22} in (2.6) to generate $u_a(ih)$, $i\in\mathbb{N}$, as follows.

$$\delta z_a(ih) = Qz_a(ih), \quad u_a(ih) = f_a(\beta_1, \beta_2, \phi, z_a(ih)), \tag{2.7}$$

where f_a is a well-designed function such that the attack remains stealthy. The following normal form realization shows the effect of the attack on the internal dynamics:

$$\begin{aligned}
\delta\xi_1(ih)&=Q_1\xi_1(ih) + Q_2e_a(ih)+(\beta_1+\beta_2u_c(ih)) \\
\delta e_a(ih)&=Q_3\xi_1(ih)+Qe_a(ih), \\
\eta(ih)&=\phi(\xi_1(ih), e_a(ih), \eta(ih)) \\
y(ih)&=\xi_1(ih),
\end{aligned} \tag{2.8}$$

where e_a=ξ_r-z_a, ξ_r is the internal dynamics, β_1,β_2,ϕ are some appropriate functions in the normal form realization, u_c is a stabilizer controller, and Q_1, Q_2, Q_3 are matrices of suitable dimensions. With respect to (2.8), while ξ_1 and e_a converge to zero, the internal states ξ_r follow the attack's unbounded state z_a. Indeed, under the attack, unstable sampling zeros cause unstable internal dynamics which is not traceable at the output.

Chapter 3

Model-Based Event-Triggered Control Against DoS Attacks

In this chapter, we study the stability of a novel nonlinear event-triggered control system under denial-of-service attacks based on an ISS-Lyapunov function analysis. A new dual-mode model-based event-triggering strategy is proposed which works based on consistency between the approximate and exact discretization of the nonlinear plant. We combine an event-triggered module with a controller based on the state prediction, together with a packetized transmission at the controller-to-actuator channel to provide the desired stability properties under DoS attacks. We also provide proof of Zeno-free behaviour for the event-based system. Our proposed method provides a maximum percentage of time that the system can tolerate attacks without performance degradation. Finally, a numerical example is used to illustrate the effectiveness of the proposed approach.

The rest of the chapter is organized as follows: In Section 3.1, the main problem is discussed and the new model-based event-triggering strategy is presented. Section 3.2 formulates the effect of DoS attack on the system, and also provides preliminary lemmas used later in the main section. Later, in Section 3.3, the asymptotic stability of the system under the DoS attack is investigated. Finally, in Section 3.4 a numerical example is proposed to show the effectiveness of our proposed method and provide a comparison with respect to related literature.

3.1 Problem Statement

Fig. 3.1 shows a schematic of the feedback system to be used throughout the chapter. The system output is connected to the computer control via a network. Information is transferred through the network as determined by an event-triggered rule connected to the sensors. The controller output is transferred to the actuators through a network via digital-to-analog (D/A) converters. We assume

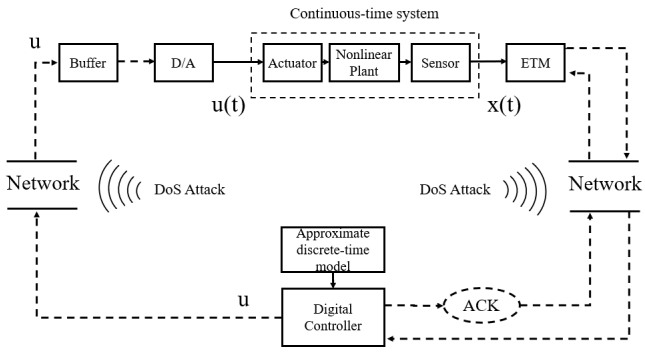

Figure 3.1: Block diagram of the closed-loop control system under DoS attack

that the plant is described by the following nonlinear model:

$$\dot{x}(t)=f(x,u) \tag{3.1}$$

where f is assumed to be locally Lipschitz, *i.e.*, for any x and $\widetilde{x}$ in a compact set X, $|f(x,u)-f(\widetilde{x},\widetilde{u})| \leq \lambda_f|(x-\widetilde{x},u-\widetilde{u})|$ where λ_f is Lipschitz constant. The control u is implemented in an event-based fashion, [63]. The transmission of information between sensors and controller takes place only at the triggering instants $\{t_n\}, n\in\mathbb{N}$, prompted by a triggering event. When a triggering event occurs at t_n, $x(t_n)$ is transmitted through the network and received by the controller. The controller uses a discrete-time approximation $F^a_{T,h}$ of the plant model (3.1) to compute the following prediction of the actual state x:

$$x^a(t_n+kT)= \begin{cases} x(t_n), & k=0 \\ F^a_{T,h}(x^a(t_n+(k-1)T), u^a(t_n+(k-1)T)), & k\in\mathbb{N} \end{cases} \tag{3.2}$$

where $F^a_{T,h}$ is a family of discrete-time approximate models of (3.1) corresponding to the sampling time T and parametrized by the modelling parameter h, and $u^a(t_n+kT)=\psi(x^a(t_n+kT))$, $n\in\mathbb{N}\cup\{0\}$, for some Lipschitz function ψ. Neglecting computational delays, at time t_i the controller sends the following stack vector of length $N+1$ to the buffer

$$(u^a(t_n), u^a(t_n+T), ..., u^a(t_n+NT)). \tag{3.3}$$

For $t_n\leq t\leq t_n+NT$, the elements of (3.3) are used to update the actuator, *i.e.*, $u(t)=u^a(t_n+kT)$ for $t_n+kT\leq t\leq t_n+(k+1)T$, $0\leq k<N$. Then, for $t\geq t_n+NT$, the actuator continues to feed the plant the last element of (3.3) until the next triggering instant t_{n+1}. Therefore, we have $u(t)=u^a(t_n+NT)$ for $t\geq t_n+NT$. Based on these observations, we can define the measurement error between the actual

and predicted state as follows:

$$e(t)=x^a(t_n+kT)-x(t),\ \text{for } t_n+kT\leq t\leq t_n+(k+1)T \tag{3.4}$$

Thus, the actuator signal can be rewritten as $u(t)=\psi(x(t)+e(t))$. We assume ψ is designed such that the equilibrium $x=0$ of the continuous-time system $\dot{x}(t)=f(x,\psi(x+e))$ is input-to-state stable (ISS) with respect to the error e. This implies the existence of a Lyapunov function V and some $\alpha_1,\alpha_2,\gamma\in\mathbb{K}_\infty,\lambda\in\mathbb{R}_{>0}$ such that the following hold:

$$\alpha_1(|x|)\leq V(x)\leq\alpha_2(|x|), \tag{3.5a}$$

$$\nabla V(x)f(x,\psi(x+e))\leq-\lambda V(x)+\gamma(|e|). \tag{3.5b}$$

As shown in Fig. 3.1, the system is vulnerable to DoS attacks. Suppose the sequences $\{h_n\}$ and $\{\tau_n\}$, $n\in\{\mathbb{N}\cup 0\}$, represent the activation instants of DoS attacks and the corresponding length of the attack, respectively. Then, the nth DoS time-interval is defined as $H_n:=\{h_n\}\bigcup[h_n,h_n+\tau_n]$. The following assumptions provide a deterministic model for the attacks (see reference [7]).

Assumption 3.1. *Let $|E(\tau,t)|$ denotes total time interval of DoS attacks over $[\tau,t]$ where $\tau,t\in\mathbb{R}_{\geq 0}$ and $t\geq\tau$, i.e., $|E(\tau,t)|:=\bigcup_{n\in\mathbb{N}\cup 0}H_n\bigcap[\tau,t]$. We assume that there exist $\eta\in\mathbb{R}_{\geq 0}$, $T_D\in\mathbb{R}_{>1}$ such that $|E(\tau,t)|\leq\eta+\frac{t-\tau}{T_D}$.*

Assumption 3.2. *Let $n_a(\tau,t)$ denotes the number of DoS attacks intervals over $[\tau,t]$. We assume that there exist $\kappa\in\mathbb{R}_{\geq 0}$, $T_n\in\mathbb{R}_{>0}$ such that $n_a(\tau,t)\leq\kappa+\frac{t-\tau}{T_n}$.*

Notice that, $\frac{1}{T_D}$ and $\frac{1}{T_n}$ represent a measure of the fraction of time over which communication is denied, and the dwell-time between any two consecutive DoS intervals, respectively. Smaller values of T_D suggests potential DoS attacks of large duration, and smaller value of T_n represent higher number of attack off-to-on instants.

3.1.1 Event-Triggered Mechanism

We depart from the continuous-time model (3.1) of a nonlinear system and denote F_T^e the exact discrete-time model of (3.1) with sampling period T, *i.e.*, $x(k+1)=F_T^e(x,u_T)$. Recognizing, however that obtaining the exact discrete-time model requires solving the nonlinear differential model equations which, in general, do not admit a closed-form solution, we assume that F_T^e is unknown, and consider an approximate discrete-time model $F_{T,h}^a$. We assume that the model approximation satisfies the one-step consistency property, defined in Definition 2.2.

Our event-triggering mechanism has two working modes; namely when attack is present when it is not. We assume that our triggering module has been equipped with a verification mechanism

to identify successfully transmitted signals (see [27, 24] for more details). Any triggering whose reception is acknowledged will be referred to as a *successful* triggering. When, no verification signal is received, the event mechanism assumes that a DoS attack is present and that communication has been lost. In such case, the event-triggering module turns into periodic sampling with constant sampling period $\Delta \in \mathbb{R}_{>0}$. This periodic sampling, together with the verification mechanism, enables the system to determine when the attack interval has ended, with an accuracy of Δ seconds. During normal operation, *i.e.* in the absence of an attack, the sampling instants are implicitly obtained through the following triggering condition:

$$t_{n+1} = \inf\{t > t_n : \gamma(4|e(t)|) > \lambda_1 V(x(t)) + \gamma(\nu T \rho(h))\} \tag{3.6}$$

where $\lambda_1 := \lambda(1-c)$, $0<c<1$, and $\nu \in \mathbb{R}_{>0}$. Note that during attack intervals the system operates in open-loop and hence, following (3.6) rather than time-triggered sampling may lead to Zeno behaviour due to the fact that the error in (3.6) does not reset to zero during an attack. We will show that our proposed sampling policy prevents the occurrence of Zeno behaviour. The proposed condition (3.6) can be seen as a model-based event-triggered scheme since the error term is defined as the difference between the system states and a reference model, which in this case is the approximate discretization of the original system.

To complete the triggering module, we proceed as follows: notice that the system is potentially vulnerable to DoS attacks. Thus, satisfying the triggering condition (3.6) may not necessarily result in successful transmission. Therefore, we divide t_n into the successful event instants, *i.e.*, $t_i^s = \{t_n : \text{DoS attack is off } \&\ n, i \in \mathbb{N}\}$ and unsuccessful event times, i.e., $t_j^{us} = \{t_n : \text{DoS attack is on } \&\ n, j \in \mathbb{N}\}$. For example, if $t_n = \{t_1, t_2, t_3\}$ and DoS status$=\{\text{on}, \text{off}, \text{on}\}$, Then, $t_i^s = \{t_2\}$, $i = \{1\}$ and $t_j^{us} = \{t_1, t_3\}$, $j = \{1, 2\}$.

Remark 3.1. *The idea behind our strategy is the following: after each event, the digital controller generates the N-point control sequence* (3.3) *that is sent to the buffers. This control input can be used to feed the plant in a time-driven fashion for as long as no new information is received from the event-triggering module. Our strategy is then to use the control sequence stored in the buffers to compensate for the lack of real data during DoS attacks. The event-triggering rule* (3.6) *decides when new information is to be transmitted, based on approximate and real data. The term $\gamma(\nu T \rho(h))$ is used to compensate for the error induced by the model approximation over N steps, by stretching the inter-event times. Notice that the well established triggering rules, such as [63, 23, 91], are not applicable in our strategy without modifying the error function and the triggering threshold. Our proposed triggering rule* (3.6) *consists of a combination of modified versions of the triggering rules in [63] and [91], and is specifically designed to perform in the presence of DoS attacks.*

3.1.2 Main Problem

We can now state our main problem to be solved. Our goal is to obtain the triggering parameters N, T, λ, c that maximize resiliency against DoS attacks. To this end, we formulate an stabilization problem and provide a design procedure to obtain the smallest possible T_D^* such that the event-based control u with triggering condition (3.6), guarantees asymptotic stability of the system (3.1) in the presence of DoS attacks with $T_D \geq T_D^*$.

3.2 Preliminary Results

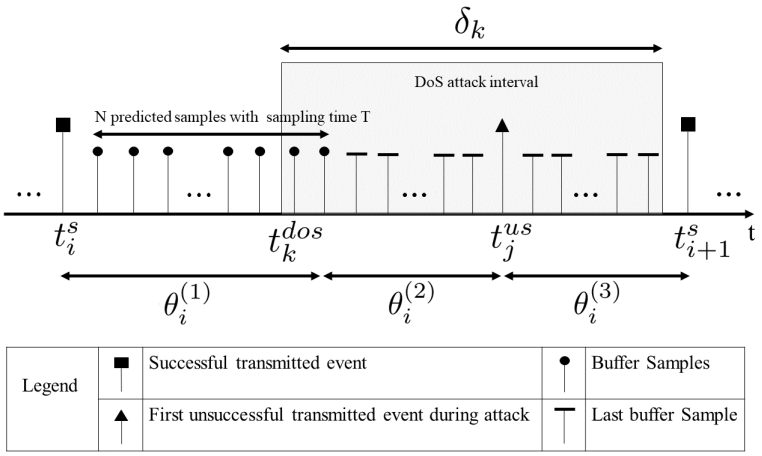

Figure 3.2: Diagram of data transmission time relationship under DoS attack.

Fig. 3.2 provides a schematic of the sampling instants as discussed in previous section. Let t_i^s be the most recent successful transmission instants between sensor and controller, enforced by (3.6). Clearly, at $t{=}t_i^s$ there is no attack present. At this instant, the controller receives the sensor measurement $x(t_i^s)$ and use it to build the stack control vector (3.3) and send it to the buffer. Neglecting transmission delay, the buffer receives $x(t_i^s)$ at the same time $t{=}t_i^s$. Therefore, according to our control structure, the actuator will continue to receive the control signal from the buffer over the finite time-sequence $\{t_i^s, t_i^s{+}T, \ldots, t_i^s{+}NT\}$. After $t{=}t_i^s{+}NT$, the actuator signal is kept constant at its last value $u^a(t_i^s{+}NT)$, until the next successful triggering instant occurs. We also denote by t_k^{dos} the time at which a DoS attack occurs which will last until time $t_k^{dos}{+}\delta_k$. Obviously, any event satisfying the triggering condition during this interval will results in an unsuccessful event that will be denoted by t_j^{us}. These observations are summarized in the following table.

At time t_j^{us}, (3.6) is satisfied thus leading to a new triggering event. Transmission of this information is however impossible due to the presence of the attack. Hence, the ETM does not

Parameter	Definition
t_i^s	Successful triggering instants
t_j^{us}	First satisfaction of event condition during attack
t_k^{dos}	DoS attack activation instants
T	Approximate model sampling time
N	Buffer
δ_k	Length of attack interval

receive the verification signal from the controller and concludes that an attack has occurred. Until the acknowledgement signal verifies the end of the attack interval, data will continue to be sent at a constant rate Δ^{-1}. As suggested by Fig. 3.2, we divide the intersampling interval $[t_i^s, t_{i+1}^s)$ into three subintervals:

i. Interval $\theta_i^{(1)}$ where the buffer provides fresh control signals. Let $\theta_i^{(1)}=[t_i^s, t_i^s+NT]$, then we define

$$\theta_1(t)=\bigcup_{i\in N_s}\theta_i^{(1)}\bigcap[0,t]. \tag{3.7}$$

where N_s is the set of successful triggering events.

ii. Interval $\theta_i^{(2)}$ during which the control signal stored in the buffer has ended. $\theta_i^{(2)}$ can be defined as follows

$$\theta_i^{(2)}=\begin{cases}(t_i^s+NT, t_j^{us}] & t_j^{us}\in(t_i^s+NT, t_{i+1}^s),\\ (t_i^s+NT, t_{i+1}^s) & \text{no event in } (t_i^s+NT, t_{i+1}^s),\\ \emptyset & t_{i+1}^s=t_i^s+NT,\end{cases}$$

then we define

$$\theta_2(t)=\bigcup_{i\in N_s}\theta_i^{(2)}\bigcap[0,t]. \tag{3.8}$$

Notice that because of the Zeno exclusion (Lemma 3.1), t_j^{us} can not happen in $[t_i^s, t_i^s+NT]$ intervals.

iii. Interval $\theta_i^{(3)}$ where a triggering is required, but is impossible due to the presence of attack. $\theta_i^{(3)}$ is defined below

$$\theta_i^{(3)}=\begin{cases}(t_j^{us}, t_{i+1}^s] & t_j^{us}\in(t_i^s+NT, t_{i+1}^s),\\ \emptyset & \text{no event in } (t_i^s+NT, t_{i+1}^s),\end{cases}$$

then we define

$$\theta_3(t)=\bigcup_{i\in N_s}\theta_i^{(3)}\bigcap[0,t]. \tag{3.9}$$

3.2.1 Stability over $\theta_i^{(1)}$

To analyze stability of the closed-loop system under DoS attack we employ the concepts of slow sampling time T_s and fast sampling time T_f in the nonlinear multi-rate approach initiated in [54]. In the absence of attacks, we assume that the sampled-data version of (3.1) with sampling time T_s is a dual-rate stable system in which the digital controller employs an approximate model $F_{T,h}^a$ and fast sampling time T_f to improve the inter-sample behaviour where $T_s{=}NT_f$ and $N{\in}\mathbb{N}_{>0}$. In this regard, we consider $T_f{=}T$ and $T_s{=}NT$. Therefore, according to [54], there exists T such that during the inter-sample period NT, defined as $\theta_i^{(1)}$ in Fig 3.2, the conditions on the Lyapunov function are satisfied and the state trajectories of the closed-loop system are bounded, assuming that [54, Assumptions 9-11] hold. What we seek in the following is to analyze the stability of the event-triggered control system provided in Fig 3.1 in the presence of DoS attack while taking into account the above fact toward the dual-rate sampled-data system.

We begin by the following assumption on (3.1):

Assumption 3.3 ([23])**.** *To avoid finite escape times during attacks, we assume the existence of some $\mu{\in}\mathbb{R}_{>0}$ such that for any $r{\in}\mathbb{R}$ and γ and α_1 in (3.5) we have $\gamma(4r) \leq \mu\alpha_1(r)$.*

Remark 3.2. *In general, one-step (Definition 2.2) and multi-step consistency (Definition 2.3) do not imply each other. However, when $f(x,u)$ and $u_T(x)$ are locally Lipschitz, then for each compact set X there exists $K{\in}\mathbb{R}_{>0}$ and T^* such that for any $0{<}T{<}T^*$ the one-step consistency implies the multi-step consistency with the following α:*

$$\alpha(\delta,T){:=}(1{+}KT)\delta{+}T\rho(h). \tag{3.10}$$

Indeed, following [78, Remark 2], since $f(x,u)$ in (3.1) and u_T are locally Lipschitz we have $|F_T^e(x,u_T(x)) - F_{T,h}^e(z,u_T(z))|{\leq}(1{+}KT)\delta$. Thus, with this type of Lipschitz continuity plus one-step consistency the conditions of [78, Lemma 3] are satisfied, resulting in multi-step consistency.

Lemma 3.1. *Let Assumption 3.3 hold and assume that the approximate model $F_{T,h}^a$ and exact model F_T^e are one-step consistent according to Definition 2.2. Then, the event triggering condition is not satisfied for $t \in \theta_i^{(1)}, i \in \mathbb{N}_s$.*

Proof. With respect to Definition 2.2, for any compact set $\overline{\mathbf{B}}(\delta_x)$, we can always find T and h such that $T\rho(h){\leq}L$ for an arbitrary fixed constant $L{>}0$. This condition is always satisfied by tuning

the sampling time T. For any given $D\in\mathbb{R}_{>0}$ with $|x(0)|\leq D$ we can define a bound $\overline{\mathbf{B}}(\delta_x)$ with the following radius.

$$\delta_x := \alpha_1^{-1}\left(e^{2(2\mu-c\lambda)(\eta+\Delta\kappa)}\alpha_2(D) + (c_{max}(1+3\delta_c))\right)$$

where α_1,α_2 are defined in (3.5) and

$$\begin{aligned}
c_{max} &= \max\{\frac{\gamma(L)+\gamma(8(\frac{\eta+\Delta}{N}+1)(1+KT)^{\frac{\eta+\Delta}{N}}L)}{(2\mu-c\lambda)},\\
&\quad \frac{L}{(2\mu-c\lambda)}, \frac{\gamma(L)}{\lambda}\}\\
\delta_c &= e^{(2(2\mu-c\lambda))\eta_*}\frac{e^{\beta_* T_n\kappa}}{1-e^{-\beta_* T_n}}\\
\eta_* &:= \eta+(1+\kappa)\Delta\\
\beta_* &= (2(2\mu-c\lambda))(\frac{1}{T_D}+\frac{\Delta}{T_n})+((1+N)T\beta)(2\mu-(1+c)\lambda).
\end{aligned}$$

Moreover, since $\alpha_1(D)\leq\alpha_2(D)$ we can conclude that $D\leq\delta_x$. Now, Find T^*, h^* and define ρ^* on $\overline{\mathbf{B}}(\delta_x)$ such that the one-step consistency holds between exact and approximate model. In Theorem 3.2 we show that $x(t)\in\overline{\mathbf{B}}(\delta_x)$, therefore, ρ^* is always valid. Now, recall that the continuous-time system (3.1) is locally Lipschitz. Also, the disturbance-free system results in $x(t_{|t=kT})=x^e(kT)$ and it is valid for any $T<T^*$; Therefore, (2.3) can be written as follows.

$$|x(t)-x^a(t_i+kT)|\leq T\rho(h) \tag{3.11}$$

for time $t_i+kT\leq t\leq t_i+(k+1)T$, and $k\in\{0,\ldots,N\}$ where $\rho(.):=\rho^*(.)+\lambda_{F^a}$ and λ_{F^a} is the Lipschitz constant of approximate model F^a. As an illustration of (3.11) consider $0\leq\delta_T\leq T$ and $k=0$, then we have:

$$\begin{aligned}
&|x(t_i+\delta_T)-x^a(t_i+T)|\\
&= |x(t_i+\delta_T)-x^a(t_i+\delta_T)+x^a(t_i+\delta_T)-x^a(t_i+T)|\\
&\leq |x(t_i+\delta_T)-x^a(t_i+\delta_T)|+|x^a(t_i+\delta_T)-x^a(t_i+T)|\\
&\leq \delta_T\rho^*(h)+\lambda_{F^a}T\leq T\rho(h)
\end{aligned} \tag{3.12}$$

where the last inequality in (3.12) is obtained using (2.3) together with the Lipschitz continuity property of approximate model F^a. Continuing the above process for $k\in\{0,\ldots,N\}$ verifies that inequality (3.11) is valid for any $k\leq N$ and $t\in[t_i+kT, t_i+(k+1)T]$. Also, based on Definition 2.3 and (3.10), the deviation between $x(t)$ and x^a can be upper-bounded by $N(1+KT)^N T\rho(h)$ after

N steps. Therefore, for $t_i \leq t \leq t_i + NT$ we have

$$|x(t) - x^a(t_i^s + kT)| \leq N(1+KT)^N T\rho(h).$$

Consequently, according to the error definition (3.4), we have $|e(t)| \leq N(1+KT)^N T\rho(h)$. Consider the worst case scenario when $|e(t)| = N(1+KT)^N T\rho(h)$, therefore, $\gamma(4|e(t)|) = \gamma(4N(1+KT)^N T\rho(h))$. Based on the triggering rule (3.6) we can define $\nu := 4N(1+KT)^N$, then

$$\gamma(4|e(t)|) = \gamma(\nu T\rho(h)). \tag{3.13}$$

Moreover, Since, $V(x(t))$ is always positive, the following inequality holds true:

$$\gamma(\nu T\rho(h)) \leq \lambda_1 V(x(t)) + \gamma(\nu T\rho(h)). \tag{3.14}$$

Substituting (3.13) into (3.14) we conclude that event triggering rule (3.6) is never violated for $[t_i, t_i + NT]$. □

The result of Lemma 3.1 implies that no triggering takes place during the interval $\theta_i^{(1)}$. To enhance the analysis in this interval we use some ideas from the framework of multirate sampled-data systems. In this context, we consider an scenario where the model updates the state at the (fast) rate $\frac{1}{T}$, whereas measurement samplings are performed at a slower rate $\frac{1}{NT}$.

Consider now the sampled-data system of Fig. 3.1. Based on the observations in Fig. 3.2, at each triggering instant t_i^s, the controller reads the measurement $x(t_i^s)$ and based on this information predicts the state over the instants $\{t_i^s + T, \ldots, t_i^s + NT\}$. These predicted states x^a are then used to compute the actuator signals at the fast sampling rate: $u^a(t_i + kT) = \psi(x^a(t_i + kT))$. Therefore, in view of (3.2), we can rewrite u^a at the fast sampling instants $t_i + kT$ as follows:

$$\begin{aligned}
u^a(t_i^s) &= \psi(x(t_i^s)), \\
u^a(t_i^s + T) &= \psi(F_{T,h}^a(x(t_i^s), u(t_i^s))), \\
&\vdots \\
u^a(t_i^s + NT) &= \psi(F_{T,h}^a(x(t_i^s + (N-1)T), u^a(t_i^s + (N-1)T))).
\end{aligned}$$

We assume that the approximate model $F_{T,h}^a$ with control signal u_T is equi-Lipschitz Lyapunov-ISS (see Definition 2 in [55]). Our next Lemma provides conditions for the ISS stability of the continuous-time system over the θ_i^1 intervals.

Lemma 3.2. *Consider the sampled-data system of Fig. 3.1. The ISS condition* (3.5) *is valid over the time intervals* $\theta_i^{(1)}$ *for continuous-time system* (3.1) *with control sequence* (3.3) *for radius ball* δ_x *and* $i \in N_s$*, if* $|x(0)| \leq D$*.*

Proof. The result of Lemma 3.1 guarantees that no new events can occur during the time interval $\theta_i^{(1)}$. Therefore, the control vector (3.3) is obtained using the predicted state based on the approximate model $F_{T,h}^a$. Now consider [55, Theorem 1], we know that choosing an appropriate sampling time T and numerical integration step h for the approximate model $F_{T,h}^a$, the discrete-time exact model F_T^e is ISS. Thus, considering [79, Theorem 5] we conclude that using the multi-rate approach leads to ISS for (3.1) in a sampled-data control system structure. Hence, the ISS condition (3.5) is satisfied and the Lyapunov function $V(x)$ decreases over $\theta_i^{(1)}$. □

3.3 Main Result

3.3.1 Zeno Exclusion

Lemma 3.3. *Under Assumption 3.1, the dual-mode event-triggering rule* (3.6) *guarantees Zeno-free behaviour for the closed-loop event-triggered system.*

Proof. Based on Lemma 3.1, no triggering occurs during the NT seconds following each triggering instant t_i^s. Moreover, for $\theta_i^{(2)}$ and $\theta_i^{(3)}$ where the verification signal is not received due to the DoS attack, sampling takes place at a constant rate Δ^{-1}. This guarantees the exclusion of Zeno phenomenon, or in other words, the existence of some $\beta{>}0$ such that

$$\phi(t) \leq \beta t, \quad \beta > 0, \tag{3.15}$$

where $\phi(t)$ is the total number of events over the $[0, t]$. □

3.3.2 Stability Analysis

In this section we study the input-to-state stability of the sampled-data system (3.1). Lemma 3.2 provides a stability analysis over the period $\theta_i^{(1)}$ using tools from multirate sampled-data control. According to Lemma 3.2, there is a Lyapunov function whose derivative is decreasing during this interval. In the interval $\theta_i^{(2)}$ there are no new triggering events and therefore the system remains stable, although with a different convergence rate. In the interval $\theta_i^{(3)}$, however, the event rule is violated at least once, the feedback signal cannot get updated due to the presence of the DoS attack. Therefore, in general, the Lyapunov function may increase over this interval. In this section, we discuss the input-to-state stability under DoS attack over the intervals $\theta_i^{(2)}$ and $\theta_i^{(3)}$.

