Cyber-physical Security of Control Systems

by

Mahsa Taheri

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

Master of Science
in
Control Systems

Department of Electrical and Computer Engineering

University of Alberta

Abstract

In recent years, Networked Control Systems have become prevalent and replaced hard wired systems. After widespread use of wireless networks and computers in control systems, a significant challenge emerged in this domain: *security*. As cyber security is insufficient in addressing the consequences of the cyber threats in control systems, cyber-physical security came into attention in which various aspects of the control system such as stability and performance under possible attacks can be investigated. One of the most common and attainable attacks is denial-of-service (DoS). In this thesis, we consider input-output stability and performance of networked control systems under DoS attack. We show that under certain conditions on the DoS attack, input-output stability is preserved at the expense of a deterioration of the $\mathcal{L}_2$ gain. The scheme is resilient enough to present a good perspective of different implementation options and enable the designer to balance the trade-off between performance and the allowable duration of the attack into consideration.

Preface

Chapter 3 has been submitted for publication in the article: M. Taheri and H. J. Marquez, "Finite Gain $\mathcal{L}_2$ Stability Analysis of a Control System Under DoS Attack", *IET Control Theory and Applications*. I was responsible for the main idea, analysis, design, mathematical derivations, simulation part and also the work drafting. Dr. Marquez contributed in 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 and brother
for their endless love and support

Acknowledgements

Firstly, I would like to express my sincere gratitude to my supervisor, Professor Horacio. J. Marquez, for his guidance and support during my graduate studies. To my committee, Dr. Mahdi Tavakoli and Dr. Qing Zhao, I am extremely grateful for your assistance and suggestions throughout this study.

I have been so fortunate for making nice friends during this journey. I especially want to thank my dearest friends Negar & Mostafa, Faezeh & Mohsen and Shahed for their friendship, support and encouragement.

Last but not least, my deepest love and gratitude goes to my parents and brother for their unconditional love, support and patience in all my lifetime.

Mahsa Taheri
Edmonton, Alberta
Canada

Contents

List of Tables

List of Figures

Notation

$\mathbb{R}$, $\mathbb{C}$	The sets of real, integer and complex numbers
$\mathbb{R}^+$, $\mathbb{N}$, $\mathbb{R}_0^+$, $\mathbb{N}_0$	The sets of positive and nonnegative real and integer numbers
$\mathbb{R}^n$	The set of real n-dimensional vector
$\mathbb{R}^{n\times m}$	The set of real $n \times m$ matrices
$\mathcal{L}_p$ or $\mathcal{L}_p^n$	Space of n-dimensional functions with well-defined p-norm
$\mathbf{C}^0$, $\mathbf{C}^1$	Class of continuous, continuously differentiable functions
$\forall$	Universal quantifier
$x \in X$	x is an element of set X
$X \subset Y$	X is a subset of Y
A^T	Transpose of matrix or vector 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 or $\mathbb{I}_n$	Identity matrix of dimension n
$\|\cdot\|$ or $\|\cdot\|$	Euclidean norm of a vector or matrix
$\|\cdot\|_\infty$ or $\|\cdot\|_\infty$	∞-norm of a vector
$\|z\|_2$ or $\|z\|_{\mathcal{L}_2}$	$\mathcal{L}_2$ norm of signal $z : \mathbb{R}_0^+ \to \mathbb{R}^n$, defined as $\|z\|_2 = (\int_0^\infty \|z(t)\|^2 dt)^{\frac{1}{2}}$
$\|z\|_\infty$ or $\|z\|_\infty$	∞-norm of signal $z : \mathbb{R}