Recall that the continuous-time system (3.1) is locally Lipschitz and disturbance-free. Hence, according to Definitions 2.2-2.3 and the proof of Lemma 3.1, it is easy to see that for $t_i^s{+}kT{\leq}t{\leq}t_i^s{+}(k{+}1)T$,

$k \in \{0, \ldots, N\}$ we have

$$|x^a(t_i^s + kT) - x(t)| \leq T\rho(h). \tag{3.16}$$

Moreover, if $|x(t_i^s + k_1 T) - x(t_i^s + k_2 T)| \leq \delta$ where $\delta \in \mathbb{R}_{\geq 0}$, $k_1, k_2 \in \mathbb{Z}^+$ and $k_1, k_2 \leq \frac{1}{T}(t_{i+1}^s - t_i^s)$, then

$$|x^a(t_i^s + (k_1+1)T) - x(t)| \leq \alpha(\delta, T) \tag{3.17}$$

for $t_i^s + k_2 T \leq t \leq t_i^s + (k_2+1)T$, where x is the system state, x^a is the state predicted by the approximate model, and α is defined in (3.10). We will use the following inequality on a class-$\mathcal{K}_\infty$ function γ during the formulation and proofs:

$$\gamma(a+b) \leq \gamma(2a) + \gamma(2b), \quad a, b \in \mathbb{R}_{\geq 0}. \tag{3.18}$$

Theorem 3.1. *Consider the closed-loop system given by* (3.1), (3.3), (3.6). *Let Assumption 3.3 hold and suppose the system is targeted by DoS attacks satisfying Assumptions 3.1 and 3.2. Then,* $V(x)$ *in* (3.5) *satisfies the following inequalities:*
(1) If t *belongs to a time interval* $\theta_i^{(1)}$*, then*

$$V(x(t)) \leq e^{-\omega_1(t - t_i^s)} V(x(t_i^s)) + \frac{\gamma(\nu T \rho(h))}{\omega_1}.$$

(2) If t *belongs to a time interval* $\theta_i^{(2)}$*, then*

$$V(x(t)) \leq e^{-\omega_2(t - t_i^s - NT)} V(x(t_i^s + NT)) + \frac{\gamma(\nu T \rho(h))}{\omega_2}.$$

(3) If t *belongs to a time interval* $\theta_i^{(3)}$*, then*

$$V(x(t)) \leq e^{\omega_3(t - t_j^{us})} V(x(t_j^{us})) + \frac{c_j}{\omega_3}(e^{\omega_3(t - t_j^{us})}),$$

where $\omega_1 = \lambda$, $\omega_2 = 2\mu - c\lambda$, $\omega_3 = \mu - \lambda$, *and* $c_j \in \mathbb{R}_{\geq 0}$ *is a constant.*

Proof. The proof consists of two parts. In the first part, we evaluate the right side of (3.5b) in the subintervals $\theta_i^{(1)}$, $\theta_i^{(2)}$, and $\theta_i^{(3)}$, and then expand the result for $\theta_1(t), \theta_2(t), \theta_3(t)$ functions. In the second part, we assign upper-bounds to the Lyapunov function by solving differential inequalities.
(i) First Part. 1) Stability analysis for $\theta_i^{(1)}$: In this interval, the stack vector (3.3) consists of the current state value and N future predicted states. Based on lemma 3.2, appropriate choices of N,h and T guarantee the stability of the closed-loop system. Thus, we can use the one-step consistency condition (3.16) to upper bound the error in this interval as $|e(t)| \leq T\rho(h)$ and hence

write

$$\gamma(|e(t)|) \leq \gamma(T\rho(h)) \tag{3.19}$$

where we use the fact that $\gamma \in \mathcal{K}_\infty$. Finally, from (3.5), (3.19) we obtain the following upper bound on $\dot{V}(x(t))$

$$\dot{V}(x(t)) \leq -\lambda V(x(t)) + \gamma(T\rho(h)). \tag{3.20}$$

2) Stability analysis for $\theta_i^{(2)}$: In this interval, the actuator uses the last element of (3.3) and holds it until a new update is received. Contrary to the previous case, here the one-step consistency does not necessarily hold. Thus, to update an upper bound on $\dot{V}$ we start with the event rule (3.6) and write

$$\begin{aligned}\gamma(|e(t)|) &= \gamma(|x^a(t_i^s + kT) - x(t)|) \\ &\leq \gamma(2|x^a(t_i^s + kT)|) + \gamma(2|x(t)|) \\ &\leq \gamma(2|x^a(t_i^s + kT)|) + \mu V(x(t))\end{aligned} \tag{3.21}$$

where the first inequality in (3.21) follows from (3.18) and the second from Assumption 3.3 and (3.5a). Considering the fact that $|e(t)| = |x^a(t_i^s + kT) - x(t)|$ we can write,

$$\begin{aligned}\gamma(2|x^a(t_i^s + kT)|) &\leq \gamma(2|e(t)| + 2|x(t)|) \\ &\leq \gamma(4|e(t)|) + \mu V(x(t)).\end{aligned} \tag{3.22}$$

Substituting (3.6) in (3.22) we obtain

$$\gamma(2|x^a(t_i^s + kT)|) \leq \lambda_1 V(x(t)) + \gamma(\nu T\rho(h)) + \mu V(x(t)). \tag{3.23}$$

Finally, substituting (3.23) into (3.21) and using (3.5), we obtain

$$\dot{V}(x(t)) \leq (\lambda_1 - \lambda + 2\mu) V(x(t)) + \gamma(\nu T\rho(h)). \tag{3.24}$$

3) Stability analysis for $\theta_i^{(3)}$: In this interval, from the definition of error in (3.4), we have

$$e(t) = x^a(t_i^s + kT) - x(t). \tag{3.25}$$

Moreover, considering (3.17) for $t \in [t_j^{us}, t_{i+1}^s]$, we obtain:

$$|x^a(t_{i+1}^s) - x(t)| \leq \alpha(\delta_j, T) \tag{3.26}$$

where $\delta_j>0$. Now, applying the triangular inequality to (3.25) and (3.26), we have:

$$|e(t)| \leq |x(t)|+|x^a(t_i^s+kT)|. \tag{3.27}$$

$$|x^a(t_{i+1}^s)|\leq|x(t)|+\alpha(\delta_j,T) \tag{3.28}$$

In the worst case, the Lyapunov function increases over the interval $\theta_i^{(3)}$, therefore, $|x^a(t_i^s+kT)|\leq|x^a(t_{i+1}^s)|$. Substituting this condition as well as (3.28) into (3.27), we obtain:

$$|e(t)| \leq 2|x(t)|+\alpha(\delta_j,T). \tag{3.29}$$

By applying the function $\gamma(\cdot)$ to both sides of (3.29) and considering the Assumption 3.3, we obtain

$$\gamma(|e(t)|)\leq\mu V(x)+\gamma(2\alpha(\delta_j,T)). \tag{3.30}$$

Finally, substituting (3.30) into (3.5b), we get:

$$\dot{V}(x(t))\leq(\mu-\lambda)V(x(t))+c_j \tag{3.31}$$

where $c_j:=\gamma(2\alpha(\delta_j,T))$.

(ii) Second Part. The next step is to solve (3.20), (3.24) and (3.31), and find an exponentially decaying upper bound for each solution. The differential inequality (3.20) can be written as follows:

$$\begin{aligned} V(x(t)) &\leq e^{-\lambda(t-t_i^s)}V(x(t_i^s))+\gamma(\nu T\rho(h))\int_{t_i^s}^{t} e^{-\lambda(t-\tau)}d\tau \\ &\leq e^{-\omega_1(t-t_i^s)}V(x(t_i^s))+\gamma(\nu T\rho(h)(\frac{1}{\omega_1}-\frac{1}{\omega_1}e^{-\omega_1(t-t_i^s)}) \\ &\leq e^{-\omega_1(t-t_i^s)}V(x(t_c))+\frac{\gamma(\nu T\rho(h))}{\omega_1} \end{aligned} \tag{3.32}$$

which gives us the desired upper bound on the Lyapunov function over $\theta_i^{(1)}$. Similarly, we can solve (3.24) to obtain the following upper bound on the Lyapunov function over $\theta_i^{(2)}$.

$$V(x(t)) \leq e^{-\omega_2(t-t_i^s-NT)}V(x(t_i^s+NT))+\frac{\gamma(\nu T\rho(h))}{\omega_2}. \tag{3.33}$$

Finally, solving the differential inequality (3.31) we obtain:

$$\begin{aligned} V(x(t)) &\leq e^{\omega_3(t-t_j^{us})}V(x(t_j^{us}))+c_j\int_{t_j^{us}}^{t} e^{(2\mu-\lambda)(t-\tau)}d\tau \\ &\leq e^{\omega_3(t-t_j^{us})}V(x(t_j^{us}))+c_j(\frac{1}{\omega_3}e^{\omega_3(t-t_j^{us})}-\frac{1}{\omega_3}) \\ &\leq e^{\omega_3(t-t_j^{us})}V(x(t_j^{us}))+\frac{c_j}{\omega_3}(e^{\omega_3(t-t_j^{us})}) \end{aligned} \tag{3.34}$$

which gives the desired upper bound over $\theta_i^{(3)}$. □

In the next Lemma, we provide upper bounds on the intervals $\theta_1(t)$, $\theta_3(t)$, and consequently we have $\theta_2(t)=[0,t]-(\theta_1(t)+\theta_3(t))$.

Lemma 3.4. *$\theta_1(t)$ and $\theta_3(t)$ which are defined in* (3.7) *and* (3.9)*, are bounded from the above by the following inequalities:*

$$\begin{aligned} &\theta_1(t) \leq (N+1)T\phi(t), \\ &\theta_3(t) \leq |E(0,t)|+\Delta n_a(0,t). \end{aligned} \tag{3.35}$$

Proof. Since the DoS attacks target the system in a random fashion and with different length intervals, several scenarios can happen in regard to activation time of events and attacks. To cover all situations, we consider the worst-case scenario. In that case, the system will send a new event exactly after a DoS attack interval starts. In other words, there exists an unsuccessful triggering at the beginning of the attack interval. Therefore, a conservative upper bound for $\theta_3(t)$ is $|E(0,t)|$ plus $\Delta n_a(0,t)$, where $\Delta n_a(0,t)$ represents the total gap between the end of an attack and new event at t_{i+1}^s. Therefore, part 2 of (3.35) is verified. In addition, we know that the number of events is limited and is restricted by (3.15). In addition, after any event, N predicted samples are used by the actuator, therefore each interval $[t_i^s, t_i^s+NT]$ will take $(N+1)T$ seconds. Consequently, we can consider $(N+1)T\phi(t)$ as an upper bound for the interval $\theta_1(t)$, and part 1 of (3.35) is satisfied. □

Theorem 3.2. *Nonlinear control system* (3.1) *with control input* (3.3) *and ETM* (3.6) *under Assumptions 3.1, 3.2, 3.3, and one-step consistency provided in* (2.3)*, is practically asymptotically stable for given $\delta_x>0$, $|x(0)|\leq\delta_x$, on compact set $\overline{\mathbf{B}}(\delta_x)$ in the presence of DoS attacks, if the attack parameters satisfy the following inequality:*

$$\frac{1}{T_D}+\frac{\Delta}{T_n} \leq \frac{\beta(N+1)T((1+c)\lambda-2\mu)+2\mu-c\lambda}{3}\mu-(1+c)\lambda.$$

Proof. Based on (3.32), (3.33), and (3.34) in Theorem 3.1, the Lyapunov function has the following

upper bound:

$$V(x(t)) \leq e^{-\omega_1\theta_1(t)}e^{-\omega_2\theta_2(t)}e^{\omega_3\theta_3(t)}V(x(0))$$
$$+c_{max}(1+3\sum_{k=1}^{N_{us}} e^{-\omega_1(t-t_k^s)}e^{-\omega_2(t-t_k^s-NT)}e^{\omega_3(t-t_k^{us})}) \tag{3.36}$$

where $c_{max}:=\max\{\frac{c_j}{\omega_3}, \frac{T\rho(h)}{\omega_2}, \frac{\gamma(\nu T\rho(h))}{\omega_1}\}$. Equation (3.36) can be obtained using a procedure similar to that in the proof of [7, Theorem 2] and therefore we omit the details. Recall $T\rho(h)\leq L$ from the proof of Lemma 3.1, and consider (3.10) where α can be represented as a function of $T\rho(h)$, Therefore, c_{max} is purely related to some constants. Also, the summation term in RHS of (3.36) is bounded from above by some constant δ_c (see [7, Lemma 4]). Thus, Equation (3.36) gives us an exponential upper bound for the Lyapunov function valid for all time. Stability in the sense of Lyapunov is obtained if the exponential function on the right-side of (3.36) has a negative rate. Substituting (3.35) in (3.36), separating the time t coefficients, and considering that we look for a negative coefficient in the exponential in (3.36), we obtain

$$\frac{1}{T_D}+\frac{\Delta}{T_n} \leq \frac{\beta(N+1)T((1+c)\lambda-2\mu)+2\mu-c\lambda}{3}\mu-(1+c)\lambda. \tag{3.37}$$

Therefore, we can write

$$V(x(t)) \leq e^{-\omega t+l}V(x(0)) + c_{max}(1+3\delta_c) \tag{3.38}$$

where ω is the overall rate of the exponential term in (3.36) which is negative assuming (3.37) hold, and $l>0$ is the upper-bound of the constant term of $-\omega_1\theta_1(t)-\omega_2\theta_2(t)+\omega_3\theta_3(t)$, defined as $l:=2(2\mu - c\lambda)(\eta + \Delta\kappa)$. To complete the proof, Substituting (3.38) into (3.5), the following upper bound for the state trajectories of the closed-loop system is obtained.

$$|x(t)|\leq\alpha_1^{-1}\left(e^l\alpha_2(|x(0)|)+c_{max}(1+3\delta_c)\right). \tag{3.39}$$

The RHS of (3.39) is equal to δ_x which was defined in Lemma 3.1 as a radius of initial local domain for function ρ. This implies that ρ is valid in all intervals. □

Equation (3.37) provides the relationship between the attack parameters (T_D, T_n), stability (λ), buffer size (N), sampling period (T), event-triggered parameter (c, ν) and event generation rate (β). From (3.37) we conclude that increasing N, we can have harsher attacks which means that the system can tolerate larger DoS attack intervals with higher frequency in comparison with previous works such as [23] and [24]. However, increasing the buffer size N comes with the cost of increasing model mismatch error, and the approximate model might violate multi-step consistency. Therefore, design parameters such as N should be chosen carefully. The following design procedure

will provide a systematic way to choose appropriate parameters:

1. Select the parameters $D, \beta, \Delta \in \mathbb{R}_{>0}$, where $|x(0)| \leq D$, β comes from (3.15), and Δ is the periodic sampling period of the attack detection process of Section II-C.

2. Find $\lambda \in \mathbb{R}_{>0}$ and $\mu \in \mathbb{R}_{>0}$ to satisfy conditions in (3.5b) and Assumption 3.3, respectively.

3. Initiate parameter N, corresponding to the length of sequence (3.3).

4. Choose an approximate model $F^a_{T,h}$ of nonlinear system (3.1) such that conditions in Definition 2.2 and 2.3 hold.

5. Find parameters h and T such that ISS condition (3.5) is preserved for (3.1) in the sampled-data framework over the time interval $\theta_i^{(1)}$.

6. Use the obtained parameters in the prior steps and find minimum values for $T_D \in \mathbb{R}_{>1}$ and $T_n \in \mathbb{R}_{>0}$ in the inequality (3.37) by tuning c such that $0 < c < 1$. Notice that as c approaches 1, performance approaches the continuous-time case at the expense of additional events generated by the triggering rule (3.6).

7. Increase N then repeat steps 4-6. Stop the procedure when either the inequality (3.37) does not hold anymore or appropriate T cannot be found with respect to step 5. Then, $N-1$ is the maximum possible length of the buffer.

8. Substitute the final value obtained for T_D and T_n into the inequalities in Assumptions 3.1-3.2 to find the maximum tolerable DoS attack interval and average frequency.

3.4 Case Study

To show the effectiveness of the proposed algorithm, we consider two nonlinear plants as follows.

Example 1: Consider the nonlinear system $\dot{x} = x^2 - x^3 + u$ (also used in [23]), and notice that the open-loop system has an unstable equilibrium point at the origin. Following [23] we consider the stabilizing controller $u = -2x$, along with the Lyapunov function $V(x) = \frac{1}{2}x^2$. The initial parameters are $\lambda = 2$, $\gamma(r) = \frac{4}{3}r^2$, $\mu = 128/3$, $c = 0.5$, and $T = 0.01$. In order to have a proper comparison between our proposed algorithm, which is based on the model, and the results of [23] in which the model is not used, we consider the same DoS attack scenario where $|E(\tau, t)| = 9$ s, $\eta = 0.54$ and $T_D = 1.33$.

Figure 3.3-(a) shows the state response of the nonlinear system over time. Compared to [23], not only the system reaches the equilibrium but also does so in only 6 seconds which is 4 second faster than the result in [23]. We emphasize that the same *initial* control law is used in both cases.

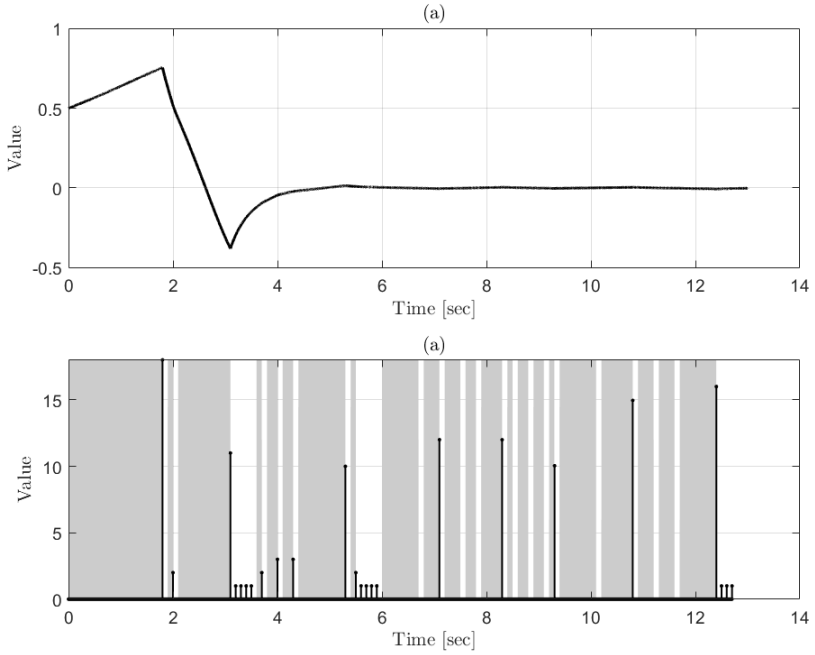

Figure 3.3: (a): Nonlinear system state response under a DoS attack. (b): Inter-sampling time.

The improvement is due to the fact that, we use the predicted control inputs as long as the buffer has unused data samples, leading to remarkably improved results.

Figure 3.3-(b) shows the successful triggering events over time. White and grey strips represent the time periods where there is no activated DoS attack and the attack intervals, respectively. Firstly, in comparison to the time-triggered strategy with sampling time T the number of events has decreased by 52%. In comparison to [23], the number has decreased by 30%, which shows the ability of the proposed event-triggering mechanism in managing network usage, despite sending the control input vector at each event time. Furthermore, the simulation also shows the ability of the proposed method to tolerate larger attack intervals followed by the fact that the system can work in the open-loop mode for a long time without needing a new event. This result is a consequence of using the model-based approach and predictions by the model a DoS attack prevents the use of feedback. Secondly, event congestion is not observed neither under normal condition nor during attacks.

Example 2: In this example we consider the problem of hovering control of the vertical takeoff and landing (VTOL) aircraft to illustrate the effectiveness of our proposed method in a practical control problem. The following model describes the motion of the VTOL aircraft in the x-y plane,

[92].

$$\begin{aligned}
\dot{x}_1 &= x_2 \\
\dot{x}_2 &= -\bar{u}_1 \sin(\theta) + \varepsilon \bar{u}_2 \cos(\theta) \\
\dot{y}_1 &= y_2 \\
\dot{y}_2 &= \bar{u}_1 \cos(\theta) + \varepsilon \bar{u}_2 \sin(\theta) - g \\
\dot{\theta} &= \omega \\
\dot{\omega} &= \bar{u}_2
\end{aligned} \tag{3.40}$$

where x and y are the position of the aircraft in the vertical–lateral plane, θ is the roll angle, and the control inputs $\bar{u}_1, \bar{u}_2$ are the thrust and the rolling moment, respectively. Also, ε>0 represents the coupling between the rolling moment and the lateral acceleration of the aircraft. Since the actuator dynamics is nonlinear, it is convenient to express the control input using hyperbolic functions, [93]. We define the control input as follows ([93]):

$$\bar{u}_i = (\tanh(u_i) + 0.5u_i) \text{ for } i = \{1, 2\}.$$

Thus, given the form of $\bar{u}_1$ and $\bar{u}_2$, which affects (3.40), the resulting nonlinear system is non-affine. As shown in [92], the origin of system (3.40) can be stabilized by the following control law:

$$\begin{aligned}
u_1 &= \sqrt{v_1^2(x_1, x_2) + (v_2(y_1, y_2) + g)^2} \\
u_2 &= -k^2 \left(\theta - \tan^{-1} \left(\frac{-v_1(x_1, x_2)}{v_2(y_1, y_2) + 1} \right) \right) - k\dot{\theta},
\end{aligned}$$

where $v_1(x_1, x_2) = -k_{11}x_1 - k_{12}x_2$, $v_2(y_1, y_2) = -k_{21}y_1 - k_{22}y_2$ and $k_{11}, k_{12}, k_{21}, k_{22} > 0$. Moreover, the Lyapunov function is in quadratic form $V(t) = 0.5(x_1^2 + x_2^2 + y_1^2 + y_2^2 + \omega^2)$. Setting k=10, k_{11}=0.1, k_{12}=0.1, k_{21}=10, k_{22}= and ε=0.01, we study the behaviour of the proposed model-based event-triggered implementation in the presence of DoS attacks. Following the design procedure, we choose parameters N=10, h=0.001, T=0.001, λ= 2, c= 0.2, β=0.05, μ= 60, κ=0.5, η=1, and functions $\rho(r) = |r|$, $\gamma(r) = r^2$. Therefore, based on (3.31), the minimum value of T_D=1.53 and T_n=0.04. To simulate the closed-loop system, we assume initial conditions $[x_1(0), x_2(0), y_1(0), y_2(0), \theta(0), \omega(0)]^T = [1, 0, 0, 0, 0, 0]^T$, and assume the approximate model $F^a_{T,h}$ is constructed using the Euler approximation method. The first event is triggered at t=0, *i.e.* t^s_0=0.

We consider the following scenario: the system is run for 10 seconds while it is exposed to DoS attack in 75% of running time duration, *i.e.*, $|E(t)|$=7.5. The attack is chosen as a periodic signal in which the DoS-on period (grey strip) and DoS-off period (white strip) is T_{on}=0.3 and T_{off}=0.1, respectively. Figure 3.4 illustrates the effectiveness of the proposed method when applied to the VTOL aircraft plant. With respect to Fig. 3.4-(a), even though there is some degradation in the

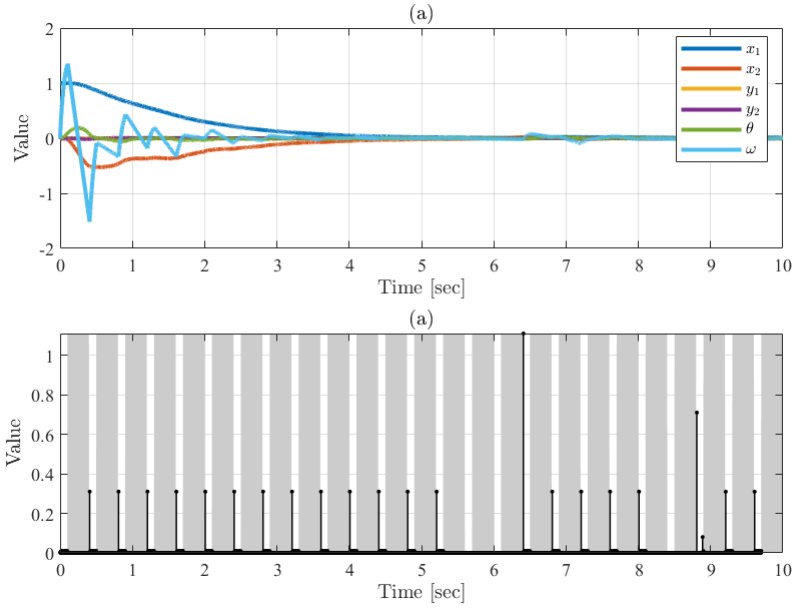

Figure 3.4: (a): Nonlinear system state response under a periodic DoS attack. (b): Inter-sampling time.

system's performance, the states trajectories remain bounded and the system continues to work, so that the proposed scheme is able to preserve stability. Moreover regarding Fig. 3.4-(b), the proposed event-triggered method efficiently manages the network, and there is no Zeno behaviour.

For the purpose of comparison, the same system with the same control law, implemented using a time-driven sampled-data system with a sampling time T=0.001 fails to stabilize the system and the state trajectories are divergent. Furthermore, when classical event triggering rules such as [23, 91], are applied to the same system, they can not provide stability due to the lengthy active DoS attack's time interval.

3.5 Summary

In this chapter we developed a model-based event-triggered control scheme for a general class of nonlinear systems under DoS attacks. Our approach can reduce the amount of communication between plant and controller and can significantly improve resilience against DoS attacks. The event triggering rule makes use of the theory of sampled-data nonlinear control and is defined based on the consistency between approximate and exact models of the plant, and hence, is structurally different from the existing related works. We provide a relation between asymptotic stability and attack parameters which is then used to improve the tolerable DoS attack intervals, when compared

to the other related works in literature. Future work will consider the effect of disturbances and measurement noise in the design, where Zeno exclusion is more critical.

Chapter 4

Multi-Rate Sampled-Data Control Against Zero-Dynamics Attack

In this chapter, we provide a novel defence strategy for a nonlinear sampled-data control system under ZDAs. In a sampled data structure, sampling zeros induced by discretization make a system vulnerable to deception attacks. we analyze the dissipativity in the zero-dynamics part of the system equipped with a multi-rate setup and find conditions on sampling rates to neutralize the attacker's target plan. We show that, under some mild conditions, using multi-rate sampling in the nonlinear sampled-data system not only preserves the dissipativity property of the intrinsic zero-dynamics but also stabilizes the extrinsic zero-dynamics induced by the sample and hold process, and as a result attenuate the effects of attacks on the system stability. Finally, a numerical example is used to illustrate the effectiveness of the proposed approach.

The rest of the chapter is organized as follows: In Section 4.1, we present the fundamental concepts and tools used throughout the sequel. In Section 4.2 we provide several preliminary lemmas for multi-rate sampling used in later sections. Section 4.3 contains the main results. Here we introduce the neutralizing strategy by investigating the preservation of dissipativity in the zero-dynamics of a system under ZDAs. Finally, in Section 4.4 we present a numerical example to show the effectiveness of our proposed approach.

4.1 Problem Statement

Fig. 4.1 shows a schematic of the feedback system used throughout the chapter. The system output is transferred through the network using A/D converters connected to the sensors. The controller output is transferred to the actuators through a network via D/A converters. We assume that the

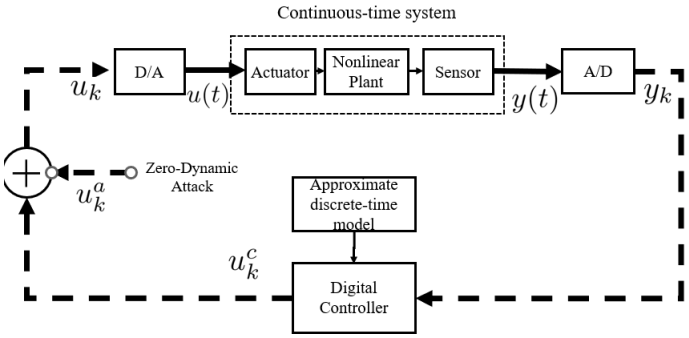

Figure 4.1: Block diagram of the control system under ZDAs

plant is described by the following nonlinear model:

$$\dot{x}(t) = f(x(t)) + g(x(t))u(t), \quad y(t) = h(x(t)), \tag{4.1}$$

where $x \in \mathbb{R}^n$, $u, y \in \mathbb{R}$, and f, g, h are locally Lipschitz function, *i.e.*, $\exists\ \lambda_f$ such that for any x and $\widetilde{x}$ in a compact set X, $|f(x,u) - f(\widetilde{x},u)| \leq \lambda_f |(x - \widetilde{x})|$.

Assume now that the system (4.1) is controlled by

$$\dot{v}(t) = s(y(t), v(t)), \quad u^c(t) = U(y(t), v(t)), \tag{4.2}$$

where $v \in R^r$ is the state of the controller and s, U are continuous, locally Lipschitz functions and zero at zero. Moreover, under no ZDAs, *i.e.* $u^a = 0$, the closed-loop system (4.1)-(4.2) satisfies the differential dissipativity condition defined in Definition 2.1.

Departing from the continuous-time model (4.1) we denote F_T^e the exact discretized model of (4.1) with sampling time T:

$$F_T^e : \{\delta x_k = f^e(x_k) + g^e(x_k)(u_k^c + u_k^a),\ y_k = h^e(x_k)\}, \tag{4.3}$$

where u_k^a in (4.3) represents a ZDA signal defined in Definition 2.5. Similarly, the exact discrete-time model of the dynamic controller (4.2) is given by $S_T^e : \{\delta v_k = s^e(y_k, v_k),\ u_k^c = U^e(y_k, v_k)\}$.

Recognizing, however, that obtaining the exact discrete-time model requires solving the nonlinear differential model equations which, in general, do not admit a closed-form solution, F_T^e and S_T^e represent *ideal* discrete-time models which are, in general, unknown. Throughout our derivations we will rely on a family of approximate discrete-time models $F_{T,h}^a$ and $S_{T,h}^a$ of (4.1) and (4.2), respectively, that can be obtained by numerical integration based on sampling time T and numerical integration step h. The deviation between the approximation and the exact model can be measured

using classical techniques in numerical analysis as provided in Chapter 2.

Remark 4.1. *For convenience, the results are expressed using the δ-operator, [94]. Corresponding results using the shift operator, q, where $\delta=(q-1)/T$ and T is the sampling time, i.e., $\delta x_k=\frac{1}{T}(x_{k+1}-x_k)$, are straightforward to obtain. To analyze and design the control system under a ZDA, we transform* (4.3) *into normal form using Definition 2.4.*

4.1.1 Multi-Rate Sampling

The digital controller in Fig. 4.1 receives the output from the sensor with sampling time T_m and transfers the control input u_k using a faster sampling times T_i, such that $T_i=m_iT_m$ where $m_i\in\mathbb{R}^+_{<1}$, $\sum_{i=1}^{q} m_i=1$, and q is the number of times that we want to update the system between two consecutive samplings of the output at kT_m and $(k+1)T_m$, $k\in\{\mathbb{N}\cup 0\}$. To compensate for the lack of output data on the controller side, $(q+1)$ samples of the control input are constructed based on a discrete-time model. Since, in general, the exact model of a nonlinear system is not available, we use the approximate model F_T^g defined in (2.4), in which $T=\max\{T_i\}$ and $i\in\{1,...,q\}$, to construct u_k^c as follows.

$$u_k^c=\begin{cases} U(h(x_k),v_k), k=iq, i\in\mathbb{Z}^+ \\ U(h(F_T^g),v_k), \text{with i.c. } u_{iq}^c=u(h(x_{iq}),v_k). \end{cases} \tag{4.4}$$

Using the above structure, we focus on neutralizing ZDAs by removing non-minimum phase sampling zeros.

Remark 4.2. *In general, the control system is free to employ any family of approximate model as long as the one-step consistency condition in Definition 2.2 holds. In this chapter, we consider the approximate model defined in* (2.4) *due to its simple zero-dynamics representation.*

4.1.2 Main Problem

Our goal is to drive the internal dynamics of a sampled-data system under a ZDA to a stable region using the multi-rate approach. To this end, we formulate a stabilization problem in the lifted time domain and obtain conditions such that the zero-dynamics part of the sampled-data system is stable, rendering ZDAs ineffective.

4.2 Preliminary Results

In this section, we show that under some mild conditions, the approximate model F_T^g defined in (2.4) can be replaced with the exact model F_T^e in (4.4) while preserving stability. We begin by the following Lemma:

Lemma 4.1. *Suppose $f(x)$ and $g(x)$ are locally Lipschitz functions, then locally Lipschitz continuity is preserved under Lie derivative on a compact set X.*

Proof. Verifying Lipschitz inequality for Lie derivative definition on $x_1, x_2 \in X$ we obtain,

$$\begin{aligned}
&\underbrace{|\frac{\sigma g(x_1)}{\sigma x_1} f(x_1) - \frac{\sigma g(x_2)}{\sigma x_2} f(x_2)|}_{(*)} \\
&\leq |\frac{\sigma g(x_1)}{\sigma x_1}||f(x_1)-f(x_2)| + |f(x_2)||\frac{\sigma g(x_1)}{\sigma x_1} - \frac{\sigma g(x_2)}{\sigma x_2}| \\
&\leq \lambda_g \lambda_f |x_1 - x_2| + |f(x_2)| \underbrace{|\frac{\sigma g(x_1)}{\sigma x_1} - \frac{\sigma g(x_2)}{\sigma x_2}|}_{(**)}.
\end{aligned} \tag{4.5}$$

Re-writing $(**)$ in (4.5) using the definition of derivative and applying the triangular inequality we have,

$$\begin{aligned}
(**) &= \frac{1}{h}|g(x_1+h) - g(x_1) - g(x_2+h) + g(x_2)| \\
&\leq \frac{1}{h}|g(x_1+h) - g(x_2+h)| + \frac{1}{h}|g(x_2) + g(x_1)| \\
&\leq \frac{2}{h}\lambda_g |x_1 - x_2|.
\end{aligned} \tag{4.6}$$

Substituting (4.6) into (4.5), we obtain,

$$(*) \leq (\lambda_g \lambda_f + \lambda_f + M_f + \frac{2}{h})|x_1 - x_2|, \tag{4.7}$$

where $|f(x)| \leq M_f$ on the compact set X follows from the Lipschitz property of $f(x)$. Inequality (4.7) implies that $L_{f(x)}g(x)$ is locally Lipschitz continuous. This completes the proof. □

Lemma 4.2. *The approximate model* (2.4) *is one-step consistent with the Euler approximate model on a compact set X.*

Proof. First, we prove that the model (2.4) is one-step consistent with the Euler model in the new coordinates z according to Definition 2.2, *i.e.*, $|z_{k+1}^u - z_{k+1}^g| \leq T\rho(T)$. Applying Euler discretization

to the system (4.1) in the new coordinates z we obtain the following state space representation, [53]:

$$F_T^u\colon\ \delta\xi_k{=}A\xi_k{+}B\left(\beta_{z_k}{+}\alpha_{z_k}u_k\right),\quad \delta\eta_k{=}\psi\left(\xi_k,\eta_k\right), \tag{4.8}$$

$$A=\left[\begin{array}{c|ccc} 0 & & & \\ \vdots & & I_{r-1} & \\ 0 & & & \\ \hline 0 & 0 & \dots & 0 \end{array}\right], B=\left[\begin{array}{c} 0 \\ \vdots \\ 0 \\ 1 \end{array}\right].$$

Substituting (4.8) and (2.4) into the LHS of one-step consistency inequality of Definition 4.2 we have,

$$\begin{aligned} &|\delta z_k^u-\delta z_k^g| = |\hat{S}_T^e z_k+\hat{G}_T^e(\beta_{z_k}{+}\alpha_{z_k}u_k)| \\ &\leq \underbrace{|\hat{S}_T^e||z_k|+|\hat{B}_T^e||\beta_{z_k}|+|G_T^e||\alpha_{z_k}||u_k|}_{(*)}, \end{aligned} \tag{4.9}$$

where $\hat{S}_T^e=\left[\begin{array}{cc} S_T^e & 0 \\ 0 & 0 \end{array}\right], \hat{B}_T^e=\left[\begin{array}{c} B_T^e \\ 0 \end{array}\right]$ and

$$S_T^e{=}\left[\begin{array}{ccccc} 0 & 0 & -\frac{T}{2} & \cdots & -\frac{T^{r-2}}{(r-1)!} \\ 0 & 0 & 0 & \cdots & -\frac{T^{r-3}}{(r-2)!} \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 0 \end{array}\right], B_T^e{=}\left[\begin{array}{c} \frac{T^{r-1}}{r!} \\ \frac{T^{r-2}}{(r-1)!} \\ \vdots \\ \frac{T}{2} \\ 0 \end{array}\right].$$

Since f and h are both locally Lipschitz, the application of Lemma 4.1 and Assumption 2.1 imply that the vector function ϕ is Lipschitz continuous on any compact set. Therefore, in the new coordinates, $H_{nf}{:}X{\to}Z$, Z is compact (thus bounded), *i.e.*, there is $M_z{\in}\mathbb{R}_{>0}$ such that $|z_k|{\leq}M_z$ for all $z{\in}Z$. In addition, the input u_k is bounded, therefore we can find $M_u{\in}\mathbb{R}_{>0}$ such that $|u_k|{\leq}M_u$. Moreover, Lipschitz continuity of h results in locally Lipschitz for α and β based on Lemma 4.1 in such a way that $|\alpha(z_k)|{\leq}M_\alpha$ and $|\beta(z_k)|{\leq}M_\beta$ for all $z{\in}Z$. Substituting these results into (4.9), the RHS is bounded by the following:

$$(*) \leq \underbrace{|\hat{S}_T^e|M_z+|\hat{B}_T^e|(M_\beta+M_\alpha M_u)}_{(**)}. \tag{4.10}$$

Defining $\rho_{\hat{S}}(T){:=}|\hat{S}_T^e|$ and $\rho_{\hat{B}}(T){:=}|\hat{B}_T^e|$, and substituting them into (4.10), we obtain:

$$(**) \leq \rho_{\hat{S}}(T)M_z+\rho_{\hat{B}}(T)(M_\beta+M_\alpha M_u). \tag{4.11}$$

$\hat{S}_T^e$, $\hat{B}_T^e$ are increasing functions with respect to T, thus, we have $\rho_z(T){:=}M_z\rho_{\hat{S}}(T)+(M_\beta+M_\alpha M_u)\rho_{\hat{B}}(T)\in k_\infty$. Substituting the later into (4.9), considering the triangular inequality, and the initial condition in the one step, *i.e.*, $z_k^u{=}z_k^g$, we obtain

$$|z_{k+1}^u - z_{k+1}^g| \leq |\delta z_k^u - \delta z_k^g| \leq T\rho_z(T). \tag{4.12}$$

Therefore, consistency is satisfied in the new coordinates z.

To prove the consistency between the Euler model and the approximate model we need to show that $|x_{k+1}^u{-}x_{k+1}^g| \leq T\rho(T)$. To this end, we reason as follows: H_{nf} is a diffeomorphism and therefore, $\phi^{-1}(z)$ is continuously differentiable and locally Lipschitz. Thus, consider λ_h as the Lipschitz constant of $\phi^{-1}(z)$ and substitute $x_k{=}\phi^{-1}(z_k)$ into the LHS of the consistency inequality of Definition 4.2. We have:

$$\begin{aligned} |x_{k+1}^u - x_{k+1}^g| &= |\phi^{-1}(z_{k+1}^u){-}\phi^{-1}(z_{k+1}^g)| \\ &\leq \lambda_h |z_{k+1}^u{-}z_{k+1}^g| \leq \lambda_h T\rho_z(T), \end{aligned} \tag{4.13}$$

where in (4.13) the second inequality follows from (4.12). This completes the proof. □

Theorem 4.1. *If the following conditions are satisfied,*

(i) The closed-loop continuous-time system with the control input $u(t)$ is dissipative.

(ii) The approximate model (2.4) *is one-step consistent with the exact model* (4.3) *and is uniform locally Lipchitz.*

Then there exist $T^*{\geq}0$ such that for any $0{<}T_i{\leq}T^*$, $i{\in}\{1,...,q\}$, the nonlinear sampled-data system (4.3) *with control input* (4.4)*, satisfies the dissipativity inequality* (2.2)*.*

Proof. Based on Definition 2.1 $u(t)$ is designed such that the dissipativity inequality (2.2) holds for the continuous time system (4.1). For the second condition, according to [78, Lemma 1], a sufficient condition for the approximate model to be one-step consistent with the exact model is the following: (i) it is one-step consistent with the Euler model, and (ii) $f(x)$ is a bounded, Lipschitz function. According to Lemma 4.2, the approximate model (2.4) is one-step consistent with the Euler approximation. In addition, $f(x)$ is Lipschitz and bounded, consequently the second condition is also verified. Consider now [57, Theorem 1], we know that, under the above conditions, choosing an appropriate sampling time T for F_T^a, the exact discrete-time model F_T^e preserves dissipativity. Thus, considering [79, Theorem 5] we conclude that using the multi-rate approach preserves dissipativity of the original system in a sampled-data implementation. Hence, condition (2.2) is satisfied under control input (4.4) and approximate model (2.4). □

4.3 Main Results

In the sequel, we investigate the feasibility of applying the proposed multi-rate approach in neutralizing ZDAs. Since a multi-rate system can be seen as a periodic system, we formulate the problem in the lifted domain in which the system is time-invariant, thus simplifying the analysis and design.

4.3.1 Lifting

Let $v{=}v_0, v_1, \cdots$ be a sequence of vectors $v_i{\in}\mathbb{R}^n$, $i{\in}\mathbb{Z}^+$. Define $\widetilde{v}$ as a sequence of vectors in $\mathbb{R}^{nq}$ as follows,

$$\widetilde{v} = \left\{ [v_0, v_1, \cdots, v_{q-1}]^\intercal, [v_q, v_{q+1}, \cdots, v_{2q-1}]^\intercal, \ldots \right\}.$$

Then, map $L{:}v{\mapsto}\widetilde{v}$ is defined based on the lifting operator L, *i.e.*, $\widetilde{v}{=}Lv$, [95]. Define the notation (k,i) to refer to the discrete time instant $j{=}kq+i$ for $i{\in}\mathbb{Z}^+_{<q}, k, j{\in}\mathbb{Z}^+$ where

$$(k,i){+}1{=}\begin{cases} (k,i{+}1), & 0{\leq}i{\leq}q{-}2 \\ (k{+}1,0), & i{=}q{-}1 \end{cases} \tag{4.14}$$

To obtain the lifted model we rewrite ξ in (2.4) as follows:

$$\begin{aligned}
&\delta\xi_{(k,1)}{=}S_{T_1}\xi_{(k,0)}{+}B_{T_1}\left(\beta_{z_{(k,0)}}{+}\alpha_{z_{(k,0)}}u_{(k,0)}\right)\\
&\delta\xi_{(k,2)}{=}S_{T_2}\xi_{(k,1)}{+}B_{T_2}\left(\beta_{z_{(k,1)}}{+}\alpha_{z_{(k,1)}}u_{(k,1)}\right)\\
&{=}S_{T_1}S_{T_2}\xi_{(k,0)}{+}S_{T_2}B_{T_1}\left(\beta_{z_{(k,0)}}{+}\alpha_{z_{(k,0)}}u_{(k,0)}\right)\\
&\;+B_{T_2}\left(\beta_{z_{(k,1)}}{+}\alpha_{z_{(k,1)}}u_{(k,1)}\right)\\
&\vdots\\
&\delta\xi_{(k+1,0)}{=}\Pi_{i=j+1}^{q}S_{T_i}\xi_{(k,q-1)}\\
&{+}B_{T_q}\left(\beta_{z_{(k,q-1)}}{+}\alpha_{z_{(k,q-1)}}u_{(k,q-1)}\right)\\
&{+}\Sigma_{j=1}^{q}(\Pi_{i=j+1}^{q}S_{T_i})B_{T_j}(\beta_{z_{(k,j)}}{+}\alpha_{z_{(k,j)}}u_{(k,j)}).
\end{aligned} \tag{4.15}$$

Define $\widetilde{\varepsilon}_{(k,0)}{:=}\left(\varepsilon_{(k,0)}, \varepsilon_{(k,1)}, \ldots, \varepsilon_{(k,q-1)}\right)^\intercal$, where $\varepsilon_{(k,i)} = \beta(z_{(k,i)}){+}\alpha(z_{(k,i)})u_{(k,i)}$, the full state lifting model related to ξ is $\delta\widetilde{\xi}_{(k+1,0)}{=}\widetilde{S}\widetilde{\xi}_{(k,0)}{+}\widetilde{B}\widetilde{\varepsilon}_{(k,0)}$ where, $\widetilde{\xi}_{(k+1,0)} = [\xi^\intercal_{(k,1)}, \xi^\intercal_{(k,2)}, ..., \xi^\intercal_{(k+1,0)}]^\intercal{\in}\mathbb{R}^{qr}$,

and

$$\widetilde{S} = \begin{bmatrix} S_{T_1} & S_{T_1}S_{T_2} & \cdots & \Pi_{i=1}^{q} S_{T_i} \\ 0_{r\times(q-1)r} & 0_{r\times(q-1)r} & \cdots & 0_{r\times(q-1)r} \end{bmatrix}^{\intercal},$$
$$\widetilde{B} = \begin{bmatrix} B_{T_1} & 0 & \cdots & 0 \\ S_{T_1}B_{T_2} & B_{T_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \Pi_{i=1}^{q-1} S_{T_i}B_{T_q} & \Pi_{i=1}^{q-2} S_{T_i}B_{T_q} & \cdots & B_{T_q} \end{bmatrix}. \tag{4.16}$$

Therefore, the equivalent lifted system for the multi-rate sampled-data structure in Fig. 4.1 is written as follows.

$$\begin{aligned} &\delta\widetilde{\xi}_{(k+1,0)}=\widetilde{S}\widetilde{\xi}_{(k,0)}+\widetilde{B}\widetilde{\varepsilon}_{(k,0)}, \quad \delta\widetilde{\eta}_{(k+1,0)}=\widetilde{\psi}(z_{(k,0)}), \\ &\widetilde{y}_{(k,0)}=\widetilde{C}\widetilde{\xi}_{(k,0)}, \end{aligned} \tag{4.17}$$

where $\widetilde{C}$ and $\widetilde{\psi}(.)$ are the lifted parts associated to the output and $\psi(.)$ in (2.4), respectively, which will be derived later.

4.3.2 Zero-Dynamics of the Lifted System

Lemma 4.3. *The transformation H and its inverse, H^{-1}, convert the system* (4.17) *into normal form.*

$$\begin{aligned} H_{qr\times qr}&=\begin{bmatrix} I_H & V_1 & \cdots & V_{r-1} \end{bmatrix}^{\intercal} \\ H^{-1}_{qr\times qr}&=\begin{bmatrix} W & E_1 & \cdots & E_r \end{bmatrix}, \end{aligned} \tag{4.18}$$

$$\begin{aligned} &\textit{where } I_H=diag\{I_h\}, V_i=diag\{\mathcal{V}_{ij}\}, W=diag\{w_j\}, \\ &E_i=diag\{e_i\}, I_h=[1,0,...,0]_{1\times r}, \mathcal{V}_{ij}=[l_{ij}, e_i^{\intercal}], w_j=[1, L_j]^{\intercal}, \\ &L_j=[l_{1j},...,l_{rj}]=\left[\frac{-r}{T_j},...,\frac{-r!}{T_j^{(r-1)}}\right] \textit{ for } i\in\mathbb{Z}^+_{\leq r}, j\in\mathbb{Z}^+_{\leq q}, \end{aligned}$$

and $e_i\in\mathbb{R}^{r\times 1}$ is the unit vector, i.e., $e_i=[\underbrace{0,...,0}_{i-1},1,0,...,0]^{\intercal}$.

Proof. Based on Definition 2.4, a state-space representation is in normal form if the output is set identically to zero, the internal dynamics is explicitly derived. We observe that applying H to (4.17) first re-arranges the order of states in such a way that all lifted states $\widetilde{\xi}^1_{(k,i)}$, $i=1,...,q$,

directly associated to the output, are collected as a vector element in $\bar{\xi}$ as follows,

$$\begin{aligned}\widetilde{\xi}_k&=\left[\left[\xi^1_{(k,1)},...,\xi^r_{(k,1)}\right]^\intercal,...,\left[\xi^1_{(k,q)},...,\xi^r_{(k,q)}\right]^\intercal\right]^\intercal\\ \bar{\xi}_k&=\left[\left[\xi^1_{(k,1)},...,\xi^1_{(k,q)}\right]^\intercal,...,\left[\xi^r_{(k,1)},...,\xi^r_{(k,q)}\right]^\intercal\right]^\intercal,\end{aligned}\tag{4.19}$$

where $\widetilde{\xi}$, the left-side vector in (4.19), represents the current states order ξ in the lifted system (4.17), and $\bar{\xi}$, the right-side vector in (4.19), shows the desired order of states in the normal form representation, *i.e.*, $\bar{\xi}_k = H\widetilde{\xi}_k$. Second, the direct effect of the control input on those parts of the state which are not observed in the output are removed. To verify the later, consider (4.17) in the new coordinates,

$$\delta\bar{\xi}_{(k+1,0)}=\bar{H}\bar{\xi}_{(k,0)}+\bar{B}\bar{\varepsilon}_{(k,0)},\quad \delta\bar{\eta}_{(k+1,0)}=\widetilde{\psi}(\bar{\xi},\bar{\eta}),\tag{4.20}$$

where $\bar{B}=H\widetilde{B}=\left[\frac{T_1^{r-1}}{r!},\frac{T_2^{r-1}}{r!},\cdots,\frac{T_q^{r-1}}{r!}|0_{r\times1},\cdots,0_{r\times1}\right]^\intercal$, and $\bar{H}=H\widetilde{S}=\left[\begin{array}{c|c}\bar{H}_{11}&\bar{H}_{12}\\\hline\bar{H}_{21}&\bar{H}_{22}\end{array}\right]$.

As shown in (4.20), the elements of $\bar{B}$ corresponding to the unobservable states of $\bar{\xi}$ are zero. Therefore, the direct term from the input is removed from $\bar{\xi}^{q+1:qr}$, thus verifying the second condition. Consequently, (4.18) can be used as a normal form transformation for the lifted system (4.17). □

Now, with respect to the normal form representation (4.20), the zero-dynamics of the lifted system is as follows:

$$\delta\bar{\eta}_{(k+1,0)}=\widetilde{\psi}(\xi^{q+1:rq}_{(k,0)},\eta_{(k,0)})\tag{4.21}$$

$$\delta\bar{\xi}^{q+1:qr}_{(k+1,0)}=\bar{H}_{22}\delta\bar{\xi}^{q+1:qr}_{(k,0)},\tag{4.22}$$

$$\text{where } \bar{H}_{22}=\left[\begin{array}{ccc}\mathrm{Bl}^2_{1q}&\cdots&\mathrm{Bl}^r_{1q}\\\vdots&\ddots&\vdots\\\mathrm{Bl}^2_{(r-1)q}&\cdots&\mathrm{Bl}^r_{(r-1)q}\end{array}\right],\mathrm{Bl}^k_{ij}=\left[\begin{array}{cc}0&V^k_{ij}\end{array}\right],$$

$$V^k_{ij}=\left[\begin{array}{cccc}V_{i1}S_{T_1}e_k&V_{i2}S_{T_1}S_{T_2}e_k&\ldots&V_{ij}\Pi^q_{\ell=1}S_{T_\ell}e_k\end{array}\right]^\intercal.$$

The subsystem (4.21) is the counterpart of the continuous-time zero-dynamics, and (4.22) is induced by the sampling zeros.

4.3.3 Stability of the Zero-Dynamics

Assumption 4.1. *Consider the following normal form representation of the continuous-time system* (4.1)*:*

$$\dot{\xi}(t)=A\xi(t)+B\left(\beta_{z(t)}+\alpha_{z(t)}u(t)\right), \quad \dot{\eta}(t)=\psi_{z(t)}, \tag{4.23}$$

where A, B *are defined in* (4.8)*. Throughout this section we assume that the zero-dynamics of* (4.23) *is minimum-phase and satisfies the dissipativity inequality, i.e., there is a continuously differentiable storage function* $V_z(t)$*, and a supply rate* $\omega(t)$ *such that the following inequality holds.*

$$\dot{V}_z(t) = \frac{\partial V_z}{\partial \eta(t)}\psi(0,\eta(t)) \leq \omega(y(t)). \tag{4.24}$$

Remark 4.3. *If the original system* (4.1) *is non-minimum phase, then stabilization of the intrinsic zero-dynamics is only possible by modifying the plant's structure, [47, 48]. However, a minimum-phase system is still vulnerable to ZDAs in sampled-data format* (4.3) *due to the unstable extrinsic zero-dynamics originated in the sampling process. Our goal is to provide conditions such that the minimum-phase property of* (4.1) *(or its modified version) is preserved when using a digital controller. Thus, the ZDA is no longer a threat.*

Theorem 4.2. *Under Assumptions 2.1, 4.1, and the dissipativity property of closed-loop system* (4.1)-(4.2)*, for any pair* $\{\delta,\nu\}\in\mathbb{R}_{>0}$*, the intrinsic zero-dynamics* (4.21) *under multi-rate control input* (4.4) *satisfy the following dissipation inequality for all* $|\eta(0)|<\delta$*.*

$$V(\bar{\eta}_{(k+1,0)}) - V(\bar{\eta}_{(k,0)}) \leq \frac{1}{T}\left(\omega(\bar{\eta}_{(k,0)}) + \nu\right). \tag{4.25}$$

Proof. We first expand the lifted internal dynamic $\widetilde{\psi}$ in (4.21) under the zero-output condition to find the relationship between intermediate states for the intrinsic zero-dynamics in the lifted-domain. We have:

$$\begin{aligned}
&\delta\eta_{(k,1)} = \psi(\eta_{(k,0)})\\
&\delta\eta_{(k,2)} = \psi(\eta_{(k,1)}) = \psi\left(\eta_{(k,0)} + T_1\psi(\eta_{(k,0)})\right)\\
&\vdots\\
&\delta\eta_{(k+1,0)} = \psi(\eta_{(k,q)}) = \psi(\Sigma_{i=1}^{q-1}T_i\delta\eta_{(k,i)}).
\end{aligned}$$

Define $\bar{\eta}_{(k+1,0)}:=[\eta_{(k,1)},\eta_{(k,2)},\cdots,\eta_{(k+1,0)}]^\intercal$, and

$$\widetilde{\psi}(\eta_{(k,0)}):=[\psi(\eta_{(k,0)}),\psi(\Sigma_{i=0}^{1}T_i\delta\eta_{(k,i)}),\cdots,\psi(\Sigma_{i=0}^{q-1}T_i\delta\eta_{(k,i)})]^\intercal$$

therefore we have

$$\delta\bar{\eta}_{(k+1,0)} = \widetilde{\psi}(\eta_{(k,0)}). \tag{4.26}$$

According to Assumption 4.1, V_z exist and it is continuously differentiable. To evaluate the dissipation inequality for the zero-dynamics (4.26), we define a new storage function V_l:

$$V_l(\bar{\eta}_{(k+1,0)}) = \sum_{i=1}^{q} V_z(\delta\eta_{(k,i)}). \tag{4.27}$$

Substituting (4.27) in the LHS of (4.25) we obtain,

$$\begin{aligned} &V_l(\bar{\eta}_{(k+1,0)}) - V_l(\bar{\eta}_{(k,0)}) = \\ &V_z(\delta\eta_{(k,1)}) + \cdots + V_z(\delta\eta_{(k,q-1)}) + V_z(\delta\eta_{(k+1,0)}) \\ &- V_z(\delta\eta_{(k-1,1)}) - \cdots - V_z(\delta\eta_{(k-1,q-1)}) - V_z(\delta\eta_{(k,0)}). \end{aligned} \tag{4.28}$$

Substituting (4.26) into (4.28), we have,

$$\begin{aligned} V_l(\bar{\eta}_{(k+1,0)}) - V_l(\bar{\eta}_{(k,0)}) = &\underbrace{V_z(\psi(\eta_{(k,0)})) - V_z(\psi(\eta_{(k-1,0)}))}_{\text{Term 1}} \\ &+ \underbrace{V_z(\psi(\Sigma_{i=0}^{1} T_i \delta\eta_{(k,i)})) - V_z(\psi(\Sigma_{i=0}^{1} T_i \delta\eta_{(k-1,i)}))}_{\text{Term 2}} \\ &\vdots \\ &+ V_z(\psi(\Sigma_{i=0}^{q-1} T_i \delta\eta_{(k,i)})) - V_z(\psi(\Sigma_{i=0}^{q-1} T_i \delta\eta_{(k,i)})). \end{aligned} \tag{4.29}$$

According to Assumption 2.1, ψ is continuously differentiable, therefore, according to Lemma 1, ψ satisfies a locally Lipschitz condition and the mean value theorem (see also [96]). Let λ be the Lipschitz constant of ψ, and $b, c > 0$ be such that $|\psi(\eta)| \leq b$ and $|\partial V_z/\partial\eta| \leq c$ on the set $|\eta| \leq \delta$. Thus, using the mean value theorem, the triangular inequality and the local Lipschitz property of ψ, we can conclude that,

$$\begin{aligned} \text{Term 1} &\leq \frac{\partial V_z}{\partial \eta}_{|\eta_*} |\psi(\eta_{(k,0)}) - \psi(\eta_{(k-1,0)})| \\ &\leq c\lambda |\eta_{(k,0)} - \eta_{(k-1,0)}| \leq c\lambda T_1 |\psi(\eta_{(kT+\theta_1 T,0)})| \leq \lambda T_1 bc, \\ \text{Term 2} &\leq \frac{\partial V_z}{\partial \eta}_{|\eta_*} |\psi(\Sigma_{i=0}^{q-1} T_i \delta\eta_{(k,i)}) - \psi(\Sigma_{i=0}^{1} T_i \delta\eta_{(k,i)})| \\ &\leq c\lambda |\eta_{(k,0)} + T_1 \psi(\eta_{(k,0)} - \eta_{(k-1,0)} - T_1 \psi(\eta_{(k-1,0)}))| \\ &\leq c\lambda T_1 |\psi(\eta_{(kT+\theta_1 T,0)})| + T_1 c\lambda^2 |\eta_{(k,0)} - \eta_{(k-1,0)}| \\ &\leq c\lambda T_1 b + c\lambda^2 T_1 T_2 |\psi(\eta_{(kT+\theta_2 T,0)})| \leq \lambda bc(T_1 + \lambda T_1 T_2), \end{aligned} \tag{4.30}$$

where $\theta_1, \theta_2 \in (0,1)$. Repeating the above argument for $i = 2, ..., q-1$, we conclude that all terms in (4.30) are bounded and combining the bounds obtained for Term 1 to Term q in (4.29), the dissipation inequality (4.25) is verified. □

Theorem 4.3. *The extrinsic zero-dynamics* (4.22) *is stable under the multi-rate control input* (4.4) *during the ZDAs defined in Definition 2.5 if* $T_i \leq T^*$ *for* $i \in \{1, ..., q\}$, *and* $q \geq r$.

Proof. The first condition guarantees the feasibility of an inferential control setup (4.4) with respect to the result in Theorem 4.1. Consider now internal dynamics given in (4.22). We know that eigenvalues of $\bar{H}_{22}$ (eig$\{\bar{H}_{22}\}$) represent sampling zeros induced by discretization. Thus, if all eig$\{\bar{H}_{22}\}$ are moved to a stable region, then the associated extrinsic zero-dynamics (4.22) is stable. Consider the matrix $\bar{H}_{22}$ derived from $\bar{H}$ in (4.20). All of the entries in the main diagonal of this matrix have terms of the form $\Pi_{\ell=1}^{q} S_{T_\ell}$. Since S_{T_ℓ} is *nilpotent*, then it is such that if $q \geq r$, then $\Pi_{\ell=1}^{q} S_{T_\ell} = 0$. Consequently, all the main diagonal elements of $\bar{H}_{22}$ are zero, making it possible to convert $\bar{H}_{22}$ into an upper-triangular matrix using standard row operations in such a way that the main diagonal elements remain zero, *i.e.*, $H_\Delta = H_u \bar{H}_{22}$ where H_Δ is the upper triangular matrix and H_u is the transformation such that eig$\{\bar{H}_{22}\}$=eig$\{H_\Delta\}$. Now, because eig$\{H_\Delta\}$ are located on the main diagonal and are identically zero, eig$\{\bar{H}_{22}\}$ are zero which means that all sampling-zeros are on the boundary of the stability region since, in the δ-operator, this region is a circle of radius 1 centred at $(-1, 0)$. To complete the proof we need to show that the multiplicity of eig$\{\bar{H}_{22}\}$ is at most equal to 1 and consequently the extrinsic zero-dynamics is stable under multi-rate sampling.

Define the set $\mathbb{Z}^c = \{\mathbb{Z}^+ - \{q, 2q, 3q, \cdots\}\}$. Notice that in $\bar{H}_{22}$, the $iq, i \in \mathbb{Z}^+$, rows have all of their entries identically zero. Thus, from (4.22) we can write, $\delta\bar{\xi}_{(k+1,0)}^{(i+1)q} = 0$, for $i \in \mathbb{Z}^+$. By rewriting the above equation with respect to the standard shift-operator and expanding it using (4.15) we have,

$$\begin{aligned} \bar{\xi}_{(k+1,0)}^{(i+1)q} &= \Pi_{\ell=1}^{q} S_{T_\ell} \delta\bar{\xi}_{(k,0)}^{(i+1)q} \\ &+ \Sigma_{j=1}^{q} (\Pi_{\ell=j+1}^{q} S_{T_\ell}) B_{T_j} \left(\beta(z_{(j-1,0)}) + \alpha(z_{(j-1,0)}) u_{(j-1,0)}\right). \end{aligned} \tag{4.31}$$

Under a ZDA the control input is manipulated by the attacker to make the output identically zero, *i.e.*, $u_{(j-1,0)} = \frac{-\beta(z_{(j-1,0)})}{\alpha(z_{(j-1,0)})}$, therefore, the second term in the RHS of (4.31) will be zero. On the other hand, S_T is a nilpotent matrix and as a result $\Pi_{\ell=1}^{q} S_{T_\ell} \delta\bar{\xi}_{(k,0)}^{(i+1)q} = 0$. Consequently we have,

$$\bar{\xi}_{(k+1,0)}^{(i+1)q} = 0, \text{ for } i \in \mathbb{Z}^+. \tag{4.32}$$

Consider now the remaining states in (4.22), *i.e.*, $\bar{\xi}_{(k+1,0)}^{q+i}$ for $i \in \mathbb{Z}^c$. With respect to $\bar{H}_{22}$ in (4.22), all of these states in the δ-operator formulation are constructed based on $\bar{\xi}_{(k+1,0)}^{(i+1)q}, i \in \mathbb{Z}^+$. As shown in (4.32), these states are equal to zero during the ZDA. Therefore, we have $\delta\bar{\xi}_{(k+1,0)}^{q+i} = 0$ for $i \in \mathbb{Z}^c$ which equivalent to the following equation in the shift-operator: $\bar{\xi}_{(k+1,0)}^{q+i} = \bar{\xi}_{(k,0)}^{q+i}$, for $i \in \mathbb{Z}^c$. Thus,

we conclude that during a ZDAs all non-zero states remain in the last update. Therefore, using the proposed method, all states of the extrinsic zero-dynamics stay in a bounded region during the attack. Indeed, the latter observation proves that all zero eigenvalues of $\bar{H}_{22}$ have multiplicity one. Therefore, the extrinsic zero-dynamics (4.22) is stable in the sense of Lyapunov during the attacks. □

It is worth mentioning that the values of T_is and q can impact performance and data transmission in a system. Higher values of q can improve performance but also increase communication bandwidth needs. To minimize the transmission rate, q should be set as low as possible.

Remark 4.4. *Theorems 4.2 and 4.3 indicate that for any minimum-phase system* (4.1)*, the use of multi-rate sampling can preserve the minimum-phase property of the sampled-data structure, provided that some mild conditions on the sampling rates are satisfied. Consequently, no unbounded stealthy ZDAs are possible, and cyber-attacks constructed based on the system's zero-dynamics will not pose significant damage to the plant.*

Remark 4.5. *Our formulation ignores the possible existence of noise and disturbances. Notice, however, that noise and disturbances do not change the inherent zero-dynamics nor the extrinsic zero-dynamics of the system. The former depends on the plant structure, [47] and [48], and the latter on the sampling rate and relative degree, [53]. Therefore, all of our results remain valid under noise and disturbances. These signals should be dealt with when the designing the original controller and do not affect our derivation in any respect.*

4.4 Case Study

To illustrate the effectiveness of the proposed method, we consider a nonlinear benchmark plant, the single-link flexible-joint robot manipulator (see reference [97]). The state-space representation of the robot is given by:

$$\dot{x} = f(x) + g(x)u, \quad y = x_1, \tag{4.33}$$

$$f(x)=\begin{bmatrix} x_2 \\ -\frac{MgL}{I}\sin(x_1) - \frac{k}{I}(x_1 - x_3) \\ x_4 \\ \frac{k}{J}(x_1 - x_3) \end{bmatrix}, \quad g(x)=\begin{bmatrix} 0 \\ 0 \\ 0 \\ \frac{1}{J} \end{bmatrix},$$

where $x=[x_1, x_2, x_3, x_4]^\intercal$. States x_1, x_2 are the angular position and velocity of the manipulator's link, and x_3 and x_4 are the angular position and velocity of the manipulator's base, respectively (see

reference [97] for more details). Since x_2, x_3, x_4 are not available from measurement, the control system is equipped with a high gain observer to estimate the states. The input signal u is applied to the base. The control law is designed using sliding mode method as follows, [98]:

$$\begin{aligned} s &= c_1\xi_1 + c_2\xi_2 + c_3\xi_3 + \xi_4 \\ u &= \left(-c_1\xi_2 - c_2\xi_3 - c_3\xi_4 - F(\xi) - \beta\,\mathrm{sgn}(s)\right)/b, \end{aligned} \tag{4.34}$$

where $\xi_1, ..., \xi_4$ are normal form states, and $F(\xi)=\frac{-MgL}{I}\sin\xi_1\left(\frac{K}{J}-\xi_2^2\right)-\left(\frac{K}{I}+\frac{K}{J}+\frac{MgL}{I}\cos\xi_1\right)\xi_3$, $b=\frac{K}{IJ}$ and $\beta=L+K$.

It is easy to see that the relative degree of the system (4.33) is 4, same as the number of states, *i.e.*, $n=r=4$. Therefore, the continuous-time system (4.33) is minimum-phase. Applying the discretization method (2.4) with sampling time $T=0.01$ seconds, the new zero-dynamics after the sample and hold process is:

$$\delta\xi_k^{2:4}=\begin{bmatrix} -400 & -1 & -0.008 \\ -12\times10^4 & -600 & -30 \\ -24\times10^6 & -12\times10^4 & -800 \end{bmatrix}\xi_k^{2:4}. \tag{4.35}$$

Although all eigenvalues are outside the stability region resulting in an unstable zero-dynamics, we see from Fig. 4.2-a that the controller u in (4.34) successfully stabilizes the robot's dynamic with initial condition $[1, 0, 1, 0]^\intercal$. Moreover, the non-minimum phase property of the zero-dynamics does not affect stability of the closed-loop system in the absence of attacks.

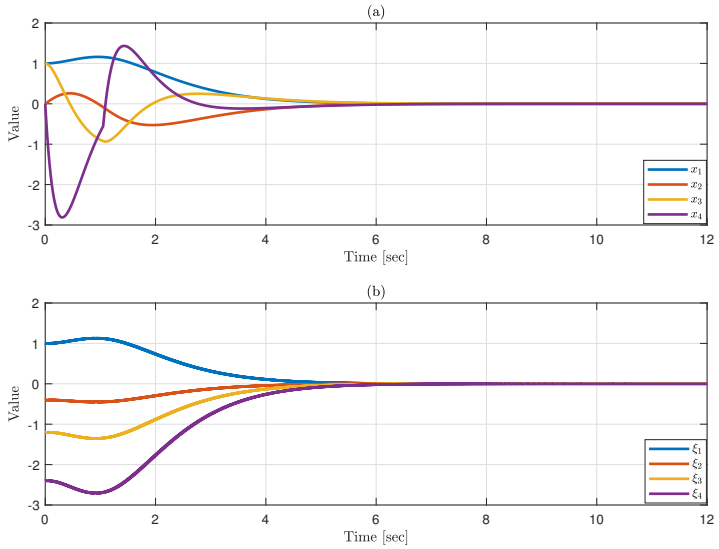

Figure 4.2: Trajectories of the original (a) and normal form (b) states.

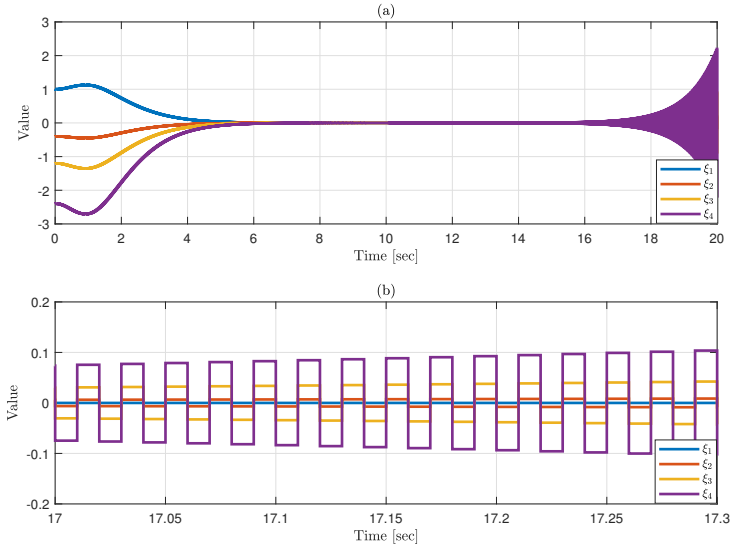

Figure 4.3: Trajectory of the normal form states (a) and details (b).

Consider now a ZDA generated based on the unstable zero-dynamics (4.35) and activated at t=10s. Fig. 4.3 shows that the internal dynamic states ξ_2, ξ_3, ξ_4 become unbounded, however the undamped oscillations are not observed in y=ξ_1, as is characteristic of the stealthy property of the

ZDA.

We now apply the proposed method. Since the relative degree is 4, then considering the condition $q \geq r$ in Theorem 4.3, we choose $q=4$ and $T_1, T_2, T_3, T_4 = \frac{T}{4}$ which results in a dual-rate control system.

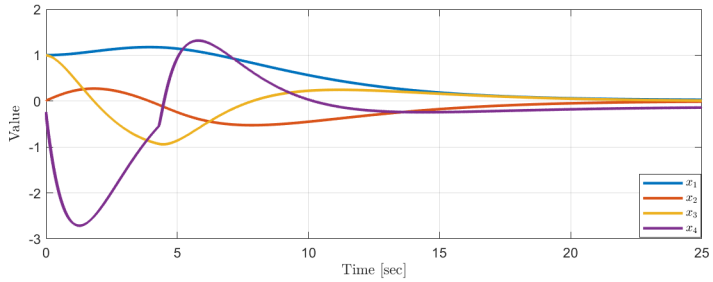

Figure 4.4: Trajectory of the dual-rate control system under ZDA.

Fig. 4.4 shows the dynamic response of the closed-loop robot under the ZDA. Although the attack is activated at $t=0$, the dual-rate controller stabilizes the system dynamics and neutralizes the malicious effect of the ZDA such that all states remain bounded. In other words, using the multi-rate approach removes non-minimum phase sampling zeros resulting in a stable zero-dynamics. As a result, any attack generated based on sampling zeros results in a bounded signal without threat to the control system.

4.5 Summary

We have developed a resilient control scheme using multi-rate sampling for systems under ZDAs. The proposed method removes the non-minimum phase zero-dynamics induced by discretization and preserve the minimum-phase property of the intrinsic zero-dynamics. The result is a sampled-data structure that is immune to zero-dynamics attacks.

Chapter 5

Event-Triggered Control Against Zero-Dynamics Attacks

It is well-known in the literature that the discretization process in a sampled-data structure potentially may induce an unstable zero-dynamics aside from the minimum-phase condition of the original system which makes the system vulnerable to cyber-attacks. We study input-to-state stability of nonlinear event-based control systems under ZDAs, and as a secure approach, propose a novel multi-objective event-triggered mechanism by resilient design of triggering strategy based on current measurements together with a history of zero-dynamics. As a result, sufficient conditions in terms of ISS and event triggering parameters are derived to guarantee stability. The proposed solution makes it possible to have a trade-off between performance and resiliency while it keeps the overall system asymptotic stable under the attack. Finally, a case study is presented to illustrate the effectiveness of the proposed approach.

The chapter layout is as follows: In Section 5.1, we present the fundamental concepts and our proposed event-triggered structure used throughout the sequel. In Section 5.2 we provide several preliminary lemmas for sampling zeros and event-triggered sampling used in later sections. Section 5.3 contains the main results. Under the developed method, here we investigate the boundedness property of the zero-dynamics of a system exposed to attacks, as well as asymptotic stability of the overall system. Finally, in Section 5.4 we present a numerical example to show the effectiveness of our proposed approach.

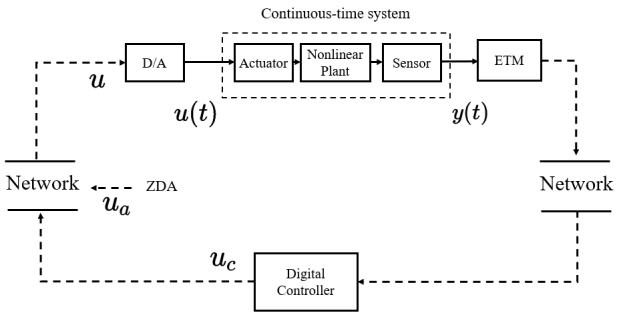

Figure 5.1: Block diagram of the closed-loop control system equipped with an event-triggered mechanism under ZDAs

5.1 Problem Statement

We consider a minimum-phase, continuous-time nonlinear system given by the following state-space realization:

$$\begin{aligned} \dot{x}(t) &= f(x(t)) + g(x(t))u(t) \\ y &= h(x(t)), \end{aligned} \tag{5.1}$$

where $x(t)\in\mathbb{R}^n$, $u(t), y(t)\in\mathbb{R}$, and f, g, h are locally Lipschitz function, *i.e.*, $\exists\ L_f$ such that for any x and $\widetilde{x}$ in a compact set X, $|f(x,u)-f(\widetilde{x},u)| \leq L_f|(x-\widetilde{x})|$.

Fig. 5.1 shows a schematic of the feedback system that will be used throughout the rest of the chapter. Here the event-triggered mechanism block continuously monitors the sensor output and determines when to send fresh data through the communication network, based on a triggering rule. We will denote by t_k, $k\in\mathbb{N}^0$, the event-time. Since the event-time is defined implicitly by the triggering rule, the resulting sampling is nonuniform. Neglecting transmission delay, we assume that the controller receives the transmitted data $y(t)$ at the event time t_k. The computer control generates the control input $u_c(t_k)=\psi(y(t_k))$ for some Lipschitz function ψ, and sends the information through the network at the same instant t_k. Assuming an insecure network, the control input may be corrupted by an attacker who injects the ZDA signal $u_a(t_k)$. A zero-order-hold device is used to maintain the actuator signal $u(t)$ constant over inter-event times, *i.e.* $u(t)=u_c(t_k)+u_a(t_k)$ for $t\in[t_k, t_{k+1})$. Thus, the difference between $y(t)$ and the last transmitted output $y(t_k)$ in the ETM for decision making, is given by

$$e(t)=y(t_k)-y(t) \text{ for } t\in[t_k, t_{k+1}). \tag{5.2}$$

In the absence of attacks, we have that $u(t)=\psi(y(t_k))$, and the actuator input is given by $u(t)=\psi(y(t)+e(t))$ using (5.2). We assume ψ is designed such that the equilibrium $x=0$ of the continuous-time sys-

tem (5.1) is input-to-state stable with respect to the error (5.2) for any initial condition $x_0 \in X$. This implies the existence of a Lyapunov function V and $\nu_1, \nu_2, \nu, \gamma \in \mathcal{K}_\infty$ such that the following conditions hold:

$$\nu_1(|x|) \leq V(x) \leq \nu_2(|x|), \tag{5.3a}$$

$$\nabla V(x)(f(x) + g(x)u) \leq -\nu(|x|) + \gamma(|e|). \tag{5.3b}$$

Let τ_k be the inter-event period at event instant t_k, *i.e.* $\tau_k = t_k - t_{k-1}$ for $k \in \mathbb{N}^0$ which in general is non-constant and determined by the event-triggering rule. The following definition introduces a generalized form of sampling zeros. The sampling zeros depend on the system's dimension n and relative degree r together with the time period τ_k between two consecutive samples at t_k and t_{k-1}, [53].

Definition 5.1 (*Sampling zeros*)**.** *Sampling zeros are the eigenvalues of a matrix $Q(\tau_k)$ associated with the time-varying linear system of dimension $r-1$, known as extrinsic zero-dynamics. The sampling zeros are induced by the sample and hold process and can be represented using the δ-operator discrete-time model, as follows:*

$$\begin{cases} \delta\eta_k = Q(\tau_k)\eta_k \\ Q(\tau_k) = T_{21}(\tau_k)A_{12}(\tau_k) + A_{22}(\tau_k) \end{cases} \tag{5.4}$$

where

$$T_{21}(\tau_k) = \begin{bmatrix} -\frac{n}{\tau_k} & \cdots & -\frac{n!}{\tau_k^{n-1}} \end{bmatrix}^\intercal,$$

$$A_{12}(\tau_k) = \begin{bmatrix} 1 \\ \frac{\tau_k}{2} \\ \vdots \\ \frac{\tau_k^{n-2}}{(n-1)!} \end{bmatrix}^\intercal, A_{22}(\tau_k) = \begin{bmatrix} 0 & 1 & \cdots & \frac{\tau_k^{n-3}}{(n-2)!} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Let $S(Q(\tau_k))$ denote the spectrum of $Q(\tau_k)$, *i.e.* $\lambda^i_{\tau_k} \in S$ for $i \in \{1, ..., r-1\}$, and τ_k be the (variable) inter-event times. The following lemma outlines the main features of the time-varying matrix $Q(\tau_k)$ and its eigenvalues associated with time-varying sampling zeros.

Lemma 5.1. *The spectrum $S(Q(\tau_k))$ has the following properties:*

I. At any event instant t_k, all eigenvalues of $Q(\tau_k)$ are real (i.e. $\lambda^i_{\tau_k} \in \mathbb{R}$).

II. The eigenvalues $\lambda^i_{\tau_k} \in S$ are monotonically decreasing with respect to τ_k, i.e.,

$$\lambda^i_{\tau_k} \leq \lambda^i_{\tau}, \quad \textit{for} \quad \tau \leq \tau_k$$

III. There exist $k_\lambda^{(2)} \in \mathbb{R}_{>0}$ *such that the following inequality holds for any* $\lambda_{\tau_k}^i \in S$ *and* τ_k*:*

$$\lambda_{\tau_k}^i \leq \frac{k_\lambda^{(2)}}{\tau_k}$$

IV. for any $\lambda_{\tau_k}^i, \lambda_{\tau_k}^j \in S$ *if* $|\lambda_{\tau_k}^j| \leq |\lambda_{\tau_k}^i|$ *at* $\tau_k = \tau$*, then the inequality is also valid for* $\tau_k \geq \tau$*.*

Proof. Part I follows from the fact that matrix $Q(\tau_k)$ is persymmetric for any value of τ_k.

To verify II, let $Q_c = \tau_k Q(\tau_k)$, and suppose λ_c^i and $\lambda_{\tau_k}^i$, $i \in \{1, ..., r-1\}$ are eigenvalues of Q_c and $Q(\tau_k)$, respectively, *i.e.*, $\lambda_c^i = \tau_k \lambda_{\tau_k}^i$. Because of the special form of Q_c (all diagonal entries are constant), the λ_c^i are constant and independent of τ_k. Thus, $\lambda_{\tau_k}^i \propto \frac{1}{\tau_k}$ which proves II.

Now suppose k_λ is chosen such that $\lambda_c^i \leq k_\lambda^{(2)}$, as a result, we have $\tau_k \lambda_{\tau_k}^i \leq k_\lambda^{(2)}$ which implies III.

Part IV follows from II when $\lambda_{\tau_k}^i = \frac{\lambda_c^i}{\tau_k}$. □

Remark 5.1. *The concept of time-varying zero-dynamics is studied in [99, 100, 101]. One realization of this approach happens when a sampled-data system is implemented using an event-triggered mechanism which then results in time-varying behaviour and variable induced sampling zeros. Our interest is to exploit this property to eliminate the impact of ZDAs.*

Suppose $|\lambda_{\tau_0}^j|$ represents the largest absolute value of the eigenvalues of $Q(\tau_0)$ in (5.4), *i.e.* $|\lambda_{\tau_0}^i| \leq |\lambda_{\tau_0}^j|$ for $\lambda_{\tau_0}^i$ $i \in \{1, ..., r-1\}$ at $\tau_0 = t_0$. Then according to the result in Lemma 5.1 part IV, the following time-varying scalar system represents the most unstable mode of the extrinsic zero-dynamics (5.4) in all $k \in \mathbb{N}^0$:

$$\delta\bar{\eta}_k = \bar{\lambda}_{\tau_k} \bar{\eta}_k. \tag{5.5}$$

where $\bar{\lambda}_{\tau_k} := \lambda_{\tau_k}^j$. In the sequel, we will use the location of this mode in our derivation.

With respect to Definition 2.5 and (2.6), a trivial solution to mitigate the impact of ZDA is to discretize the system using a sufficiently large sampling period, *i.e.* $h \to \infty$, which may then render stable eigenvalues for Q in (5.4), resulting in minimum-phase sampling zeros. This approach, however, is not adequate since it forces the use of very low sampling rates, resulting in poor performance with large inter-sample ripple and possible aliasing effect (see for example [95, Example 8.4.2]). Since the location of the sampling zeros depends on the time period between samples h, a non-constant sampling rate may offer the possibility to enforce minimum-phase zero-dynamics, thus rendering ZDAs ineffective.

It is worth mentioning that to carry out a ZDA, the attacker must possess system knowledge and disruption resources including the system model, event-triggering mechanism, and access to the controller-actuator communication channel, [30]. Additionally, even in the presence of system model uncertainty, a robust ZDA technique, is discussed in [43].

Remark 5.2. *We assume that the adversary has full system knowledge, including plant dynamics and event-triggering rule. Therefore, the available event-triggered mechanisms such as [88], [63] cannot guarantee resiliency for the system. The reason is that although these methods originate time-varying sampling zeros, the triggering rule is not explicitly designed to stabilize the extrinsic zero-dynamics and may result in divergent internal states in the presence of ZDA. A new triggering condition is required that takes into account changes in sampling zeros.*

5.1.1 Event-Triggered Mechanism

Let t_k, be the most recent sampling instant. The control signal is updated again at t_{k+1} according to the following rule:

$$t_{k+1}=\inf\{t\geq t_k+\tau\colon |e|>\sigma\alpha(|y|)+\theta|\widetilde{\eta}|\}, \tag{5.6}$$

where $\sigma,\ \theta\in\mathbb{R}_{>0}$, $\alpha\in\mathcal{K}_\infty$, $\tau\in\mathbb{R}_{>0}$ is the minimum inter-event time, and $\widetilde{\eta}$ is the solution of the following differential equation for $t\in[t_k, t_{k+1})$:

$$\dot{\widetilde{\eta}} = \hat{\lambda}_{\tau_k}\widetilde{\eta} + \sigma\alpha(|y|) - |e. \tag{5.7}$$

Moreover, $\hat{\eta}$ is the solution of a continuous-time counterpart of the time-varying discrete-time dynamics (5.5), *i.e.*,

$$\dot{\hat{\eta}} = \hat{\lambda}_{\tau_k}\hat{\eta}, \tag{5.8}$$

where $\hat{\lambda}$ is the counterpart of $\bar{\lambda}$ in the continuous-time framework. In the rest of the chapter, $\hat{\eta}$ and $\widetilde{\eta}$ are referred to as the *internal state* and *auxiliary state*, respectively. Moreover, we define I_k as the inter-event time interval $[t_{k-1}, t_k)$, and assume $I_k<\infty$. In addition, the set of all triggered instants t_k is denoted by S_{ev}.

It is worth mentioning that the idea behind using the triggering policy (5.6) is to add a sense of zero-dynamics (5.4) to the triggering threshold. In this way, undamped deviations of $\hat{\eta}$ lead to an increase of the inter-event time τ_k, *i.e.*, $\tau_k<\tau_{k+1}$ which results in $\hat{\lambda}_{\tau_{k+1}}<\hat{\lambda}_{\tau_k}$ and has the effect of bounding the extrinsic zero-dynamics (5.4) due to the connection between $\hat{\eta}$ in (5.8) and η in (5.4) *via* (5.5).

5.1.2 Main Problem

We can now state the main problem to be solved. Our goal is to lead the internal dynamics of a nonlinear system under ZDAs to a stable region by using the event-triggered sampling approach. To this end, we formulate a stabilization problem to obtain the design parameters σ, θ, τ, and $\alpha(.)$

such that the event-based control u with triggering condition (5.6), guarantees asymptotic stability of the system (5.1) while neutralizes the ZDAs.

5.2 Preliminary Results

We start with the following lemma where we obtain a relationship between the inter-event times τ_k and the error e defined in (5.2). The result will be employed to analyze the stability of the system under the event-triggered condition (5.6) in the next section.

Lemma 5.2. *Consider the nonlinear system* (5.1) *under the proposed triggering policy* (5.6)*. For any* $\delta\in\mathbb{R}_{>0}$*, there exist positive constants* τ*,* σ*,* M_δ*, and* M_y *such that the inter-event time* τ_k *is lower bounded by the following inequality for any* $\hat{\eta}_0\in\mathbb{R}$*, and* $\widetilde{\eta}_0\geq 0$

$$\tau_k \geq \frac{1}{\beta_m}\ln\left(c_1|e|+c_2\right), \tag{5.9}$$

if $x\in B(\delta)$*,* $\frac{\partial\alpha}{\partial|h(x)|}\left|\frac{\partial h(x)}{\partial x}\right||x|\leq M_\delta$*, and* $|h(x)|\leq M_y$*,*

where $c_1=\frac{\beta_1}{k_2\beta_1+k}$*,* $c_2=\frac{k}{\beta_1 k_2+k}$*,* $\beta_1=2L_gL_\psi M_\delta$*,* $\beta_2=\widetilde{\lambda}_\tau$*,* $\beta_m=max\{\beta_1,\beta_2\}$*,* $k=\sigma L_f L_g L_\psi M_\delta M_y$*,* $k_1=\theta\widetilde{\eta}_0$*, and* $k_2=\frac{k_1}{|\beta_2-\beta_1|}$*.*

Proof. The triggering condition (5.6) is satisfied at the event instant so that at t_k we have $|e|=\sigma\alpha(|y|)+\theta|\widetilde{\eta}|$, therefore, the derivative of $|e|$ is as follows:

$$\dot{|e|}=\sigma\frac{\partial\alpha}{\partial|y|}\dot{|y|}+\theta\dot{|\widetilde{\eta}|} \tag{5.10}$$

$$\dot{|y|} \leq |\frac{\partial h}{\partial x}||x|\left(L_f+L_gL_\psi|y_{t_k}|+2L_gL_\psi|e|\right). \tag{5.11}$$

Inequality (5.11) follows from Lipschitz property of f,g,ψ, and h in (5.1). Substituting (5.11) into (5.10) we obtain:

$$\begin{aligned}|\dot{e}| \leq{}& \sigma\frac{\partial\alpha}{\partial|y|}L_f|x|+\sigma\frac{\partial\alpha}{\partial|y|}|x|L_gL_\psi\,|y_{t_k}|\left|\frac{\partial h}{\partial x}\right| \\ &+2\sigma\frac{\partial\alpha}{\partial|y|}|x|L_gL_\psi\left|\frac{\partial h}{\delta x}\right||e|+\theta\dot{|\widetilde{\eta}|}.\end{aligned} \tag{5.12}$$

Since $|x|\leq B(\delta)$, we can find positive values for M_δ and M_y such that $\frac{\partial\alpha}{\partial|y|}\left|\frac{\partial h}{\partial x}\right||x|\leq M_\delta$ and $|y|\leq M_y$. Substituting these conditions into (5.12), we have:

$$\dot{|e|} \leq k+2L_gL_\psi M_\delta|e|+\theta\dot{|\widetilde{\eta}|}. \tag{5.13}$$

Further, by substituting $|e|$ into (5.7) and then the result into (5.13) we have:

$$\dot{|e|} \leq k + 2L_g L_\psi M_\delta |e| + \theta \hat{\eta}_0 e^{\hat{\lambda}(\tau)t}, \tag{5.14}$$

where (5.14) follows from the positivity of $\widetilde{\eta}$ and the result of part II in Lemma 5.1. Solving the differential inequality (5.14) with respect to $|e|$, we obtain:

$$|e| \leq \frac{k_1}{\beta_2 - \beta_1} e^{\beta_m \tau_k} + \frac{k}{\beta_1} \left(e^{\beta_m \tau_k} - 1 \right). \tag{5.15}$$

Finally, inequality (5.15) justifies the relationship (5.9) between inter-event time τ_k and error $|e|$. □

Remark 5.3. *Notice that when the error e is negligible, the event-triggering rule does not generate new events, thus there is no transmission of information through the network. Therefore, using a lower bound for inter-event period τ_k is unessential. However, for large values of $|e|$, the traditional triggering condition provides a high average rate for events to ensure that e converges as soon as possible. In this case, having a lower bound on the inter-event period is vital to adjust the triggering instants and avoid undamped sampling zeros. Inequality* (5.9)*, indeed, justifies the aforementioned observation in our approach when the lower bound on the inter-event period τ_k is tuned based on the value of e using the proposed triggering rule* (5.6)*.*

We now present several lemmas and definitions that we'll be needed in the next section.

Lemma 5.3. *Given a function $f{:}[t_k, t_{k+1}) \to \mathbb{R}_{\geq 0}$, we can find a constant $M_l > 0$ such that the following inequality holds.*

$$M_l f(t) \leq \ln(f(t) + 1) \leq f(t). \tag{5.16}$$

Proof. Using the definition of the logarithmic functions we can verify the RHS inequality in (5.16) as follows.

$$\ln(f(t) + 1) = \int_0^{f(t)} \frac{dr}{r + 1} \leq \int_0^{f(t)} \frac{dr}{1} = f(t).$$

The LHS of inequality (5.16) is valid for some $M_l > 0$ because the function $f(t)$ is defined over a limited time interval $[t_k, t_{k+1})$. □

Lemma 5.4. *There exist some $r_\lambda, k_\lambda^{(1)}, t_\lambda \in \mathbb{R}_{>0}$ such that the following inequality holds for chi-squared distribution with $\kappa = 4$ in $0 < t \leq t_\lambda$.*

$$e^{-\frac{1}{2}\ln^2(\frac{k_\lambda^{(1)}}{t})} \leq r_\lambda \left(\frac{t}{k_\lambda^{(1)}} \right)^{(\frac{\kappa}{2} - 1)} e^{-\frac{1}{2}\left(\frac{t}{k_\lambda^{(1)}}\right)} \tag{5.17}$$

Proof. Let $f_\lambda(t)=\frac{f_n(t)}{f_d(t)}$ where it is a continuous function over $0<t\leq t_\lambda$, and f_n and f_d correspond to LHS and RHS of (10), respectively, *i.e.*,

$$f_n(t) = e^{-\frac{1}{2}\ln^2(\frac{k_\lambda^{(1)}}{t})}, \quad f_d(t) = \left(\frac{t}{k_\lambda^{(1)}}\right) e^{-\frac{1}{2}\left(\frac{t}{k_\lambda^{(1)}}\right)}.$$

To validate (5.17) one just needs to show that there exist at least one maxima for f_λ over $0<t\leq t_\lambda$. In this regard the derivative of f_λ is obtained as follows.

$$f'_\lambda(t) = e^{-\frac{1}{2}\ln^2(\frac{k_\lambda^{(1)}}{t})+\frac{1}{2}\left(\frac{t}{k_\lambda^{(1)}}\right)} \times \left(\frac{k_\lambda^{(1)}\ln(\frac{k_\lambda^{(1)}}{t}) - k_\lambda^{(1)} + \frac{1}{2}t}{t^2}\right),$$

where it has two roots in $0<t\leq t_\lambda$ (associated with the maxima and the minima of f_λ). By choosing appropriate $k_\lambda^{(1)}$, the biggest root of f'_λ can be placed on t_λ, therefore, only one maximum is possible for f_λ over $0<t\leq t_\lambda$ which then verifies (5.17). □

Definition 5.2 (*Hermite-Hadamard inequality*)**.** *Let $f:[a,b]\to\mathbb{R}$ be a convex function. Then*

$$f\left(\frac{\tau+t}{2}\right) \leq \frac{1}{t-\tau}\int_\tau^t f(u)du \leq \frac{f(\tau)+f(t)}{2}. \tag{5.18}$$

5.3 Main Results

In this section, we firstly investigate the Lyapunov stability of the nonlinear system (5.1) under the triggering rule (5.6). Then, we study the boundedness of the extrinsic zero-dynamics states (5.4) induced by the sampling zeros under the proposed method.

Theorem 5.1. *The nonlinear system* (5.1) *with the event-triggering policy* (5.6) *is asymptotically stable if for any $\varepsilon>0$ where $x_0\in B(\varepsilon)$, there exist some positive constants τ, σ, M_l, and function α satisfying the following inequalities for all $x\in\mathbb{R}^n$.*

$$\nu(|x|)>\gamma(\mu_2\alpha(|h(x)|)+\mu) \tag{5.19a}$$

$$\frac{\mu_3}{\mu_2}\leq\frac{\mu_4+\mu_1^2}{2\mu_2} \tag{5.19b}$$

where $\mu = \mu_1 + \mu_1^2 + \mu_4$ and

$$\mu_1 = \frac{1 + h_7 - l_2}{h_8 - l_3 - \frac{1}{2}l_5}, \quad \mu_2 = \frac{l_5}{2h_8 - 2l_3 - l_5}$$
$$\mu_3 = \frac{l_4}{h_8 - l_3 - \frac{1}{2}l_5}, \quad \mu_4 = \frac{l_1}{h_8 - l_3 - \frac{1}{2}l_5}$$

$$\begin{aligned}
&h_1(y_\tau) = e^{\frac{1}{2}\ln^2(\frac{k_\lambda}{\tau})}\sigma\alpha(|y(\tau)|)\\
&l_1 = \widetilde{\eta}_0 r_\lambda \Gamma_2 + \widetilde{\eta}_0 h_1(y_\tau)\Gamma_2\Gamma_4\\
&l_2 = \widetilde{\eta}_0 r_\lambda \Gamma_1 + \widetilde{\eta}_0 h_1(y_\tau)(\Gamma_2\Gamma_3 + \Gamma_4^2)\\
&l_3 = \widetilde{\eta}_0 h_1(y_\tau)\Gamma_1\Gamma_3, \quad l_4 = \frac{\sigma}{2}\widetilde{\eta}_0\Gamma_4, \quad l_5 = \frac{\sigma}{2}\widetilde{\eta}_0\Gamma_3\\
&h_7 = M_l(\Gamma_4 - \tau), \quad h_8 = M_l\Gamma_3\\
&\Gamma_1 = \frac{k_1 k}{|\beta_2 - \beta_1|\beta_m k_\lambda \beta_1} e^{-\frac{1}{2\beta_m k_\lambda}\ln(\frac{k}{\beta_1})}\\
&\Gamma_2 = \frac{1}{\beta_m k_\lambda}\ln(\frac{k}{\beta_1}) e^{-\frac{1}{2\beta_m k_\lambda}\ln(\frac{k}{\beta_1})}\\
&\Gamma_3 = \frac{k_1 k}{|\beta_2 - \beta_1|\beta_m \beta_1}, \quad \Gamma_4 = \frac{1}{\beta_m}\ln(\frac{k}{\beta_1}),\\
&k_\lambda = \max\{k_\lambda^{(1)}, k_\lambda^{(2)}\}.
\end{aligned}$$

Proof. We proceed as follows: we depart from the ISS condition (5.3) and rewrite the error e in (5.3b) with some terms constructed based on the design parameters. As a result, constraints in (5.19) are obtained to preserve Lyapunov stability for the system (5.1) under the triggering condition (5.6). To this end, we begin by solving the auxiliary differential equation (5.7) which is then substituted in the event-triggered rule (5.6) to make a connection between the design parameters and the error e:

$$\begin{aligned}
\widetilde{\eta} = &\underbrace{e^{-\frac{1}{2}\ln^2(\frac{k_\lambda}{t})}}_{B} \times\\
&\left[\widetilde{\eta}_0 + \underbrace{\int_0^t e^{\frac{1}{2}\ln^2(\frac{k_\lambda}{\tau})}\sigma\alpha(|y|)d\tau}_{A} - \underbrace{\int_0^t e^{\frac{1}{2}\ln^2(\frac{k_\lambda}{\tau})}|e|d\tau}_{D}\right].
\end{aligned} \tag{5.20}$$

Re-writing A and D in (5.21) based on Hermite-Hadamard's relation, and re-stating B using the

results in Lemma 5.4, we obtain:

$$
\begin{aligned}
A &\leq \frac{(t-\tau)}{2}\left(e^{\frac{1}{2}\ln^2(\frac{k_\lambda}{t})}\sigma\alpha(|y(t)|)+e^{\frac{1}{2}\ln^2(\frac{k_\lambda}{\tau})}\sigma\alpha(|y(\tau)|)\right)\\
D &\geq (t-\tau)e^{\frac{1}{2}\ln^2(\frac{k_\lambda}{t+\tau})}\sigma\alpha(|e(t+\tau)|)\\
B &\leq r_\lambda\left(\frac{t}{k_\lambda}\right)e^{-\frac{1}{2}\left(\frac{t}{k_\lambda}\right)}.
\end{aligned}
\tag{5.21}
$$

Moreover,

$$
\begin{aligned}
B\times D &\geq \underbrace{e^{-\frac{1}{2}\ln^2(\frac{k_\lambda}{t})}e^{-\frac{1}{2}\ln^2(\frac{k_\lambda}{t+\tau})}}_{(*)}|e|(t-\tau)\\
&\geq |e|(t-\tau),
\end{aligned}
\tag{5.22}
$$

where the last inequality in (5.22) follows by the fact that $(*)\geq 1$. Substituting (5.21) and (5.22) into (5.20) we have:

$$
\begin{aligned}
\widetilde{\eta} &\leq r_\lambda\widetilde{\eta}_0\left(\frac{t}{k_\lambda}\right)e^{-\frac{1}{2}\left(\frac{t}{k_\lambda}\right)}+\widetilde{\eta}_0\frac{(t-\tau)}{2}\sigma^2\alpha(|y|)\\
&\quad+\frac{(t-\tau)}{2}h_1\left(y_\tau\right)r_\lambda\widetilde{\eta}_0\left(\frac{t}{k_\lambda}\right)e^{-\frac{1}{2}\left(\frac{t}{k_\lambda}\right)}-|e|(t-\tau),
\end{aligned}
\tag{5.23}
$$

where

$$
\begin{aligned}
&\left(\frac{t}{k_\lambda}\right)e^{-\frac{1}{2}\left(\frac{t}{k_\lambda}\right)}=\frac{1}{\beta_m k_\lambda}\ln(c_1|e|+c_2)e^{-\frac{1}{2\beta_m k_\lambda}\ln(c_1|e|+c_2)}\\
&\leq\left(\frac{1}{\beta_m k_\lambda}\ln(c_2)+\frac{c_1}{\beta_m k_\lambda c_2}|e|\right)e^{-\frac{1}{2\beta_m k_\lambda}\ln(c_2)}.
\end{aligned}
\tag{5.24}
$$

Inequality (5.24) is obtained using (5.9) together with the inequalities (5.16) and $e^{-\frac{1}{2\beta_m k_\lambda}\ln(1+\frac{c_1}{c_2}|e|)}\leq 1$.

In addition, considering inequalities (5.9) and (5.16), the following relation holds for inter-event time τ_k.

$$
\begin{aligned}
|e|(t-\tau)&\geq|e|\left(\frac{1}{\beta_m}\ln\left(c_1|e|+c_2\right)-\tau\right)\\
&\geq h_7|e|+h_8|e|^2.
\end{aligned}
\tag{5.25}
$$

Substituting (5.24) and (5.25) into (5.23), we obtain the following inequality for $\widetilde{\eta}$:

$$\begin{aligned}\widetilde{\eta} \leq\ & l_1 + (l_2 - l_7)|e| + (l_3 - l_8)|e|^2 \\ & + l_4\alpha(|y|) + l_5|e|\alpha(|y|).\end{aligned} \tag{5.26}$$

Substitute (5.26) into the triggering condition (5.6), we have:

$$\begin{aligned}|e| \leq\ & \sigma\alpha(|y|) + l_1 + (l_2 - l_7)|e| \\ & + (l_3 - l_8)|e|^2 + l_4\alpha(|y|) + l_5|e|\alpha(|y|) \\ & \leq l_1 + (l_2 - h_7)|e| + (l_3 + \frac{1}{2}l_5 - h_8)|e|^2 \\ & + (l_4 + \sigma)\alpha(|y|) + \frac{1}{2}l_5\alpha^2(|y|),\end{aligned} \tag{5.27}$$

where the last inequality of (5.27) follows from the relation $|e|\alpha(|y|) \leq \frac{1}{2}|e|^2 + \frac{1}{2}\alpha^2(|y|)$ which is obtained using young's inequality. Consequently, rearranging (5.27), we obtain:

$$|e|^2 + \mu_1\frac{1}{2}|e| \leq \mu_2\alpha^2(|y|) + \mu_3\alpha(|y|) + \mu_4. \tag{5.28}$$

Adding μ_1 to both sides of (5.28), we have:

$$\begin{aligned}(|e| - \mu_1)^2 &\leq |e|^2 + \mu_1|e| + \mu_1^2 \\ &\leq \mu_2\left(\alpha^2(|y|) + \frac{\mu_3}{\mu_2}\alpha(|y|) + \frac{\mu_4 + \mu_1^2}{\mu_2}\right).\end{aligned} \tag{5.29}$$

Since $\frac{\mu_4+\mu_1^2}{2\mu_2} \geq \frac{\mu_3}{\mu_2}$ holds with respect to condition (5.19b), based on (5.29), we obtain:

$$|e| \leq \mu_2\alpha(|y|) + \mu. \tag{5.30}$$

Substituting (5.30) into (5.3b), we have:

$$\dot{V}(x) \leq -\nu(|x|) + \gamma(\mu_2\alpha(|h(x)|) + \mu). \tag{5.31}$$

Finally, since condition (5.19a) holds, the RHS of (5.31) is negative, and the result follows. □

We now turn our attention to the zero dynamics. In the next theorem we obtain conditions such that the auxiliary state $\widetilde{\eta}$ and internal state $\hat{\eta}$ remain bounded, thus resulting in bounded behaviour for all modes in extrinsic zero-dynamics (5.4). This dynamics is time-varying, due to the variable sampling zeros induced by the event-triggered mechanism. Therefore, the following analysis is cast as a piecewise linear system and uses elements from the theory of switching systems.

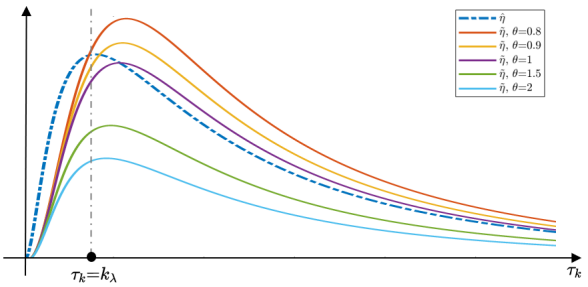

Figure 5.2: The shape of trajectories $\hat{\eta}$ and $\widetilde{\eta}$ at constant time t with respect to $\tau_k \in [t_k, t)$ for different values of θ.

Lemma 5.5. *Consider the solution of systems* (5.7) *and* (5.8) *starting at* t_k*, and let* $max\{\hat{\eta}(t)\}=\hat{\eta}(\hat{t}_m)$ *and* $max\{\widetilde{\eta}(t)\}=\widetilde{\eta}(\widetilde{t}_m)$*. There exist some* $\theta \in \mathbb{R}_{>0}$ *such that.*

$$\hat{t}_m \leq \widetilde{t}_m. \tag{5.32}$$

Proof. Consider the differential equation (5.7). Consider first the case when $\sigma\alpha(|y|)=0$. At event instant t_k we have $|e(t)|=\theta|\widetilde{\eta}|$ and $\hat{\eta}=e^{-\frac{1}{2}\ln^2(\frac{k_\lambda}{\tau_k})}\hat{\eta}_{t_k}$, which results in $\dot{\widetilde{\eta}}=\frac{1}{\tau_k}\ln(\frac{k_\lambda}{\tau_k})e^{-\frac{1}{2}\ln^2(\frac{k_\lambda}{\tau_k})}\hat{\eta}_{t_k}-\theta|\widetilde{\eta}|$ and can be solved numerically. Figure 5.2 shows the trajectories of $\widetilde{\eta}$ and $\hat{\eta}$, with respect to τ_k for different values of θ. According to Fig. 5.2, the maxima of $\hat{\eta}$ can happen at $\tau_k=k_\lambda$, while, the maxima of $\widetilde{\eta}$ depends on k_λ as well as θ. Consequently, by choosing an appropriate θ the time instant $\widetilde{t}_m$ always happens with a lag $\hat{t}_m$, *i.e.*, $\hat{t}_m \leq \widetilde{t}_m$. For a case when $\sigma\alpha(|y|)\neq 0$, the positive term $\sigma\alpha(|y|)$ causes additional lag for $\widetilde{t}_m$ with respect to $\hat{t}_m$. Thus inequality (5.32) is also valid in this case. □

Remark 5.4. *Regarding the result in Lemma 5.5,* $\widetilde{\eta}$ *follows any increase/decrease of* $\hat{\eta}$*. Therefore, the term* $\theta|\widetilde{\eta}|$ *in the RHS of the triggering rule* (5.6) *can be used to monitor the oscillation of the extrinsic zero-dynamics* (5.4)*. Moreover, doing so allows us to employ* $\widetilde{\eta}$ *in the rest of the derivation to evaluate the bounded property of zero-dynamics.*

Theorem 5.2. *If the parameter* $\theta \in \mathbb{R}_{>0}$ *is chosen such that the inequality* (5.32) *is satisfied, then the extrinsic zero-dynamics* (5.4) *is bounded under the event-triggering rule* (5.6)*.*

The proof of Theorem 5.2 requires some preliminary steps. We first investigate the boundedness property of the switching system (5.7). In order to determine the overall convergence rate for the switching system (5.7) we must examine the relationship between the trajectory of $\widetilde{\eta}$ and the event-triggering condition (5.6) in each interval I_k. To this end, we denote $r_k>0$ ($r_k \leq 0$) as the divergence (convergence) rate of the unstable (stable) mode of (5.7) in the time interval I_k, *i.e.*, $r_k=\frac{\widetilde{\eta}_{t_k}-\widetilde{\eta}_{t_{k-1}}}{\tau_k}$.

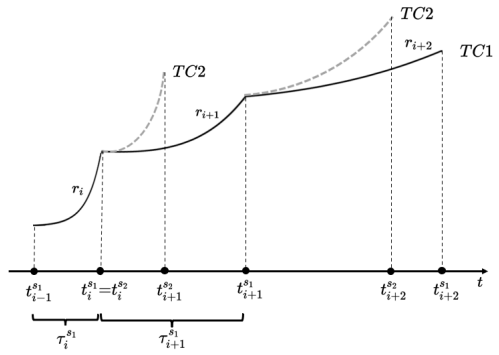

Figure 5.3: A schematic of $\widetilde{\eta}$'s trajectory under two triggering conditions (5.34)

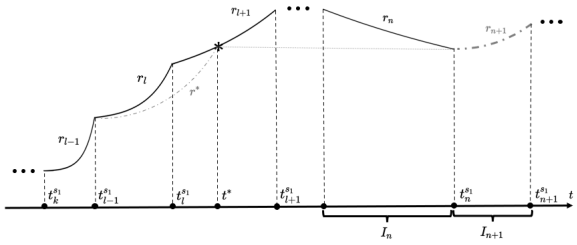

Figure 5.4: A schematic of $\widetilde{\eta}$'s trajectory under the proposed method

Proposition 5.1. *Consider an arbitrary interval* $I_k{=}[t_{k-1}, t_k)$ *and assume in this interval the system* (5.7) *has an unstable mode with the divergence rate* r_k*. Then, under the triggering condition* (5.6) *we have that* $r_k{\leq}r_j$ *for* $j{\in}\mathbb{N}_{<k}$.

Proof. A schematic of Proposition 5.1 is shown in Fig. 5.3 and 5.4. The proof consist of two parts: ***First***, suppose all modes of (5.7) in some consecutive time intervals, $\{I_i, \cdots, I_k\}$, are unstable. Indeed, the divergence rate of trajectory $\widetilde{\eta}$ associated to $\{I_i, \cdots, I_k\}$, has positive values $\{r_i, \cdots, r_k\}$. We now show that the following inequality holds.

$$r_k{\leq}r_{k-1}{\leq}\cdots{\leq}r_i. \tag{5.33}$$

Our proof is based on an iterative procedure and the comparison lemma. Consider the system in Fig. 5.1 under two different triggering conditions.

$$\begin{aligned} &\text{TC1: } |e|{>}\sigma\alpha(|y|){+}\theta|\widetilde{\eta}| \\ &\text{TC2: } |e|{>}\sigma\alpha(|y|) + M_{i+1}, \end{aligned} \tag{5.34}$$

where $M_{i+1}{\geq}0$ is a constant. Suppose $t_j^{s_1}$ and $t_j^{s_2}$ for $j{\in}\{i, \cdots, k\}$ represent the triggering instants

in TC1 and TC2 with M_i=0. Let $\tau_j^{s_1}$=$t_j^{s_1}$−$t_{j-1}^{s_1}$ denote the inter-event period for TC1. Consider now the trajectories starting at t=t_{i-1}^{s1} for both triggering conditions. The next event under both triggering condition TC1 and TC2 is triggered at the same time, *i.e.* $t_i^{s_1}$=$t_i^{s_2}$=$t_{i-1}^{s_1}$+$\tau_i^{s_1}$ as shown in Fig. 5.3. Now if the next event instant in TC2 takes place when $t_{i+1}^{s_2}$=$t_{i-1}^{s_1}$+2τ_i^{s1}, we have, $|e|$=$\sigma\alpha(|y|)$ at $t_{i+1}^{s_2}$. Since the system is the same, the error at t=$t_{i-1}^{s_1}$+2$\tau_i^{s_1}$ is same for both TC1 and TC2. Substituting $|e|$=$\sigma\alpha(|y|)$ in TC1, we obtain $\sigma\alpha(|y|)$>$\sigma\alpha(|y|)$+$\theta|\widetilde{\eta}|$ which is not valid. Therefore, $t_{i+1}^{s_1}$>$t_{i-1}^{s_1}$+2$\tau_i^{s_1}$ which results in r_{i+1}<r_i.

Now we add the positive term M_{i+1}:=$\theta|\widetilde{\eta}|_{|t=t_{i+1}^{s1}}$ in the RHS of TC2 so that $t_{i+1}^{s_2}$=$t_{i+1}^{s_1}$. Following the previous steps for the interval I_{i+2} with the modified triggering condition TC2 given by:

$$\text{TC2: } |e(t)|>\sigma\alpha(|y|) + M_{i+1}.$$

we have the following: If we assume that $t_{i+2}^{s_2}$=$t_{i+1}^{s_2}$+$\tau_{i+1}^{s_1}$, then $|e|$=$\sigma\alpha(|y|)$+M_{i+1} at $t_{i+2}^{s_2}$, and as a result, we have $\sigma\alpha(|y|)$+M_{i+1}≥$\sigma\alpha(|y|)$+$\theta|\widetilde{\eta}|$ for TC1 at t_{i+2}^{s2}. Since we assume r_{i+1} is positive, $\theta|\widetilde{\eta}|$≥M_{i+1} in interval I_{i+2}. Therefore, TC1 is not violated at $t_{i+2}^{s_2}$ and we have $t_{i+2}^{s_1}$>$t_{i+1}^{s_1}$+$\tau_{i+1}^{s_1}$, as a result r_{i+2}<r_{i+1}. Therefore, iterating the procedure for I_j, j∈{i+3, ⋯ , k}, inequality (5.33) is verified.

Second, suppose that in an arbitrary time interval I_n, the switched system (5.7) has a stable mode as shown in Fig. 5.4, *i.e*, r_n≤0. We claim that under the triggering condition (5.6), r_{n+1} can not be arbitrary, and it is limited by r_i, i∈$\mathbb{N}_{<n}$. The proof is as follows:

Define M_n:=$\theta|\widetilde{\eta}|_{t=t_n^{s1}}$. Since r_n≤0, there exist some t^*∈$[0, t_n^{s1})$ such that $\theta|\widetilde{\eta}|_{t=t^*}$=$M_n$, and let t^*∈$[t_l^{s1}, t_{l+1}^{s1})$ where t_l^{s1},t_{l+1}^{s1}∈S_{ev}. Suppose t^* is also an event instant for the same system under the triggering condition {TC2: $|e(t)|$>$\sigma\alpha(|y|)$+M_{l-1}} in associated time interval t∈$[t_{l-1}^{s1}, t^*)$, and let r^* be the divergence rate of the corresponding trajectory. According to the first part, starting from t_n^{s1}, the next event for TC1 with the initial triggering threshold $\sigma\alpha(|y|)$+M_{l-1} occurs at t_{n+1}^{s1} when t_{n+1}^{s1}−t_n^{s1}≥t^*−t_{l-1}^{s1}. Thus, the possible divergence rate in this interval satisfies r_{n+1}<r^*. On the other hand, since interval $[t_{l-1}^{s1}, t^*)$≥$[t_{l-1}^{s1}, t_l^{s1})$, therefore, r^*≤r_l which results in r_{n+1}<r_l. Consequently, any possible positive r_{n+1} is bounded from the above by the divergence rates of the past unstable modes. □

Remark 5.5. *Proposition 5.1 gives insight into the behaviour of the time-varying zero-dynamics* (5.7) *in any arbitrary interval with respect to the inter-event period* τ_k. *This observation can be employed to analyze the boundedness property of zero-dynamics* (5.4).

Proposition 5.2. *Let* N_{S_m} *be the number of switching instants for* $\widetilde{\eta}$ *over the time interval sequence* S_m={$I_k, \cdots, I_n$} *with associate modes* {$\lambda_k, ..., \lambda_n$}., *and let* $T_{S_m}^-$, $T_{S_m}^+$, $\lambda_{S_m}^-$, *and* $\lambda_{S_m}^+$ *be the total activation time of the stable and unstable subsystems, and the largest negative and positive modes of* (5.7) *in* S_m, *respectively. Then, there exist constants* h *and* β *such that the following conditions*

hold for any $m\in\mathbb{N}$.

$$\lambda^{+}_{S_m} T^{+}_{S_m} - \lambda^{-}_{S_m} T^{-}_{S_m} \leq h \tag{5.35a}$$

$$N_{S_m} \leq \beta. \tag{5.35b}$$

Proof. According to the first part of Proposition 5.1, S_m includes some consecutive unstable modes together with at least one stable mode. Since $\tau_k<\infty$, $T^{+}_{S_m}$ and $T^{-}_{S_m}$ are both finite, which justify (5.35a) for the sequence S_m. Moreover, because of the existence of τ the minimum inter-event time, the total number of switching instants over the sequence S_m can not exceed $\frac{S_m}{\tau}$, which guarantees that (5.35b) holds. Furthermore, based on results of the second part of Proposition 5.1, the divergence rates of the unstable modes in the next time section S_i, $i> m$, must be smaller than the divergence rates of the unstable modes in S_m, which verifies conditions (5.35) over any S_i, $i\in\mathbb{N}_{>m}$. □

Proof of Theorem 5.2. According to Propositions 5.1 and 5.2, the auxiliary dynamic (5.7) is time-varying based on the interval between events τ_k. Therefore, it can be viewed as a switched system with stable and unstable modes. Now with respect to [87, Theorem 1], the stability condition for (5.7) in any section of time S_m is as follows.

$$|\widetilde{\eta}|\leq c e^{aN_{S_m}} e^{(\lambda^{+}_{S_m} T^{+}_{S_m} - \lambda^{-}_{S_m} T^{-}_{S_m})} |\widetilde{\eta}_0|, \tag{5.36}$$

where a and c are constants. Substituting (5.35) into (5.36), RHS of (5.36) is bounded by a steady exponential term $ce^{a\beta}e^{h}|\widetilde{\eta}_0|$ which renders a bounded trajectory for the auxiliary state $\widetilde{\eta}$ over any time section S_m. Regarding Lemma 5.5; choosing an appropriate θ, the auxiliary state $\widetilde{\eta}$ follows any increase/decrease of the internal state $\hat{\eta}$, which results in a bounded trajectory for $\hat{\eta}$. Since $\hat{\eta}$ is the most unstable mode of the extrinsic zero-dynamics (5.4), it follows that, according to the results in part III and IV of Lemma 5.1, all modes of the extrinsic zero-dynamics, which are represented by (5.4), are forced to stay bounded the entire time. □

Remark 5.6. *According to the theorem 5.1, the event-triggered rule* (5.6) *provides the asymptotic stability of the closed loop system, satisfying the inequalities* (5.19a) *and* (5.19b)*. Therefore, with respect to the theorem 5.2, in order to eliminate the risk of ZDAs on the extrinsic zero dynamics, one needs to design the parameters in the event-triggering condition* (5.6) *ensuring that inequalities* (5.19) *and* (5.32) *are satisfied. Consequently, extrinsic zero dynamics states of the sampled-data system in Fig. 5.1 remain bounded and unsuitable for exploitation by an adversary for cyber-attack purposes.*

Remark 5.7. *It is worth mentioning that under the ZDAs, the term* $\widetilde{\eta}(t)$ *in* (5.6)*, which is closely tied up with* (5.4)*, prevents the event generator from having a high rate of average triggered instants.*

This condition results in enlarged enter-event intervals, which eventually dampen the extrinsic zero-dynamics (4) due to the inverse relation revealed in Lemma 5.1. This is the tool that we have developed to mitigate the extrinsic zero-dynamics (5.4)*, as proven in Theorem 5.2. As a side effect, it prevents the system from exhibiting Zeno behaviour under attack due to the induced large enter-event time* τ_k*.*

5.4 Case Study

To illustrate the effectiveness of the proposed approach, we consider a nonlinear benchmark plant, the single-link flexible-joint robot manipulator. The state-space representation of the robot is given by:

$$\begin{cases} \dot{x} = f(x) + g(x)u \\ y = x_1 \end{cases} \tag{5.37}$$

$$f(x)=\begin{bmatrix} x_2 \\ -\frac{MgL}{I}\sin(x_1) - \frac{k}{I}(x_1 - x_3) \\ x_4 \\ \frac{k}{J}(x_1 - x_3) \end{bmatrix}, \quad g(x)=\begin{bmatrix} 0 \\ 0 \\ 0 \\ \frac{1}{J} \end{bmatrix},$$

where $x=[x_1, x_2, x_3, x_4]^\intercal$. For a detailed description of the model the reader is referred to [97]. An observer-based LQR controller is designed based on linearized model of (5.37) to stabilize the nonlinear system around the operating point $[1.32, 0, 3.22, 0]$.

We now apply our proposed method. Choosing τ=0.06, σ=10, θ=0.1, α=$|y|$, and $\bar{\eta}_0$=0.1 with $\nu(|x|)$=$|x|$ and $\gamma(|e|)$=$|e|$ so that conditions in (5.19) and (5.32) are satisfied. It is easy to see that the relative degree of the system (5.37) is 4, the same as the number of states, *i.e.*, n=r=4. Therefore, the continuous-time system (5.37) is minimum-phase. However, a new non-minimum phase zero-dynamics appears induced by the sample and hold process with sampling time T=0.01s as follows:

$$\delta\eta_k=\begin{bmatrix} -400 & -1 & -0.008 \\ -12\times10^4 & -600 & -30 \\ -24\times10^6 & -12\times10^4 & -800 \end{bmatrix}\eta_k. \tag{5.38}$$

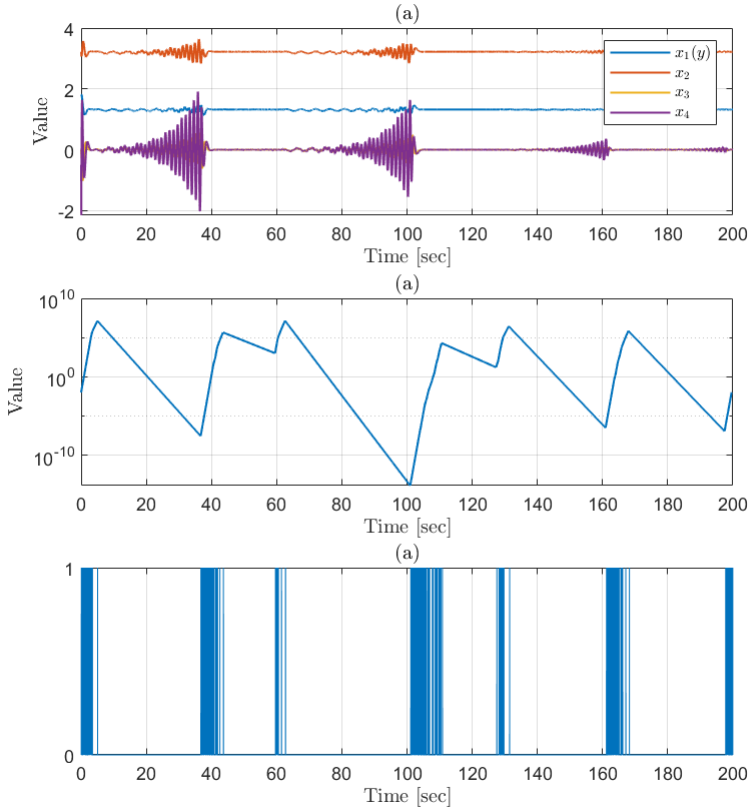

Figure 5.5: (a): States responses. (b): Trajectory of the sampling zero $\widetilde{\eta}$. (c): Events instants t_k under (5.6).

Consider now a ZDA generated based on the unstable zero-dynamics (5.38) and activated at t=0s when the initial condition of states is 10% deviated from the operating point. Figure 5.5-a shows the system response under the proposed method when it is exposed to the attack. We see that, although the system performance is degraded compared to normal situation, the controller, however, successfully neutralizes the attack gradually damping the deviations. The trajectory of $\hat{\eta}$, the most unstable mode of the extrinsic zero-dynamics, is shown in Fig. 5.5-b. To have a better view of the response, the plot is shown on a logarithmic scale. We observe that using the proposed triggering condition, the extrinsic zero-dynamics remains bounded. More precisely, the proposed method (5.6) takes care of the sampling zeros in such a way that whenever the trajectory in 5.5-b starts to deviate, intervals between events become longer, which can be seen in Fig. 5.5-c. Thus, the positive rates of (5.8) gradually decrease resulting in a stable mode for internal state $\hat{\eta}$.

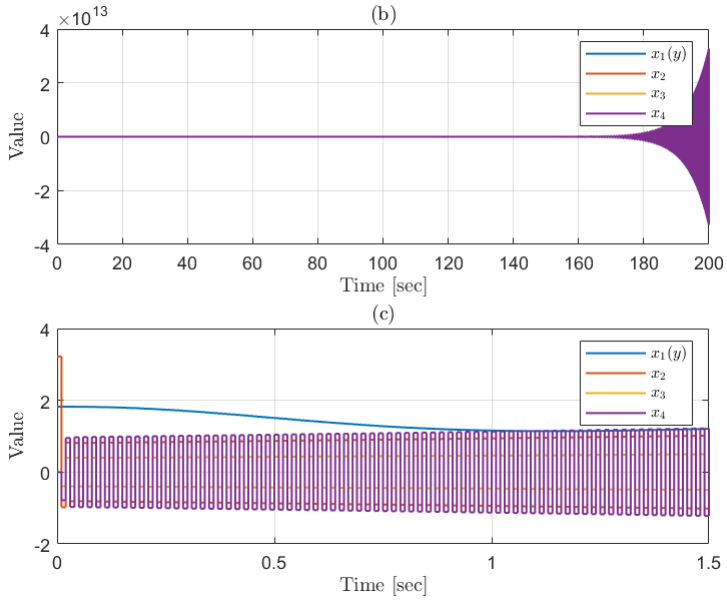

Figure 5.6: Trajectory of the states (a) and details (b).

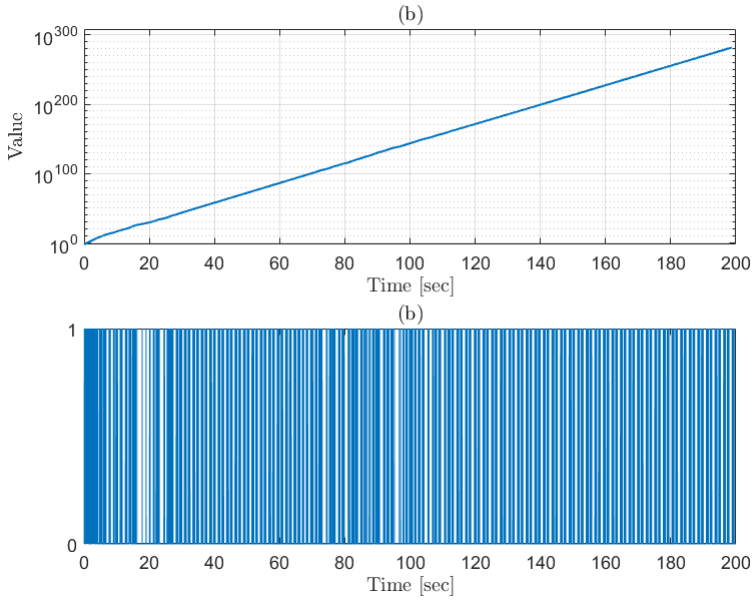

Figure 5.7: (a): Trajectory of the sampling zero $\hat{\eta}$. (b): Events instants t_k under (5.39).

For the purpose of comparison, we apply the following triggering rule to the same system:

$$t_{k+1}=\inf\{t>t_k+\tau:\ |e(t)|>\sigma\alpha(|y(t)|)\}. \tag{5.39}$$

The event-triggering condition (5.39) is the well established triggering rule proposed in [63] and employed in multiple studies in networked control systems. The main difference between (5.39) and (5.6) is that the former is developed based on the static relation of e and y in which the dynamic changes are absent. However in the latter, we deploy the deviation of the extrinsic zero-dynamics so that it can supervise not only e but also $\hat{\eta}$. Figure 5.6 shows the system response under the static triggering rule (5.39) when it is compromised by the ZDA. The simulation result reveals that the internal dynamic states x_2, x_3, x_4 become unbounded even though the exponential behaviour is not observed in y, as is characteristic of the stealthy property of the ZDA. As a result, although the deviation of the output y is compensated and settled on the operating point, the internal dynamics is unbounded. This failure reflects the fact that there is no control of the sampling zeros using the static event-based method (5.39). Indeed, according to Fig. 5.7, the lack of correlation between the event instants and the rate of the internal state's trajectory $\hat{\eta}$ in any sub-interval τ_k results in unbounded extrinsic zero-dynamics. This can be employed by an adversary to target the internal dynamics as illustrated in Fig. 5.6.

5.5 Summary

In this chapter, we have developed a resilient control scheme using event-triggered sampling for an affine class of nonlinear systems under ZDAs. Our approach can mitigate the malicious effect of the attacks and as a result significantly improve resilience against cyber threats. We show that the proposed event-based strategy can provide boundedness of the non-minimum phase extrinsic zero-dynamics induced by discretization while guaranteeing asymptotic stability of the overall system. Consequently, the sampled-data structure is no longer vulnerable to ZDAs.

Chapter 6

Model-Based Event-Triggered Control Against ZDAs

It is commonly recognized that a non-minimum phase system is vulnerable to undetectable cyber-attacks known as ZDAs. Interestingly, even though the physical plant is minimum-phase, high rate discretization can introduce non-minimum phase behaviour, increasing susceptibility to ZDAs in cyber-physical systems. This chapter presents an effective approach for addressing such a security issue. Our approach involves a novel inferential control setup activated at asynchronous sample instants, prompted by a well-designed model-based event triggering method. Rigorous analysis using switched system theory demonstrates that the proposed method can converge the zero-dynamics response to a safe region resulting in minimum-phase property while preserving overall Lyapunov stability, leading to a secure closed-loop structure under the attack. Simulation results confirm the effectiveness of the proposed design.

The chapter layout is as follows: In Section 6.1, we present the fundamental concepts and our proposed event-triggered structure used throughout the sequel. In Section 6.2 we provide several preliminary lemmas for sampling zeros and event-triggered sampling used in later sections. Section 6.3 contains the main results. Under the developed method, here we investigate the boundedness property of the zero-dynamics of a system exposed to attacks, as well as asymptotic stability of the overall system. Finally, in Section 6.4 we present a numerical example to show the effectiveness of our proposed approach.

6.1 Problem Statement

The feedback system in the chapter is illustrated in Fig. 6.1. It comprises of a digital control connected to the system output via a network. The event triggering block receives output measure-

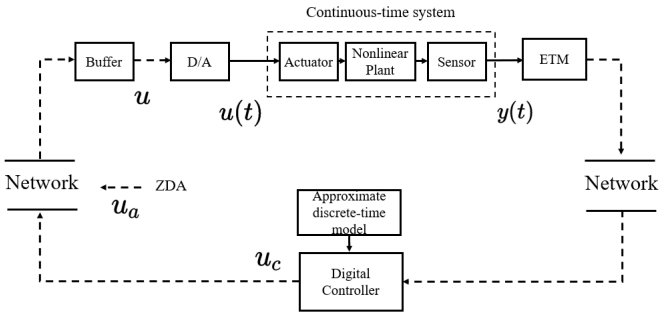

Figure 6.1: Block diagram of the closed-loop control system equipped with an event-triggered mechanism under ZDAs.

ments from the sensors and decides when to transfer information to the controller. The controller output is transmitted through the network and is received by the actuators after passing through the digital-to-analog converters. The plant is described by the following nonlinear model:

$$\dot{x}(t) = f(x(t)) + g(x(t))u(t), \quad y(t) = h(x(t)), \tag{6.1}$$

where $x \in \mathbb{R}^n$, $u, y \in \mathbb{R}$, and f, g, h are locally Lipschitz function, *i.e.*, $\exists\ \mathcal{L}_f$ such that for any x and $\widetilde{x}$ in a compact set X, $|f(x,u) - f(\widetilde{x},u)| \leq \mathcal{L}_f |(x - \widetilde{x})|$.

We denote F_T^e the exact discrete-time model of (6.1) with sampling period T, *i.e.*,

$$F_T^e : \{\delta x_k = f_e(x_k) + g_e(x_k)(u_c + u_z),\ y_k = h_e(x_k)\},$$

Here the exact discrete-time model F_T^e represents an ideal discretization that we assume is unknown. Notice that finding F_T^e requires solving the nonlinear differential equation (6.1) which, more often than not, does not have a closed form solution. In the absence of F_T^e, we consider an approximate discrete-time model, $F_{T,h}^a$, which can always be found using numerical integration techniques. To represent the deviation between the exact model and its approximation we assume that $F_{T,h}^a$ satisfies the following consistency properties defined in chapter 2.

Definition 6.1. *We denote $F_{T,h}^u$ the Euler discrete-time model of* (6.1) *with sampling period T for $k \in \mathbb{N}^0$, i.e.,*

$$F_T^u : \{\delta x_k = f(x_k) + g(x_k)u_k,\ y_k = h(x_k)\},$$

Remark 6.1. *Even though F_T^e is unknown, we can check whether or not the approximate model satisfies definition 2.2 or 2.3 using the following sufficient conditions.*

(i) If $F_{T,h}^a$ is locally Lipschitz uniformly in u_T and $F_{T,h}^a$ is one step consistent with the Euler approximation F_T^u, then $F_{T,h}^a$ is one step consistent with F_T^e (see [78, Lemma 1]).

(ii) In general one-step consistency and multi-step consistency does not imply each other. However, if $f(x)$, $g(x)$ and $u_T(x)$ are locally Lipschitz, there exist $K{\in}\mathbb{R}_{>0}$ and $T^*{>}0$ such that for any $0{<}T{<}T^*$, $\alpha(\delta,T){=}(1{+}KT)\delta{+}T\rho(h)$ (see [78, Remark 2] together with [78, Lemma 3]).

6.1.1 Event-Based Inferential Control Setup

The inferential control u_c in (6.1) is implemented using a so-called event-based method. In this approach, information is only exchanged between the sensor and the controller at specific triggering instances $\{t_i\}, i{\in}\mathbb{N}$, following the occurrence on an event. When an event occurs at t_i, the state $x(t_i)$ is transmitted over the network and received by the controller. The controller then uses a discrete-time approximation $F^a_{T,h}$ of the plant model (6.1) to calculate the predicted output y_a given by:

$$y_a(t_i{+}nT){=}\begin{cases} h_a(x(t_i)), & n{=}0 \\ h_a(F^a_{T,h}(x,u_c)), & n\in\mathbb{N} \end{cases}$$

where $F^a_{T,h}$ is a family of discrete-time approximate models of (6.1), T and h are the sampling time and integration step, respectively, and $u_c(t_i{+}nT){=}\psi(y_a(t_i{+}nT))$, $n{\in}\mathbb{N}_0$, for some Lipschitz function ψ. We neglect the computation delay and assume that the controller sends the stack vector of the length $N{+}1$ to the *buffer* at t_i.

$$(u_c(t_i), u_c(t_i{+}T), ..., u_c(t_i{+}NT)). \tag{6.2}$$

Note that under no ZDA ($u_a{=}0$), the actuator uses the term $u_c(t_i{+}nT)$ in (6.2) to update the plant input for $t_i{\le}t{\le}t_i{+}NT$, *i.e.*, $u(t){=}u_c(t_i{+}nT)$ for $0{\le}n{<}N$ and $t_i{+}nT{\le}t{\le}t_i{+}(n{+}1)T$. After that, for $t{>}t_i{+}NT$ the actuator keeps the plant input constant with value $u(t){=}u_c(t_i{+}NT)$ until the next triggering instant t_{i+1}. Therefore, we have $u(t){=}u_c(t_i{+}NT)$ for $t_i{+}NT{\le}t{<}t_{i+1}$.

We define the measurement error between the actual and predicted output as follows:

$$e(t){=}y_a(t_i{+}kT){-}y(t), \text{ for } t_i{+}nT{\le}t{\le}t_i{+}(n{+}1)T \tag{6.3}$$

and rewrite the actuator signal as $u(t){=}\psi(y(t){+}e(t))$.

Assumption 6.1. *We assume ψ is designed such that the equilibrium $x{=}0$ of the continuous-time system $\dot{x}(t) = f(x) + g(x)\psi(h(x){+}e)$ is input-to-state stable with respect to the error e. Thus there exists a Lyapunov function $V : \mathbb{R}^n \to \mathbb{R}$ and some $\alpha_1, \alpha_2, \gamma{\in}\mathbb{K}_\infty, \lambda{\in}\mathbb{R}_{>0}$ that satisfy the following*

conditions:

$$\alpha_1(|x|) \leq V(x) \leq \alpha_2(|x|), \tag{6.4a}$$

$$\nabla V(x)(f(x)+g(x)\psi(h(x)+e)) \leq -\lambda V(x)+\gamma(|e|). \tag{6.4b}$$

Assumption 6.2. *We assume that the approximate model $F^a_{T,h}$ is one-step consistent with the exact model F^e_T, and it is equi-Lipschitz Lyapunov-ISS. Moreover, the control law ψ is uniformly locally Lipschitz with respect to y.*

6.1.2 Sampling zeros dynamical system

The zero-dynamics of system (6.1) is the internal dynamics when input and initial conditions result in zero output, [102, 53]. In the sampled-data framework proposed in Fig. 6.1, this includes a sampled version of the continuous-time zero dynamics (intrinsic part) and a linear subsystem (extrinsic zero-dynamics) caused by the sample and hold process. Sampling zeros are the eigenvalues of matrix $Q(\tau_i)$ associated with extrinsic zero-dynamics, and vary with time if the inter-sample time $\tau_i{=}t_i{-}t_{i-1}$ is not fixed which can be represented as a switching dynamical system using the δ-operator as follows, [53]:

$$\begin{cases} \delta\eta_i{=}Q(\tau_i)\eta_i \\ Q(\tau_i){=}T_{21}(\tau_i)A_{12}(\tau_i) + A_{22}(\tau_i) \end{cases} \tag{6.5}$$

where

$$T_{21}(\tau_i){=}\begin{bmatrix} -\frac{n}{\tau_i} & \cdots & -\frac{n!}{\tau_i^{n-1}} \end{bmatrix}^{\intercal},$$

$$A_{12}(\tau_i){=}\begin{bmatrix} 1 \\ \frac{\tau_i}{2} \\ \vdots \\ \frac{\tau_i^{n-2}}{(n-1)!} \end{bmatrix}^{\intercal}, A_{22}(\tau_i){=}\begin{bmatrix} 0 & 1 & \cdots & \frac{\tau_i^{n-3}}{(n-2)!} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 \end{bmatrix}.$$

6.1.3 Zero-Dynainter-samplemics Attacks

As it can be concluded from 2.5, (2.6) and the example therein, in a sampled-data system with constant sampling time T and a relative degree $r{\geq}2$, using a fast sampling rate leads to non-minimum phase sampling zeros. Therefore, the attacker can exploit the unstable $Q(T)$ to generate $u_z(nT)$, $n{\in}\mathbb{N}$. This vulnerability is demonstrated by an example on a nonlinear system in [103]. Omitting the details of the example, the malicious effect of a ZDA in this scenario is that it has the

potential to mask any unbounded deviation of the internal dynamics from the output. Indeed, the attacker injects an output-zeroing input to the plant, therefore, while the output converge to the operating point, the internal dynamics follows unbounded states of the attack's dynamical system created by the non-minimum phase extrinsic zero-dynamics. Consequently, unstable sampling zeros cause unstable internal dynamics that cannot be detected at the output.

To combat the effects of ZDAs, one trivial strategy is to increase the sampling period when discretizing the system, *i.e.* $T \to \infty$. This can stabilize the eigenvalues for Q in (6.5) resulting in minimum-phase sampling zeros. However, this solution has limitations as it necessitates low sampling rates, resulting in a poor system performance with significant inter-sample ripple and the possibility of aliasing (see for example [95, Example 8.4.2]). Since the dynamics of the sampling zeros depend on the time period between samples, τ_i, a non-uniform sampling strategy can be utilized to induce non-uniform switching behaviour. As a result, it is possible to find a stabilizing switching signal that provides the minimum-phase property for the sampling zeros dynamical system (referred to as extrinsic zero-dynamics), thus, rendering ZDAs ineffective. Under certain conditions to be clarified later, using a well-designed event-triggered method can effectively provide a stabilizing switching signal for the extrinsic zero-dynamics and overall stability of the closed-loop system.

6.1.4 Main Problem

It is now clear that the main challenge to address is as follows. Our goal is to simultaneously stabilize the nonlinear dynamical system (6.1) together with the extrinsic zero-dynamics (6.5) by using the inference-based control setup (6.2) with a well-designed triggering condition. To this end, we formulate the stability problem and obtain a relationship between ISS and the triggering parameters such that the inferential event-based control setup guarantees both the minimum-phase property and Lyapunov stability of the closed loop system (6.1) under ZDAs.

6.2 Preliminary Results

In this section, we firstly analyze the stability of the extrinsic zero-dynamics (6.5) under the event-triggered mechanism. This results in a switching zero-dynamics whose stability is studied using switching system theory. The following Lemmas characterize the behaviour of the switching zero-dynamics under asynchronous sampling, known as a switching signal.

Lemma 6.1. *For the switching system* (6.5) *there exist some fixed* $k_\lambda > 0$ *such that the following statements are valid with respect to* k_λ *and* τ_i*:*
For any interval $\tau_i = [t_{k-1}, t_k)$, $k \in \mathbb{N}^0$*:*

1. If $\tau_i \leq k_\lambda$, then Q is not Schur stable over $t \in [t_{k-1}, t_k)$ which results in the existence of an unstable mode for (6.5).
2. If $\tau_i > k_\lambda$, then Q is Schur stable in $t \in [t_{k-1}, t_k)$ which results in the existence of a stable mode for (6.5).

Proof. The properties of the spectrum $S\{Q(\tau_i)\}$ are outlined in chapter 5. As indicated by the results in Theorem (5.1), because of the special form of Q, the eigenvalues of $Q(\tau_i)$ decrease monotonically with respect to τ_i, *i.e.*, for any $\lambda \in S\{Q\}$, $\lambda \propto \frac{1}{\tau_i}$. Therefore, there exist a positive constant k_λ such that $\max\{|\lambda_i| | \lambda_i \in S\{Q\}, i=1, ..., n\} = \frac{k_\lambda}{\tau_i}$. Now, if $\tau_i > k_\lambda$, all eigenvalues are located inside the stability region, resulting in a stable mode and *vice versa*. Therefore, the stability of a switching dynamical system (6.5) is directly related to τ_i. □

Lemma 6.2. *For any stable/unstable mode $Q(\tau_i)$, there exist a scalar constant $a>0$ such that $|Q(\tau_i)| \leq a|\lambda_m(\tau_i)|$, where $|\lambda_m(\tau_i)|$ represents the largest absolute value of the eigenvalues of $Q(\tau_i)$ at $t=\tau_i$, i.e. $|\lambda_m(\tau_i)| \leq |\lambda(\tau_i)^j|$ for $\lambda_(\tau_k)^i$ $i \in \{1, ..., r-1\}$.*

Proof. Computing the scalar a is a straightforward utilizing algebraic matrix theory. □

We define $\mathcal{S}(t, t_0)$ as a set of all triggering instant t_i during $t \in [t_0, t]$, and $n(t, t_0)$, $\Xi^+(t, t_0)$ ($\Xi^-(t, t_0)$) as the total number of switching instants in $\mathcal{S}(t, t_0)$ and total duration of unstable (stable) modes of switching extrinsic zero-dynamics (6.5) in $t \in [t_0, t]$, respectively, then propose the stability condition of system (6.5) as follows:

Theorem 6.1. *The dynamical system* (6.5) *is exponentially stable under any arbitrary switching sequence $\mathcal{S}$ if there exist constants $n_0, t_0, \tau_z, T_z \in \mathbb{R}_{>0}$ such that the following conditions are satisfied:*

$$n(t, t_0) \leq n_0 + \frac{t - t_0}{\tau_z} \tag{6.6a}$$

$$\Xi^+(t, t_0) \leq \xi_0 + \frac{t - t_0}{T_z} \tag{6.6b}$$

Proof. Consider the linear switching system (6.5). At any switching time t_i, the solution of (6.5) can be written as follows:

$$\eta(t_k) = Q(\tau_k)Q(\tau_{k-1}) \cdots Q(\tau_0)\eta(0). \tag{6.7}$$

According to Lemma 6.1, the switching system (6.5) contains stable and unstable modes for $t < t_k$. Assume τ_i (τ_j), $i \in \{1, ..., N_s\}$ ($j \in \{1, ..., N_u\}$) indicates the time interval where (6.5) has stable

(unstable) modes. Therefore, we can partition (6.7) as follows:

$$\eta(t_k)=\Pi_{i=1}^{i=N_s}Q(\tau_i)\Pi_{j=1}^{i=N_u}Q(\tau_j)\eta(0) \tag{6.8}$$

Define $\lambda_i=|\lambda(\tau_i)|$ and $\lambda_j=|\lambda(\tau_j)|$ as the norm of the smallest and largest eigenvalues of the stable and unstable mode in τ_i and τ_j, respectively. Using Lemma 6.2 and substituting λ_i and λ_j into (6.8) we have:

$$\begin{aligned}|\eta(t_k)|&\leq\Pi_{i=1}^{i=N_s}a_i\lambda_i\Pi_{j=1}^{j=N_u}a_j\lambda_j|\eta(0)|\\&\leq\Pi_{i=1}^{i=N_s}e^{(a_i+\ln(\lambda_i))}\Pi_{j=1}^{j=N_u}e^{(a_j+\ln(\lambda_j))}|\eta(0)|\\&\leq e^{a_m n(t)+\ln(\lambda^+)\Xi^+(t)+\ln(\lambda^-)\Xi^-(t)}|\eta(0)|\end{aligned} \tag{6.9}$$

where $a_m=\max\{a_i,a_j\}$, $\lambda^+=\max\{|\lambda_j|\}$, and $\lambda^-=\max\{|\lambda_i|\}$, $j\in\{1,...,N_u\}$ and $i\in\{1,...,N_s\}$. The exponentially stability of the system (6.5) is guaranteed if the exponential rate of the RHS in (6.9) is monotonically decreasing. Thus, considering the condition (6.6b) we can choose an arbitrary scalar $\lambda^*\leq\lambda^-$ and $k_0>0$ to have the following inequality:

$$\ln(\lambda^+)\Xi^+(t)+\ln(\lambda^-)\Xi^-(t)\leq\ln(\lambda^*)t+k_0 \tag{6.10}$$

such that $T_z=\frac{\ln(\lambda^+)-\ln(\lambda^-)}{\ln(\lambda^*)-\ln(\lambda^-)}$, and $\xi_0=\frac{k_0}{\ln(\lambda^+)-\ln(\lambda^-)}$.

Substituting (6.10) into (6.9) we have:

$$|\eta(t_k)|\leq e^{a_m n(t)+\ln(\lambda^*)t+k_0}|\eta(0)|. \tag{6.11}$$

Now, substituting condition (6.6a) into the exponential rate in the RHS (6.11), we can choose an arbitrary scalar $\alpha\geq k_0$ and $\bar{\lambda}\leq\lambda^*$ to obtain the following inequality:

$$a_m n(t)+\ln(\lambda^*)t+k_0\leq\alpha+\ln(\bar{\lambda})t \tag{6.12}$$

such that $N_0=\frac{\alpha-k_0}{a_m}$ and $\tau_z=\frac{a_m}{\ln(\bar{\lambda})-\ln(\lambda^*)}$.

Finally, substituting (6.12) into (6.11) and considering the fact that $0\leq\bar{\lambda}\leq\lambda^-\leq1$, the RHS of inequality (6.11) has a monotically decaying rate. Therefore, the switching system (6.5) is exponentially stable under the switch signal $\mathcal{S}$, provided that conditions (6.6) hold. □

6.2.1 Event-Triggering Condition

Let t_i, be the most recent sampling instant. The control signal is updated again at t_{i+1} according to the following rule:

$$
\begin{aligned}
t_{i+1}=\inf\{t>t_i:&\\
&\gamma(4|e(t)|)>\lambda_1\gamma(4|y(t|)+\gamma(\nu T\rho(h)) && \text{(6.13a)}\\
&\wedge\, n(t)\leq n_0+\frac{t}{\tau_z} && \text{(6.13b)}\\
&\wedge\, \Xi^+(t)\leq\xi_0+\frac{t}{T_z}\} && \text{(6.13c)}
\end{aligned}
$$

where $\lambda_1:=\lambda(1-c)$, $0<c<1$, $\nu\in\mathbb{R}_{>0}$, and $e(t)$ is defined in (6.3). The second and third conditions in (6.13) are derived from the criteria in Theorem 6.1 to ensure that the triggering sequence t_i satisfies the stability condition of switching extrinsic zero-dynamics (6.5). Typically, the ETM module first evaluates the first condition (6.13a) to make a decision on event triggering instant t_i, but satisfying (6.13a) may not guarantee successful transmission. Therefore, we denote t_j^{us} as unsuccessful event times, *i.e.*, $t_j^{us}=\{t:$(6.13a) holds but (6.13b) or (6.13c) does not hold & $j\in\mathbb{N}\}$. In this regard, we partition $[t_i, t_{i+1}]$ into the following three sub-intervals:

$$
[t_i, t_{i+1}]=\Delta_1(t_{i+1}, t_i)\cup\Delta_2(t_{i+1}, t_i)\cup\Delta_3(t_{i+1}, t_i) \tag{6.14}
$$

where

$$
\Delta_1(t_{i+1}, t_i):=[t_i, t_i+NT]
$$

$$
\Delta_2(t_{i+1}, t_i):=\begin{cases}(t_i+NT, t_j^{us}] & t_j^{us}\in(t_i+NT, t_{i+1}),\\ (t_i+NT, t_{i+1}) & t_j^{us}\notin(t_i+NT, t_{i+1}),\\ \emptyset & t_{i+1}=t_i+NT,\end{cases}
$$

$$
\Delta_3(t_{i+1}, t_i):=\begin{cases}(t_j^{us}, t_{i+1}] & t_j^{us}\in(t_i+NT, t_{i+1}),\\ \emptyset & t_j^{us}\notin(t_i+NT, t_{i+1}).\end{cases}
$$

Lemma 6.3. *Under the Assumption 6.2, the event-triggering rule* (6.13) *guarantees Zeno-free behaviour for the closed-loop event-triggered system.*

Proof. According to the error definition (6.3) and Remark 6.1, for $t_i^s\leq t\leq t_i^s+NT$ we have $|e(t)|\leq N(1+KT)^N T\rho(h)$.

Consider the worst case scenario when $|e(t)|=N(1+KT)^N T\rho(h)$. We have $\gamma(4|e(t)|)=\gamma(4N(1+KT)^N T\rho(h))$. Based on the first triggering condition (6.13a) we can define $\nu:=4N(1+KT)^N$, then $\gamma(4|e(t)|)=\gamma(\nu T\rho(h))$, and as a result, $\gamma(4|e(t)|)\leq\lambda_1\gamma(4|y(t)|)+\gamma(\nu T\rho(h))$. Thus, we conclude that condition (6.13a) is never violated for $[t_i, t_i+NT]$ which guarantees Zeno-free behaviour. □

Remark 6.2. *According to Lemma 6.3, once an event instant t_i^s occurs no additional triggering happens within the time period $[t_i, t_i+NT]$. This guarantees the presence of $\beta>0$ such that $\phi(t)\leq\beta t$, where $\phi(t)$ represents the total number of times that* (6.13a) *is satisfied in* $[0, t]$.

6.3 Main Results

In this section we analyze the stability of the nonlinear system (6.1) using the common Lyapunov function method. We firstly, investigate some bounds on the time intervals defined in (6.14) in the following Lemma to be used in Theorem 6.2.

Lemma 6.4. *Consider the event-triggering condition* (6.13) *and define the time interval* $[t_i, t]$ *as follows:*

$$[t, t_i]=\Delta_1(t, t_i)\bigcup\Delta_2(t, t_i)\bigcup\Delta_3(t, t_i)$$

where $\Delta_m(t, t_i)=\underset{i=0}{\overset{n(t)}{\cup}}\Delta_m(t_i, t_{i-1})\bigcap[0, t]$ *for* $m\in\{1, 2, 3\}$, *then sub-intervals* $\Delta_m(t, t_i)$ *are bounded from the above by the following inequalities:*

$$\Delta_1(t, t_i)\leq(N+1)Tn(t, t_i) \tag{6.15a}$$

$$\Delta_3(t, t_i)\leq\Xi^+(t, t_i)-(\phi(t, t_i)-n(t, t_i))(N+1)T \tag{6.15b}$$

$$\Delta_2(t, t_i)\leq(t-t_i)-\Delta_1(t, t_i)-\Delta_3(t, t_i) \tag{6.15c}$$

Proof. With respect to (14) $\Delta_1(t_{i+1}^s, t_i^s)$ is a fixed length interval with the length of $(N+1)T$ after any successful triggering time t_i^s, therefore, the total length of $\Delta_1(t_{i+1}, t_i)$, $t_i\in\mathcal{S}\bigcap[t_i, t]$ is upper-bounded by the total number of events $n(t, t_i)$ multiplied by $(N+1)T$ which verifies (6.15a). To evaluate inequality (6.15b), we consider the worst case as follows: if $t_j^{us}\in[t_i, t_{i+1}]$, then $t_j^{us}=t_i+NT$ for $t_i\in\mathcal{S}\bigcap[t_i, t]$. Thus using the definition Δ_3 in (6.14) and ϕ in Remark 6.2, (6.15b) is verified. Finally, the remaining part in $[t_i, t]$ upper-bounds $\Delta_2(t, t_i)$ which verifies (6.15c). □

Lemma 6.5. *Consider the nonlinear system* (6.1) *and assume that the approximate discrete-time model $F_{T,h}^a$ satisfies the one-step consistency of Definition 2.2. Then for $k\in\{0, ..., N\}$ and $i\in\mathbb{N}^0$ we*

have:

$$\textit{1) for } t_i{+}kT{\leq}t{\leq}t_i{+}(k{+}1)T : |x(t){-}x^a(t_i{+}kT)|{\leq}T\rho(h) \tag{6.16a}$$

$$\textit{2) for } t_i{\leq}t{\leq}t_i{+}NT : |x(t){-}x^a(t_i{+}kT)|{\leq}\alpha(\delta,T). \tag{6.16b}$$

Proof. Recall that the disturbance free continuous-time system (6.1) is locally Lipschitz. Thus, $x(t_{|t=kT})=x^e(kT)$ $\forall T<T^*$. Consider $0{\leq}\delta_T{\leq}T$ and $k{=}0$, then we obtain the following:

$$\begin{aligned}
&|x(t_i{+}\delta_T){-}x^a(t_i{+}T)|\\
&{\leq}|x(t_i{+}\delta_T){-}x^a(t_i{+}\delta_T)|{+}|x^a(t_i{+}\delta_T){-}x^a(t_i{+}T)|\\
&{\leq}\delta_T\rho^*(h) + \lambda_{F^a}T{\leq}T\rho(h)
\end{aligned} \tag{6.17}$$

where $\rho(.){:=}\rho^*(.){+}\lambda_{F^a}$ and λ_{F^a} is the Lipschitz constant of approximate model F^a. The final inequality in (6.17) is derived by utilizing a one-step consistency in conjunction with the Lipschitz continuity property of the approximate model F^a. By continuing this process for $k{\in}\{0,\ldots,N\}$ we have that inequality (6.16a) holds true for any values of $k{\leq}N$ and $t{\in}[t_i{+}kT, t_i{+}(k{+}1)T]$.

Additionally, as outlined in Definition 2.3 and Remark 6.1, the deviation between $x(t)$ and x^a can be bounded by $N(1{+}KT)^NT\rho(h)$ after N steps. As a result, we conclude that for $t_i{\leq}t{\leq}t_i{+}NT$ we have:

$$|x(t){-}x^a(t_i{+}kT)|{\leq}N(1{+}KT)^NT\rho(h). \tag{6.18}$$

Defining $\alpha(\delta,T){=}N(1{+}KT)^NT\rho(h)$, inequality (6.18) implies the second condition (6.16b). □

Assumption 6.3. *In order to prevent finite escape times during $[t_i, t_{i+1}]$, we assume the presence of some $\mu{\in}\mathbb{R}_{>0}$ such that for any $r{\in}\mathbb{R}$ and γ and α_1 in* (6.4) *there exist $\nu{>}0$ such that $\gamma(\nu r) \leq \mu\alpha_1(r)$.*

Theorem 6.2. *Under Assumptions 6.1-6.2, given any $\delta_x{>}0$, the nonlinear system* (6.1) *under control setup* (6.2) *and triggering rule* (6.13) *is Lyapunov stable for all $|x(0)|{\leq}\delta_x$ if the parameters in* (6.6) *satisfy the following inequality:*

$$\frac{\widetilde{T}(\omega_1{-}2\omega_2{+}\omega_3)}{\tau_z}{+}\frac{\omega_3{-}\omega_2}{T_z}{\leq}\beta\widetilde{T}(\omega_3{-}\omega_2){-}\omega_2 \tag{6.19}$$

where $\widetilde{T}{=}(N{+}1)T$, and $\omega_1{=}{-}\lambda$, $\omega_2{=}{-}(\mu(\lambda_1{+}2){-}\lambda)$, $\omega_3{=}\mu{-}\lambda$.

Proof. To prove the theorem we consider first the right-hand side of (6.4b) within an arbitrary inter-event time interval $[t_i, t_{i+1}]$ and expand the result for $[0, t]$.

Any interval $[t_i, t_{i+1}]$ in (6.14) can be divided into three sub-intervals $\Delta_1(t_{i+1}, t_i)$, $\Delta_2(t_{i+1}, t_i)$, $\Delta_3(t_{i+1}, t_i)$. Beginning with $\Delta_1(t_{i+1}, t_i)$, according to Lemma 6.3, no further triggering events

occur. Therefore, the Lyapunov function $V(x)$ remains non-increasing, and this is supported by the control input sequence (6.2) at any $t{=}t_i$, given that the approximate model $F^a_{T,h}$ is created by selecting suitable values of T and N based on Assumption 6.2 and the results in [55, Theorem 1]. Thus, one-step consistency is satisfied and we obtain:

$$\gamma(|e(t)|) \leq \gamma(\mathcal{L}_f T \rho(h)) \tag{6.20}$$

where (6.20) is derived using the Lipschitz continuity together with the one-step consistency condition in the basis of (6.16a). Therefore, substituting (6.20) into (6.4b) and solving the resulting differential inequality, we have the following upper-bound on $V(x(t))$ for $t{\in}[t_i, t_i{+}NT]$ with $\omega_1{=}\lambda$.

$$V(x) \leq e^{-\omega_1(t-t_i)} V(x(t_i)){+}\alpha_1 \tag{6.21}$$

where $\alpha_1{=}\frac{\gamma(\mathcal{L}_f \nu T \rho(h))}{\omega_1}$.

In $\Delta_2(t_{i+1}, t_i)$, the actuator employs the last element of (6.2) and holds it until a new update is received. Unlike the previous scenario, here the one-step consistency does not necessarily hold. Thus, to obtain an upper-bound on $\dot{V}$ we start with the fact that $|e(t)|{=}|y^a(t_i{+}kT){-}y(t)|$, and we can write:

$$\gamma(2|y^a(t_i{+}kT)|) \leq \gamma(4|e(t)|){+}\gamma(4|y(t)|) \tag{6.22}$$

where the right hand side in (6.22) follows from the following inequality on a the function $\gamma{\in}\mathcal{K}_\infty$: $\gamma(a{+}b) \leq \gamma(2a){+}\gamma(2b)$.

Moreover, using the triangular inequality we have:

$$\gamma(|e(t)|){\leq}\gamma(2|y^a(t_i{+}kT)|){+}\gamma(2|y(t)|). \tag{6.23}$$

Substituting (6.22) into (6.23) we obtain:

$$\gamma(|e(t)|){\leq}\gamma(4|e(t)|){+}\gamma(4|y(t)|){+}\gamma(2|y(t)|). \tag{6.24}$$

From the Lipschitz property of $h(x)$ we can write $|y|{\leq}\mathcal{L}_h|x|$. Moreover, the triggering condition (6.13a) is not violated in this time interval, *i.e.* $\gamma(4|e(t)|){\leq}\lambda_1\gamma(4|y(t)|){+}\gamma(\nu T\rho(h))$. Therefore, substituting the aforementioned inequalities into (6.24), we have:

$$\gamma(|e(t)|){\leq}(\lambda_1{+}2)\gamma(4\mathcal{L}_h|x(t)|){+}\gamma(\nu T\rho(h)). \tag{6.25}$$

Substituting (6.25) into the right-hand side of (6.4b) and considering Assumption 6.3 with $\nu{=}4\mathcal{L}_h$,

we obtain the following upper-bound on $\dot{V}(x)$:

$$\dot{V}(x(t))\leq(-\lambda+\mu(\lambda_1+2))V(x(t))+\gamma(\nu T\rho(h)). \tag{6.26}$$

Finally, solving (6.26) results in the following upper-bound on $V(x(t))$ for $t\in[t_i+NT, t_j^{us}]$ with $\omega_2=\mu(\lambda_1+2)-\lambda$.

$$V(x(t)) \leq e^{-\omega_2(t-t_i-NT)}V(x(t_i^+NT)), +\alpha_2. \tag{6.27}$$

where $\alpha_2=\frac{\gamma(\nu T\rho(h))}{\omega_2}$.

In $\Delta_3(t_{i+1}, t_i)$, we assume that the condition (6.13a) holds and the system needs to send a new event, however, due to stability conditions (6.6) on the extrinsic zero-dynamics, at least one of (6.13b) or (6.13c) is not satisfied. As a result, a new unsuccessful event is created and the Lyapunov function $V(x)$ may increase. Thus, the condition on the Lyapunov function is established as follows: from the definition of error in (6.3), we have

$$|e(t)|\leq 2|y(t)|+\mathcal{L}_h\alpha(\delta, T) \tag{6.28}$$

where (6.28) is derived by utilizing the multi-step consistency between models outlined in Definition 2.3 together with (6.16b). Substituting (6.28) into (6.4b), we get:

$$\dot{V}(x(t))\leq(\mu-\lambda)V(x(t))+\alpha_3, \tag{6.29}$$

where $\alpha_3:=\gamma(2\mathcal{L}_h\alpha(\delta, T))$.
Finally, solving the differential inequality (6.29) we obtain an upper-bound on $V(x)$ with exponential rate $\omega_3=\mu-\lambda$ as follows:

$$V(x(t)) \leq e^{\omega_3(t-t_j^{us})}V(x(t_j^{us}))+\frac{\alpha_3}{\omega_3}(e^{\omega_3(t-t_j^{us})}), \tag{6.30}$$

which gives the desired upper bound over $t\in[t_j^{us}, t_{i+1}^{s}]$.

Consequently, using (6.21), (6.27), and (6.30), the following inequality holds for the Lyapunov function $V(x(t))$ over $t\in[t_i, t_{i+1}]$:

$$\begin{aligned} V(x)\leq & e^{\omega_3\Delta_3(t_{i+1},t_i)-\omega_2\Delta_2(t_{i+1},t_i)-\omega_1\Delta_1(t_{i+1},t_i)}V(x(t_i)) \\ & +\alpha_1 e^{\omega_3\Delta_3(t_{i+1},t_i)-\omega_2\Delta_2(t_{i+1},t_i)}+(\alpha_2+\alpha_3)e^{\omega_3\Delta_3(t_{i+1},t_i)}. \end{aligned} \tag{6.31}$$

Using the common Lyapunov function technique in the switching system, we can substitute $V(x(t_i))$

into (6.31) for $i\in\{0,...,n(t)\}$, and extend the inequality (6.31) over $t\in[0,t]$ as follows:

$$\begin{aligned}
V(x)\leq & e^{\omega_3\Delta_3(t,0)-\omega_2\Delta_2(t,0)-\omega_1\Delta_1(t,0)}V(x(0)) \\
& +\alpha_1\left[\sum_{i=0}^{n(t)} e^{\omega_3\Delta_3(t,t_i)-\omega_2\Delta_2(t,t_i)-\omega_1\Delta_1(t,t_i)}\right. \\
& \left.\times e^{\omega_3\Delta_3(t_i,t_{i-1})-\omega_2\Delta_2(t_i,t_{i-1})}\right] \\
& +(\alpha_3+\alpha_2)\left[\sum_{i=0}^{n(t)} e^{\omega_3\Delta_3(t,t_i)-\omega_2\Delta_2(t,t_i)-\omega_1\Delta_1(t,t_i)}\right. \\
& \left.\times e^{\omega_3\Delta_3(t_i,t_{i-1})}\right] \\
& \leq \overbrace{e^{\omega_3\Delta_3(t,0)-\omega_2\Delta_2(t,0)-\omega_1\Delta_1(t,0)}}^{A}V(x(0))+(\alpha_3+\alpha_2+\alpha_1) \\
& \times \underbrace{\sum_{i=0}^{n(t)} e^{\omega_3\Delta_3(t,t_i)-\omega_2\Delta_2(t,t_i)-\omega_1\Delta_1(t,t_i)}e^{\omega_3\Delta_3(t_i,t_{i-1})}}_{B}.
\end{aligned} \tag{6.32}$$

If the exponential rate of A in (6.32) is negative, and the summation B is bounded from above over the entire time, then we can make sure that Lyapunov function $V(x)$ is monotonically decreasing over the time interval $[0,t]$. Hence, we substitute the upper-bound of $\Delta_m(t,0)$, $m=\{1,2,3\}$, from (6.15) into A in (6.32) and make it negative to obtain the following inequality condition:

$$\underbrace{(\omega_2-\omega_1)\frac{\widetilde{T}}{\tau_z}-\omega_2+(\omega_2+\omega_3)\left(\frac{1}{T_z}-(\beta+\frac{1}{\tau_z}).\widetilde{T}\right)}_{r^*}\leq 0 \tag{6.33}$$

Notice that inequality (6.33) verifies condition (6.19). Next, we analyze the convergency of the summation B in (6.32). We can rewrite B as follows:

$$B\leq e^{(c^*-\omega_3\widetilde{T}-\tau_z N_0)}\sum_{i=0}^{n(t)} e^{(r^*+\omega_3)\tau_z n(t,t_i)}, \tag{6.34}$$

where $c^*=(\omega_2-\omega_1)\widetilde{T}N_0+(\omega_2+\omega_3)(t_0+\widetilde{T}N_0)$, and inequality (6.34) follows from the upper-bounds on $\Delta_m(t,t_i)$, $m=\{1,2,3\}$, obtained in (6.15) together with condition (6.6a). Since the coefficient of ω_3 in r^* is less than -1, *i.e.*, $\frac{1}{T_z}-(\beta+\frac{1}{\tau_z})\widetilde{T}<-1$, we can easily verify that the term $(r^*+\omega_3)$ is

negative, therefore, the summation part in the right-hand side of (6.32) converges as follows:

$$\sum_{i=0}^{n(t)} e^{(r^*+\omega_3)\tau_z n(t,t_i)} \leq \frac{1}{1-e^{(r^*+\omega_3)\tau_z}}. \tag{6.35}$$

Finally, the negative exponential rate of A and bounded summation term B in (6.32) leads to decreasing Lyapunov function $V(x)$ over $[0,t]$. This implies the Lyapunov stability of the closed-loop nonlinear system (6.1)-(6.2) with triggering rule (6.13).

Substituting now (6.32) into (6.4), we obtain the following upper-bound for $x(t)$:

$$|x(t)| \leq \alpha_1^{-1}\left(e^{c^*}\alpha_2(|x(0)|) + \frac{1}{1-e^{(r^*+\omega_3)\tau_z}}\right). \tag{6.36}$$

The right-hand side of (6.36) is the compact set X which was denoted in Definitions 2.2-2.3 and can be calculated offline as a radius of initial local domain for the function ρ and Lipschitz constants. This implies that ρ, $\mathcal{L}_f$, $\mathcal{L}_g$, and $\mathcal{L}_h$ are valid in all intervals. □

Remark 6.3. *Inequality* (6.19) *provides the relationship between the extrinsic zero-dynamics stability parameters (τ_a, T_a), the system stability parameter (λ), buffer size (N), sampling period (T), event-triggered parameter (c, ν) and event generation rate (β). From* (6.19)*, we conclude that increasing N leads to a larger upper bound for* (6.19)*. This allows for greater growth in $\frac{1}{\tau_a}$ and $\frac{1}{T_a}$, and accordingly create larger allowable $n(t)$ and $\Xi^+(t)$ in* (6.6a) *and* (6.6b)*. As a result, the switching extrinsic zero-dynamics* (6.5) *remains bounded and stable even when more unstable modes are present in $t \in [0,t]$.*

6.4 Case Study

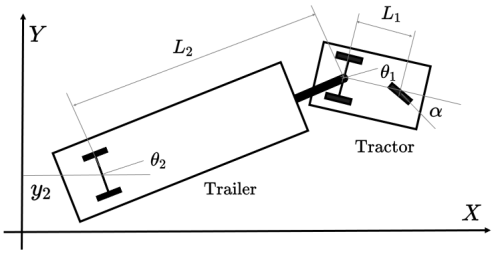

Figure 6.2: Schematic of single trailer articulated vehicle in (X,Y)-plane.

To evaluate the effectiveness of our proposed method, we consider the single trailer articulated vehicle model discussed in [104]. Figure 6.2 illustrates the schematic of an articulated vehicle, with

the Y-axis representing the vertical position and X-axis representing the desired horizontal position. The steering angle of the tractor, represented by $\alpha = \tan^{-1}(u)$, where u serves as the control input. L_1 and L_2 are the wheelbase distances, and θ_1 and θ_2 are the orientations, respectively. Our goal is to control the vehicle's position along the X-axis using the steering angle. We define: $[x_1, x_2, x_3] := [y_2, \theta_1, \theta_2]$, therefore, the state space representation of the system is as follows:

$$\begin{aligned}
\dot{x}_1 &= \tan(x_3) \\
\dot{x}_2 &= -\frac{\tan(x_2)}{L_1 \cos(x_3)} + \frac{1}{L_2 \cos(x_2)\cos(x_3)} u \\
\dot{x}_3 &= \frac{\tan(x_2)}{L_1 \cos(x_3)} \\
y &= x_1
\end{aligned} \tag{6.37}$$

where L_1=2 and L_2=4. The normal form representation of (6.37) is given by:

$$\dot{z}_1 = z_2, \quad \dot{z}_2 = z_3, \quad \dot{z}_3 = F(z) + b(z)\tan(\alpha)$$

where $x_1 = z_1$, $x_2 = \tan^{-1}(L_2 \cos^3(\tan^{-1}(z_2)) z_3)$, $x_3 = \tan^{-1}(z_2)$, $F(z) = \frac{(-\cos(x_3) + 3\cos(x_2)\sin(x_3)\sin(x_2)) L_1 \sin(x_2)}{L_2^2 L_1 \cos^5(x_3)\cos^3(x_2)}$ and $b(z) = \frac{L_2 \cos(x_3)}{L_2^2 L_1 \cos^5(x_3)\cos^3(x_2)}$.

A control system for the articulated vehicle is designed by combining a sliding mode control method with a high gain observer, as follows:

$$\begin{aligned}
s &= c_1 z_1 + c_2 \hat{z}_2 + \hat{z}_3 \\
u &= (-c_1 \hat{z}_2 - c_2 \hat{z}_3 - F(z) - \beta \operatorname{sgn}(s)) / b(z)
\end{aligned}$$

where $\hat{z}_2$ and $\hat{z}_3$ are the estimations of z_2 and z_3, respectively. The remaining parameters are c_1=6.5, c_2=11.5, and β=3.5. It is clear that the relative degree of the system (6.37) is equal to the order of the system, *i.e.*, r=n=3. Therefore, the continuous-time system is minimum-phase. However, when a digital controller governs the vehicle, the following extrinsic-zero dynamics appears after using the discretization method induced by the sample-and-hold process, [53].

$$\delta\eta_{\tau_{i+1}} = \underbrace{\begin{bmatrix} -\frac{3}{\tau_i} & -\frac{1}{2} \\ -\frac{6}{\tau_i^2} & -\frac{3}{\tau_i} \end{bmatrix}}_{Q(\tau_i)} \eta_{\tau_i} \tag{6.38}$$

From $Q(\tau_i)$ we can infer that the eigenvalues are related to the inter-event time τ_i, and thus, the time interval between two consecutive event directly impacts the stability of the extrinsic zero-dynamics (6.38). For example, under a fixed inter-event time, *i.e.*, τ_i=T, $k \in \mathbb{N}_0$, when the value of

T is small, the eigenvalues of $Q(T)$ are outside the stability region, which in turn make the extrinsic zero-dynamics (6.38) non-minimum phase.

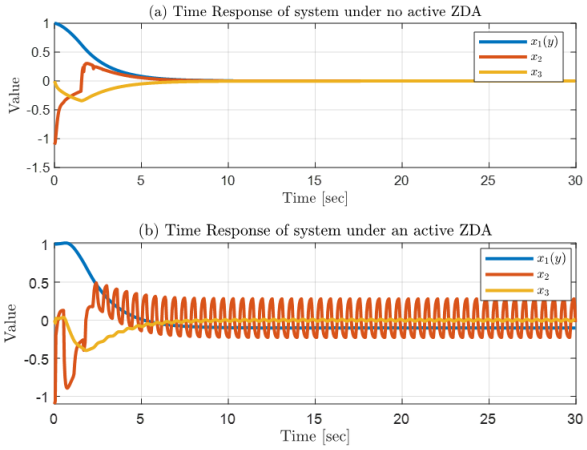

Figure 6.3: Time response of the states with fixed sampling time T.

The time response of the vehicle under digital sliding mode control with fixed sampling time is illustrated in Fig. 6.3. We assume initial conditions $[1, -1.1, 0]$. As can be seen in Fig. 6.3-(a), under no ZDAs, despite the extrinsic zero-dynamics being non-minimum phase for T=0.5s, the system remains stable. Consider now the effect of the ZDAs generated using the non-minimum phase zero-dynamics (6.38) applied to the input. The internal dynamics of the vehicle (states x_2 and x_3) may not remain bounded, as shown in Fig. 6.3-b. Indeed, the attack input is designed to make the internal dynamics pass through the kernel of the output at any sample time Tk, $k \in \mathbb{N}_0$. Thus the malicious effect of the attack is hidden from the output and the controller does not detect any abnormal deviation in the internal dynamics. This illustrates the stealthy characteristic of the ZDA, as the attack does not affect the measurement part, but affects the internal dynamics.

In the sequel, we depart from the fixed inter-event time T and let the triggering condition (6.13) and control setup (6.2) governs the system. We choose parameters n_0= 7.5, t_0= 1.54, τ_a= 5, T_a= 1.76, N=15, h=0.001, T=0.04, λ= 2, c= 0.2, β=0.05, μ= 60, κ=0.5, η=1, and functions $\rho(r)=|r|$, $\gamma(r)=r^2$. We assume the approximate model $F^a_{T,h}$ is constructed using the Euler approximation method. The first event is triggered at t=0, *i.e.* t_0=0.

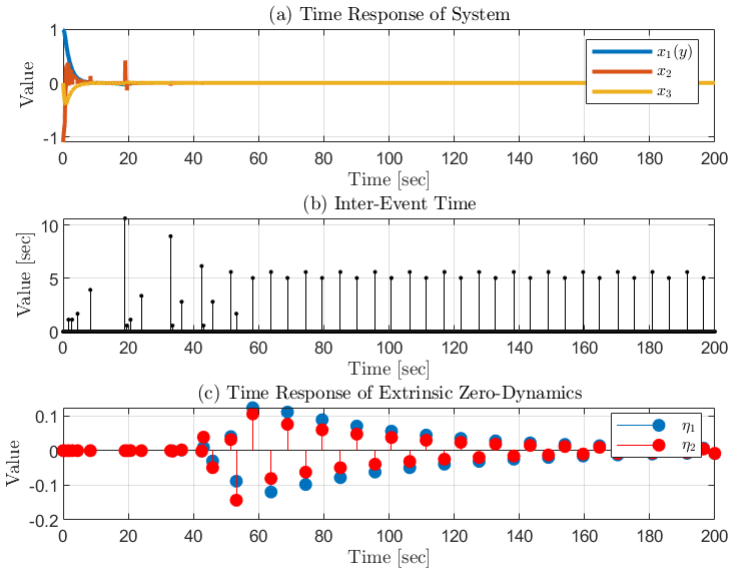

Figure 6.4: Time response of the system under ETM (6.13) and without ZDA.

Figure 6.4 illustrates the effectiveness of the proposed method. As we can see, the event instants shown in 6.4-b are carefully executed such that, firstly, states with non-zero initial condition become bounded and converge to the equilibrium point (Fig. 6.4-a), which verifies the result in Theorem 6.2. Secondly, the switching extrinsic zero-dynamics (6.38) becomes bounded and eventually converges to zero (Fig. 6.4-c), as guaranteed in Theorem 6.1.

The significance of our proposed method in ensuring a stable extrinsic zero-dynamics can be observed in Fig. 6.5 where an active ZDA targets the system. When the system is governed by the triggering condition (6.13) and inferential control setup (6.2), the zero-dynamics (6.38) is minimum-phase. Therefore, even if an attacker propagates a malicious signal input using (6.38), there may be some bounded deviations, but it is not destructive and the internal dynamics of the system remain stable, as demonstrated in Fig. 6.5-a.

For the purpose of comparison, we apply the ZDA to a typical event-triggered control system. In this case, the control structure remains the same, but we remove the restriction criterion induced by the stability of extrinsic zero-dynamics on triggering condition (6.13). Therefore, the event is triggered whenever (6.13a) is satisfied regardless of the (6.13b)-(6.13c), i.e:

$$t_{k+1}=\inf\{t>t_k\colon \gamma(4|e|)>\lambda_1\gamma(4|y|)+\gamma(\nu T\rho(h))\} \tag{6.39}$$

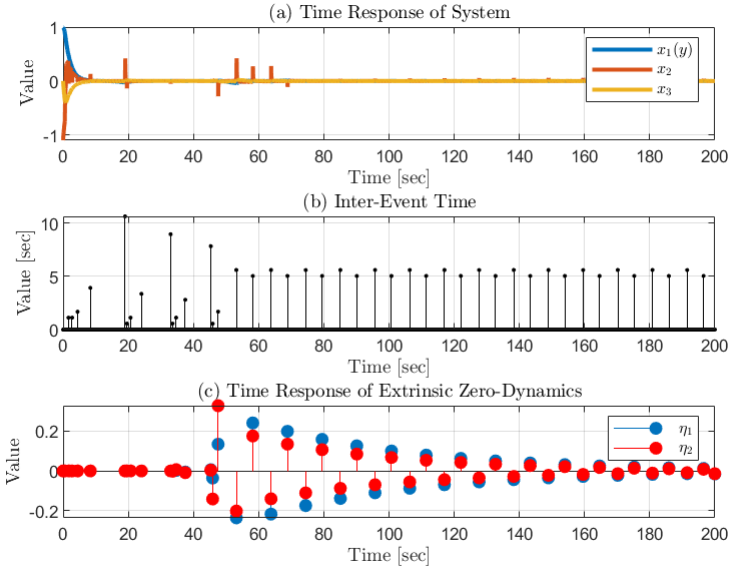

Figure 6.5: Time response of the system under ETM (6.13) and active ZDA.

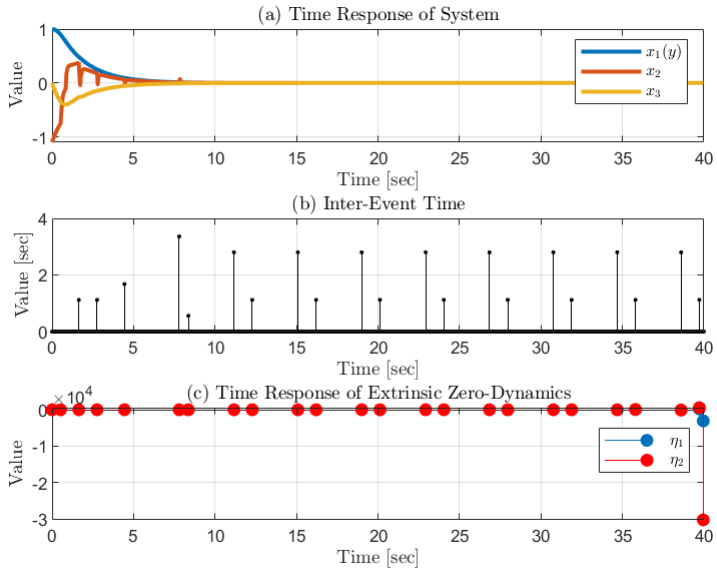

Figure 6.6: Time response of the system under ETM (6.39) and without ZDA.

As seen in Fig. 6.6, using a typical triggering condition (6.39), while the vehicle is stabilized under the control setup (6.2), there is no control on extrinsic zero-dynamics under such a condition

and eventually it becomes unstable as shown in Fig. 6.6-c.

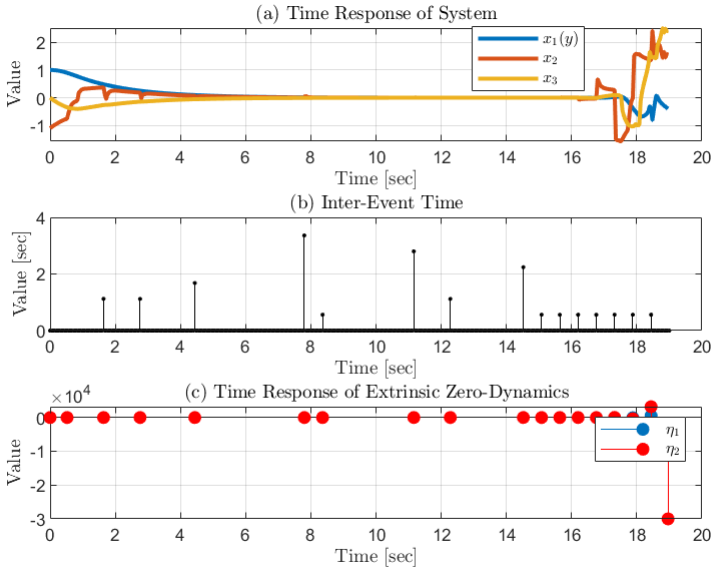

Figure 6.7: Time response of the system under ETM (6.39) and active ZDA.

In Fig. 6.7, the system equipped with the triggering condition (6.39) runs under an active ZDA and becomes unstable at t=18s despite the control setup being the same as our proposed method. This observation highlights the importance of a well-designed triggering condition in countering ZDAs. Therefore, the event instants are executed in such a way that the control input simultaneously stabilizes the zero-dynamics and the system itself, eliminating any vulnerable spots and serving as a proactive strategy.

Remark 6.4. *It is worth noting that both the typical event-triggering condition* (6.39) *(Fig. 6.7-a) and the fixed constant sampling (Fig. 6.3-b), result in an unstable system and are vulnerable to ZDAs. However, running under event-triggered mechanism* (6.39)*, attacks cannot remain stealthy, and their malicious effects eventually appear as deviations in the system's output, as shown in Fig 6.7-a. Conversely, the same effect does not occur when using the fixed time-triggered approach, as illustrated in Fig. 6.3-b. This is mainly because the use of event-triggered sampling results in unpredictable and random inter-sample time interval from the attacker's point of view. This feature makes the system's dynamics act as a so-called moving target, which is the type of strategy proposed in [47] as a detection method against stealthy attacks. As a result, the closed-loop system's dynamics become difficult to estimate by the attacker. This observation, along with what we proposed in this chapter, highlights the advantage of using the event-triggered methods instead of the time-triggered to deal with stealthy attacks in network control systems.*

6.5 Summary

In this chapter, we propose a novel control scheme that enhances the resiliency of affine nonlinear systems against ZDAs. Our approach integrates model-based event-triggered method and inferential control setup. We developed a new event-triggering condition based on the stability of switching systems with stable and unstable modes to provide the stabilizing switching signal for the extrinsic zero-dynamics in the event-based structure. Additionally, with the help of the common Lyapunov function technique, we established conditions on the event-triggered controls parameters to ensure stability under ZDAs. We demonstrated that the strategy we have devised results in minimum-phase behaviour of the extrinsic zero-dynamics while maintaining Lyapunov stability, leading to significant improvements in protection against cyber threats.

Chapter 7

Summary and Conclusion

This thesis focuses on cybersecurity and resilient control design for a nonlinear system under cyber attacks. While we explore a secure control method against DoS attacks, our primary focus is on ZDAs, which constitute an active area of research in deception attacks. The main objective of this thesis is to contribute to advancing the understanding of these attacks in sampled-data systems and to design a secure control framework. This framework leverages asynchronous sampling in event-triggered schemes, serving as a self-defence mechanism to counteract ZDAs whenever the system is targeted by an adversary.

In Chapter 3, we propose an inference-based control approach to compensate for the lack of sensor information during DoS attacks. Previous works on nonlinear systems do not provide a stabilization strategy during the DoS attack. While in our scenario the controller uses the plant model to predict future states ahead of time and uses this information as a substitute for sensor measurements. In this regard, we propose a novel model-based event-triggering strategy to communicate sensor measurements and the control block. The use of discrete-time models of nonlinear systems requires solving a nonlinear differential equation that typically does not admit a closed form solution. Thus, our formulation is framed in the theory of sampled-data nonlinear control and consistency of approximate discrete time model. We show that the triggering rule can be designed based on an approximate model, however assuming only mild conditions, the rule is guaranteed to work for the actual system. The inferential controller and event-triggered sampling are effectively combined to balance network traffic induced by packetized data transmission in the control loop. Contrary to the restriction of synchronous attacks existent in previous works and the one side restriction on the attacker channel's target condition, our method allows the control system to be asynchronously targeted on the sensor to controller and controller to actuator channels. Furthermore, the assumption on the maximum number of consecutive packets dropout, which is the case in packetized transmitting strategy is also relaxed.

In chapter 4, our goal was to extend the existing research on the benefit of multi-rate sampling

for the stability of the system under ZDAs. Using the concept of dissipativity as a fundamental tool in control systems analysis and design, we study the effect of ZDAs in nonlinear systems. We formulate our solution in the lifted-domain and analyze the dissipativity property of the internal dynamics of a multi-rate nonlinear sampled-data system based on an augmented system constructed using the lifting operator. The theory of lifting and its application in periodic linear systems is well established. In this chapter we apply the same principles to a nonlinear system and provide a framework for analysis and design a model-based resilient control of nonlinear systems in the lifted-domain. Using a model to generate predicted states and input signals in linear systems is trivial because of the existence of explicit solutions for the linear differential equations. In the nonlinear case, however, this is not a trivial task since most nonlinear differential equations do not admit a closed-form solutions. Therefore, the only resource available is to use an approximate solution. Our approach is consistent with the use of approximate models in the nonlinear sampled-data theory. Therefore, our solution is cast in the context of this body of literature and provides a model-based solution that is applicable to nonlinear systems under ZDAs. The framework provided in this chapter is one of the first attempts to implement such algorithm in nonlinear sampled-data systems under stealthy attack.

In chapter 5, we study the effect of ZDAs on the stability of nonlinear sampled-data systems implemented using an event-triggered mechanism. We formulate the problem as a switched systems and analysis the stability of the overall system using the concept of average dwell time. We use the event-triggered approach to eliminate the vulnerability of ZDAs induced by the sampling process. The new triggering decision depends not only on the plant output but also on the deviation of extrinsic zero-dynamics. Indeed, the triggering condition explicitly includes the zero-dynamics and therefore introduces a trade-off between performance and resiliency while maintaining asymptotic stability during attacks. As in the classical event-triggering approach, our scheme also reduces unnecessary communication demands when compared to traditional triggering conditions under ZDAs. However, the event-triggered approach proposed here is drastically different from the traditional use of event-triggered sampling discussed in the existing literature. The event-triggered approach was introduced and is primarily used to limit the transfer of information between system components to what is necessary, thus reducing network congestion in bandwidth-limited systems. We utilize the event-triggered mechanism as a secure solution to counteract ZDAs and ensure system resilience. The adjustable interval time between events serves as a key parameter that effectively safeguards against these attacks. Moreover, our proposed method not only neutralizes the ZDAs but makes the system immune to the so-called zero-stealthy attack. This type of attack arises when the control system works in a multi-rate sampling framework. Notice that previous works, although effective in resolving the unstable sampling zeros problem, make the system vulnerable to this type of cyber-attacks, due to the use of multi-rate sampling methods. Our proposed event-triggered mechanism, simply does not have this problem and is therefore immune to zero-stealthy attacks.

It is also worth mentioning that the multirate approach that has been presented in the chapter 4, although effective, ignores network bandwidth constraints and may result in excessive transfer of information between components. In this work we address practical limitations in networked control systems and tackle the problem from an entirely different angle. Using the event-driven approach becomes vital when a hybrid attack (for example, a combination of a ZDA and a DoS attack) targets the system, forcing open loop operation for relatively long periods of time.

In Chapter 6, we investigate an event-triggered inferential-based control scheme for nonlinear sampled-data systems under ZDAs. While the multi-rate methods explored in Chapter 4 faced challenges due to high communication bandwidth demands, the event-triggered strategy discussed in Chapter 5 experienced performance degradation. Our innovative approach tackles these obstacles and surpasses previous efforts. We introduced a novel event-triggering strategy to facilitate communication between sensor measurements and the control block. Our proposed triggering scheme is based on the model-based framework, but with modifications, including a new error equation and a threshold criterion obtained from the stability analysis of the extrinsic zero-dynamics. By employing the concept of switched system theory, we addressed the simultaneous stabilization of the nonlinear sampled-data system and its zero-dynamics under the proposed triggering condition. This allowed us to establish criteria for design, ensuring a stable, minimum-phase closed-loop system. I tis worth to mention that our solution outperforms the approach presented in Chapter 5, achieving exponential stability for the extrinsic zero-dynamics, rendering the system immune to the effects of ZDAs. Additionally, our solution eliminates issues related to extended inter-event sampling times encountered in Chapter 5.

7.1 Directions for Future work

Our proposed results in this thesis can be pursued in the following areas:

- Resilient control against ZDAs is crucial for non-minimum phase linear/nonlinear systems. Therefore, studying the security of these type of systems is essential due to their inherent vulnerability to stealthy attacks. Whether in continuous time or within a sampled-data framework, these systems are susceptible to ZDAs. One effective approach to tackle this issue involves formulating the problem as a switching system and utilizing the concept of switching systems, where all sub-systems are unstable. This method helps analyze the stability of the zero-dynamics and assess the feasibility of potential solutions.

- The concepts of relative degree, normal-form transformation, zero-dynamics, and sampling zeros are rarely studied for MIMO systems. However, most large-scale plants are typically represented as multi-input multi-output systems, requiring additional research to enhance the understanding of their security under ZDAs. The existing approach in the literature is not

applicable for cases with more than one output, rendering it an open problem for further study.

- The theory of zero-dynamics and its concepts, such as controlled invariant subspace, kernel space, sampling zeros, and relative degree, remain open areas of study in hybrid systems like event-based, switching, and piece-wise affine systems. Gaining a deeper understanding of these systems' behaviour enables the control community to offer effective solutions for mitigating cyber attacks and ensuring security for the overall system. Therefore, exploring these fundamental definitions in hybrid systems is valuable and worthwhile.

- Comprehensive protection against cyber attacks in sampled-data control systems. Most references in the literature consider a scenario in which an attacker employs a single form of attack. In a realistic scenario, however, an attacker can employ various forms of malicious attacks to target the control system. Moreover, a combination of published methods does not provide an optimal solution to confront combined attacks, thus opening an important research challenge to explore the analysis and design of combined defence methods in control systems.

- Extension of previous results with respect to the practical feedback issues such as network constraints, input and output disturbances, measurement noise, and model uncertainties. As it is well studied in the literature, the impact of disturbance on any control system equipped with an event-triggered method is critical due to the possible occurrence of Zeno phenomena. Moreover, although a communication network offers benefits to the control system in terms of time and budget, there are unavoidable constraints such as jitter, bandwidth limitations, and packet dropout which demand further exploration and improvement of the proposed methods. Consequently, the last part of this research will take into account the effects of these limitations.

References

[1] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 2018.

[2] Y. Mo and B. Sinopoli, "Secure estimation in the presence of integrity attacks," *IEEE Trans. Autom. Control.*, vol. 60, no. 4, pp. 1145–1151, 2014.

[3] T. Yang, C. Murguia, M. Kuijper, and D. Nešić, "A multi-observer based estimation framework for nonlinear systems under sensor attacks," *Automatica*, vol. 119, p. 109043, 2020.

[4] Q. Wang and H. Yang, "A survey on the recent development of securing the networked control systems," *Systems Science & Control Engineering*, vol. 7, no. 1, pp. 54–64, 2019.

[5] A. Cetinkaya, H. Ishii, and T. Hayakawa, "An overview on denial-of-service attacks in control systems: Attack models and security analyses," *Entropy*, vol. 21, no. 2, p. 210, 2019.

[6] J. Wu and T. Chen, "Design of networked control systems with packet dropouts," *IEEE Trans. Autom. Control.*, vol. 52, no. 7, pp. 1314–1319, 2007.

[7] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Autom. Control.*, vol. 60, no. 11, pp. 2930–2944, 2015.

[8] Z.-H. Pang, L.-Z. Fan, H. Guo, Y. Shi, R. Chai, J. Sun, and G.-P. Liu, "Security of networked control systems subject to deception attacks: A survey," *International Journal of Systems Science*, vol. 53, no. 16, pp. 3577–3598, 2022.

[9] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," *Proc. Int. Conf. High Confidence Networked Systems*, pp. 55–64, 2012.

[10] K. J. Åström, P. Hagander, and J. Sternby, "Zeros of sampled systems," *Automatica*, vol. 20, no. 1, pp. 31–38, 1984.

[11] G. Kranc, "Input-output analysis of multirate feedback systems," *IRE Transactions on Automatic Control*, vol. 3, no. 1, pp. 21–28, 1957.

[12] D. Glasson, "Development and applications of multirate digital control," *IEEE Control Systems Magazine*, vol. 3, no. 4, pp. 2–8, 1983.

[13] J. Wu, C. Peng, H. Yang, and Y.-L. Wang, "Recent advances in event-triggered security control of networked systems: a survey," *International Journal of Systems Science*, pp. 1–20, 2022.

[14] C. Peng and H. Sun, "Switching-like event-triggered control for networked control systems under malicious denial of service attacks," *IEEE Trans. Autom. Control.*, vol. 65, no. 9, pp. 3943–3949, 2020.

[15] M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Secure control of cyber physical systems subject to stochastic distributed dos and deception attacks," *Int. J. Syst. Sci.*, vol. 51, no. 9, pp. 1653–1668, 2020.

[16] A.-Y. Lu and G.-H. Yang, "Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service," *IEEE Trans. Autom. Control.*, vol. 63, no. 6, pp. 1813–1820, 2017.

[17] Y. Zhu and W. X. Zheng, "Observer-based control for cyber-physical systems with periodic dos attacks via a cyclic switching strategy," *IEEE Trans. Autom. Control.*, vol. 65, no. 8, pp. 3714–3721, 2019.

[18] H. Shisheh Foroush and S. Martínez, "On triggering control of single-input linear systems under pulse-width modulated dos signals," *SIAM. J. Control. Optim.*, vol. 54, no. 6, pp. 3084–3105, 2016.

[19] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "Sinr-based dos attack on remote state estimation: A game-theoretic approach," *IEEE Trans. Control. Netw. Syst.*, vol. 4, no. 3, pp. 632–642, 2016.

[20] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," *International Workshop on Hybrid Systems: Computation and Control*, pp. 31–45, 2009.

[21] G. K. Befekadu, V. Gupta, and P. J. Antsaklis, "Risk-sensitive control under markov modulated denial-of-service (dos) attack strategies," *IEEE Trans. Autom. Control.*, vol. 60, no. 12, pp. 3299–3304, 2015.

[22] M. Wakaiki, A. Cetinkaya, and H. Ishii, "Stabilization of networked control systems under dos attacks and output quantization," *IEEE Trans. Autom. Control.*, vol. 65, no. 8, pp. 3560–3575, 2019.

[23] C. De Persis and P. Tesi, "Networked control of nonlinear systems under denial-of-service," *Syst. Control Lett.*, vol. 96, pp. 124–131, 2016.

[24] V. Dolk, P. Tesi, C. De Persis, and W. Heemels, "Event-triggered control systems under denial-of-service attacks," *IEEE Trans. Control. Netw. Syst.*, vol. 4, no. 1, pp. 93–105, 2016.

[25] S. Feng and P. Tesi, "Resilient control under denial-of-service: Robust design," *Automatica*, vol. 79, pp. 42–51, 2017.

[26] S. Feng, A. Cetinkaya, H. Ishii, P. Tesi, and C. De Persis, "Networked control under dos attacks: Tradeoffs between resilience and data rate," *IEEE Trans. Autom. Control.*, vol. 66, no. 1, pp. 460–467, 2020.

[27] Y.-C. Sun and G.-H. Yang, "Periodic event-triggered resilient control for cyber-physical systems under denial-of-service attacks," *J. Franklin Inst.*, vol. 355, no. 13, pp. 5613–5631, 2018.

[28] H. Yang, H. Xu, Y. Xia, and J. Zhang, "Stability analysis on networked control systems under double attacks with predictive control," *Int. J. Robust Nonlinear Control*, vol. 30, no. 4, pp. 1549–1563, 2020.

[29] X.-M. Zhang, Q.-L. Han, X. Ge, and L. Ding, "Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3616–3626, 2019.

[30] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[31] X. Huang and J. Dong, "A robust dynamic compensation approach for cyber-physical systems against multiple types of actuator attacks," *Appl. Math. Comput.*, vol. 380, p. 125284, 2020.

[32] Y. Mo and B. Sinopoli, "Secure control against replay attacks," *Proc. Annu. Allert. Conf. Commun. Control Comput.*, pp. 911–918, 2009.

[33] X.-M. Li, Q. Zhou, P. Li, H. Li, and R. Lu, "Event-triggered consensus control for multi-agent systems against false data-injection attacks," *IEEE Trans. Cybern.*, vol. 50, no. 5, pp. 1856–1866, 2019.

[34] A. Rosich, H. Voos, and M. Darouach, "Cyber-attack detection based on controlled invariant sets," *Proc. Eur. Control Conf.*, pp. 2176–2181, 2014.

[35] E. Eyisi and X. Koutsoukos, "Energy-based attack detection in networked control systems," *Proc. Int. Conf. High confidence networked systems*, pp. 115–124, 2014.

[36] Y. Chen, S. Kar, and J. M. Moura, "Dynamic attack detection in cyber-physical systems with side initial state information," *IEEE Trans. Autom. Control.*, vol. 62, no. 9, pp. 4618–4624, 2016.

[37] A. Khazraei, H. Kebriaei, and F. R. Salmasi, "A new watermarking approach for replay attack detection in lqg systems," *Proc. Conf. Dec. Control.*, pp. 5143–5148, 2017.

[38] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control.*, vol. 58, no. 11, pp. 2715–2729, 2013.

[39] R. Zhao, Z. Zuo, Y. Wang, and W. Zhang, "False data injection attack for switched systems," *IEEE Control Systems Letters*, 2023.

[40] K. Zhang, C. Keliris, T. Parisini, and M. M. Polycarpou, "Stealthy integrity attacks for a class of nonlinear cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 67, no. 12, pp. 6723–6730, 2021.

[41] H. Guo, J. Sun, and Z.-H. Pang, "Stealthy false data injection attacks with resource constraints against multi-sensor estimation systems," *ISA transactions*, vol. 127, pp. 32–40, 2022.

[42] D. Mikhaylenko and P. Zhang, "Stealthy local covert attacks on cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 67, no. 12, pp. 6778–6785, 2021.

[43] G. Park, H. Shim, C. Lee, Y. Eun, and K. H. Johansson, "When adversary encounters uncertain cyber-physical systems: Robust zero-dynamics attack with disclosure resources," *Proc. Conf. Dec. Control.*, pp. 5085–5090, 2016.

[44] Y. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Trans. Autom. Control.*, vol. 61, no. 9, pp. 2618–2624, 2015.

[45] C. Murguia, I. Shames, J. Ruths, and D. Nešić, "Security metrics and synthesis of secure control systems," *Automatica*, vol. 115, p. 108757, 2020.

[46] S. C. Anand, A. M. Teixeira, and A. Ahlén, "Risk assessment of stealthy attacks on uncertain control systems," *IEEE Transactions on Automatic Control*, 2023.

[47] P. Griffioen, S. Weerakkody, and B. Sinopoli, "A moving target defense for securing cyber-physical systems," *IEEE Trans. Autom. Control.*, vol. 66, no. 5, pp. 2016–2031, 2020.

[48] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Revealing stealthy attacks in control systems," *Proc. Annu. Allert. Conf. Commun. Control Comput.*, pp. 1806–1813, 2012.

[49] S. D. Bopardikar and A. Speranzon, "On analysis and design of stealth-resilient control systems," *Proc. Int. Symp. Resilient Control Syst.*, pp. 48–53, 2013.

[50] S. X. Ding, L. Li, D. Zhao, C. Louen, and T. Liu, "Application of the unified control and detection framework to detecting stealthy integrity cyber-attacks on feedback control systems," *Automatica*, vol. 142, p. 110352, 2022.

[51] J. Kim, J. Back, G. Park, C. Lee, H. Shim, and P. G. Voulgaris, "Neutralizing zero dynamics attack on sampled-data systems via generalized holds," *Automatica*, vol. 113, p. 108778, 2020.

[52] M. Naghnaeian, N. H. Hirzallah, and P. G. Voulgaris, "Security via multirate control in cyber–physical systems," *Syst. Control Lett.*, vol. 124, pp. 12–18, 2019.

[53] J. I. Yuz and G. C. Goodwin, "On sampled-data models for nonlinear systems," *IEEE Trans. Autom. Control.*, vol. 50, no. 10, pp. 1477–1489, 2005.

[54] I. G. Polushin and H. J. Marquez, "Multirate versions of sampled-data stabilization of nonlinear systems," *Automatica*, vol. 40, no. 6, pp. 1035–1041, 2004.

[55] X. Liu, H. J. Marquez, and Y. Lin, "Input-to-state stabilization for nonlinear dual-rate sampled-data systems via approximate discrete-time model," *Automatica*, vol. 44, no. 12, pp. 3157–3161, 2008.

[56] X. Liu and H. J. Marquez, "Preservation of input-to-state stability under sampling and emulation: multi-rate case," *Int. J. Control*, vol. 80, no. 12, pp. 1944–1953, 2007.

[57] H. Beikzadeh and H. J. Marquez, "Dissipativity of nonlinear multirate sampled-data systems under emulation design," *Automatica*, vol. 49, no. 1, pp. 308–312, 2013.

[58] A. Üstüntürk, "Output feedback stabilization of nonlinear dual-rate sampled-data systems via an approximate discrete-time model," *Automatica*, vol. 48, no. 8, pp. 1796–1802, 2012.

[59] H. Beikzadeh and H. J. Marquez, "Multirate output feedback control of nonlinear networked control systems," *IEEE Trans. Autom. Control.*, vol. 60, no. 7, pp. 1939–1944, 2014.

[60] J. H. Ahrens, X. Tan, and H. K. Khalil, "Multirate sampled-data output feedback control with application to smart material actuated systems," *IEEE Trans. Autom. Control.*, vol. 54, no. 11, pp. 2518–2529, 2009.

[61] C. Ling and C. Kravaris, "Multirate sampled-data observer design based on a continuous-time design," *IEEE Trans. Autom. Control.*, vol. 64, no. 12, pp. 5265–5272, 2019.

[62] K. J. Åström and B. Bernhardsson, "Comparison of periodic and event based sampling for first-order stochastic systems," *IFAC Proceedings Volumes*, vol. 32, no. 2, pp. 5006–5011, 1999.

[63] P. Tabuada, "Event-triggered real-time scheduling of stabilizing control tasks," *IEEE Trans. Autom. Control.*, vol. 52, no. 9, pp. 1680–1685, 2007.

[64] W. P. Heemels, K. H. Johansson, and P. Tabuada, "An introduction to event-triggered and self-triggered control," *Proc. Conf. Dec. Control.*, pp. 3270–3285, 2012.

[65] Z.-H. Zhang, D. Liu, C. Deng, and Q.-Y. Fan, "A dynamic event-triggered resilient control approach to cyber-physical systems under asynchronous dos attacks," *Inf. Sci.*, vol. 519, pp. 260–272, 2020.

[66] S. Hu, D. Yue, Q.-L. Han, X. Xie, X. Chen, and C. Dou, "Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks," *IEEE trans. Cybern.*, vol. 50, no. 5, pp. 1952–1964, 2019.

[67] L. Gao, F. Li, and J. Fu, "Event-triggered output feedback resilient control for ncss under deception attacks," *Int. J. Control Autom. Syst.*, vol. 18, no. 9, pp. 2220–2228, 2020.

[68] D. Zhao, Z. Wang, G. Wei, and Q.-L. Han, "A dynamic event-triggered approach to observer-based pid security control subject to deception attacks," *Automatica*, vol. 120, p. 109128, 2020.

[69] A. Eslami and K. Khorasani, "Cyber-attack detection by using event-based control in multi-agent cyber-physical systems," in *2023 European Control Conference (ECC)*. IEEE, 2023, pp. 1–6.

[70] X. Wang and G. Feng, "Dynamic event-triggered h-infinity filtering for ncss under multiple cyber-attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2023.

[71] X. Wang, G. Wang, Z. Fei, and Z. Li, "Secure interval estimation for event-triggered cyber-physical systems under stealthy attacks," *IEEE Transactions on Control of Network Systems*, 2023.

[72] G. Chen, Y. Liu, D. Yao, H. Li, and C. K. Ahn, "Event-triggered tracking control of nonlinear systems under sparse attacks and its application to rigid aircraft," *IEEE Transactions on Aerospace and Electronic Systems*, 2023.

[73] Y. Zhang, Y. Ren, and D.-W. Ding, "Resilient control co-design for cyber-physical systems with dos attacks via a successive convex optimization approach," *Journal of the Franklin Institute*, vol. 360, no. 9, pp. 6253–6274, 2023.

[74] N. He, K. Ma, and H. Li, "Resilient predictive control strategy of cyber–physical systems against fdi attack," *IET Control Theory & Applications*, vol. 16, no. 11, pp. 1098–1109, 2022.

[75] L. A. Montestruque and P. J. Antsaklis, "On the model-based control of networked systems," *Automatica*, vol. 39, no. 10, pp. 1837–1843, 2003.

[76] J. Lunze and D. Lehmann, "A state-feedback approach to event-based control," *Automatica*, vol. 46, no. 1, pp. 211–215, 2010.

[77] E. Garcia and P. J. Antsaklis, "Model-based event-triggered control for systems with quantization and time-varying network delays," *IEEE Trans. Autom. Control.*, vol. 58, no. 2, pp. 422–434, 2012.

[78] D. Nešić, A. R. Teel, and P. V. Kokotović, "Sufficient conditions for stabilization of sampled-data nonlinear systems via discrete-time approximations," *Syst. Control Lett.*, vol. 38, no. 4-5, pp. 259–270, 1999.

[79] D. Nešić, A. R. Teel, and E. D. Sontag, "Formulas relating kl stability estimates of discrete-time and sampled-data nonlinear systems," *Syst. Control Lett.*, vol. 38, no. 1, pp. 49–60, 1999.

[80] M. Doostmohammadian and N. Meskin, "Finite-time stability under denial of service," *IEEE Syst. J.*, vol. 15, no. 1, pp. 1048–1055, 2020.

[81] R. Kato, A. Cetinkaya, and H. Ishii, "Security analysis of linearization for nonlinear networked control systems under dos," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 4, pp. 1692–1704, 2021.

[82] D. E. Quevedo and D. Nešić, "Input-to-state stability of packetized predictive control over unreliable networks affected by packet-dropouts," *IEEE Trans. Autom. Control.*, vol. 56, no. 2, pp. 370–375, 2010.

[83] D. M. de la Peña and P. D. Christofides, "Lyapunov-based model predictive control of nonlinear systems subject to data losses," *IEEE Trans. Autom. Control.*, vol. 53, no. 9, pp. 2076–2089, 2008.

[84] H. Yang, H. Xu, Y. Xia, and J. Zhang, "Stability analysis on networked control systems under double attacks with predictive control," *Int. J. Robust Nonlinear Control.*, vol. 30, no. 4, pp. 1549–1563, 2020.

[85] B. A. Bamieh and J. B. Pearson, "A general framework for linear periodic systems with applications to h/sup infinity/sampled-data control," *IEEE Trans. Autom. Control*, vol. 37, no. 4, pp. 418–435, 1992.

[86] Y. Yamamoto, "New approach to sampled-data control systems-a function space method," *Proc. IEEE Conf. Dec. Control*, pp. 1882–1887, 1990.

[87] G. Zhai, B. Hu, K. Yasuda, and A. N. Michel, "Stability analysis of switched systems with stable and unstable subsystems: an average dwell time approach," *Int. J. Syst. Sci.*, vol. 32, no. 8, pp. 1055–1061, 2001.

[88] A. Girard, "Dynamic triggering mechanisms for event-triggered control," *IEEE Trans. Autom. Control*, vol. 60, no. 7, pp. 1992–1997, 2014.

[89] J. Lunze and D. Lehmann, "A state-feedback approach to event-based control," *Automatica*, vol. 46, no. 1, pp. 211–215, 2010.

[90] H. J. Marquez, *Nonlinear control systems: analysis and design*. Wiley-Interscience Hoboken, NJ, 2003, vol. 1.

[91] J. Lunze and D. Lehmann, "A state-feedback approach to event-based control," *Automatica*, vol. 46, no. 1, pp. 211–215, 2010.

[92] R. Sepulchre, M. Jankovic, and P. V. Kokotovic, *Constructive nonlinear control*. Springer Science & Business Media, 2012.

[93] T. Bian, Y. Jiang, and Z.-P. Jiang, "Adaptive dynamic programming and optimal control of nonlinear nonaffine systems," *Automatica*, vol. 50, no. 10, pp. 2624–2632, 2014.

[94] A. Feuer and G. Goodwin, *Sampling in digital signal processing and control*. Springer Science & Business Media, 2012.

[95] T. Chen and B. A. Francis, *Optimal sampled-data control systems*. Springer Science & Business Media, 2012.

[96] R. L. Wheeden and A. Zygmund, *Measure and integral*. Dekker New York, 1977, vol. 26.

[97] M. W. Spong and M. Vidyasagar, *Robot dynamics and control*. John Wiley & Sons, 2008.

[98] H. Ullah, F. M. Malik, A. Raza, N. Mazhar, R. Khan, A. Saeed, and I. Ahmad, "Robust output feedback control of single-link flexible-joint robot manipulator with matched disturbances using high gain observer," *Sensors*, vol. 21, no. 9, p. 3252, 2021.

[99] A. Ilchmann and M. Mueller, "Time-varying linear systems: Relative degree and normal form," *IEEE transactions on automatic control*, vol. 52, no. 5, pp. 840–851, 2007.

[100] T. Berger and A. Ilchmann, "Zero dynamics of time-varying linear systems," *Preprint available online, Institute for Mathematics, Ilmenau University of Technology*, pp. 10–05, 2010.

[101] T. Berger, A. Ilchmann, and F. Wirth, "Zero dynamics and stabilization for analytic linear systems," *Acta Applicandae Mathematicae*, vol. 138, no. 1, pp. 17–57, 2015.

[102] H. J. Marquez, *Nonlinear control systems: analysis and design*. Wiley-Interscience Hoboken, NJ, 2003, vol. 1.

[103] A. Nazarzadeh and H. J. Marquez, "Secure nonlinear sampled-data control system against stealthy attack: Multi-rate approach," *IEEE Trans. Autom. Control*, early access. doi: 10.1109/TAC.2023.3256764.

[104] M. Sampei and T. Kobayashi, "Applications of nonlinear control theory to path tracking control of articulated vehicles with double trailers," *IFAC Proceedings Volumes*, vol. 26, no. 2, pp. 129–132, 1993.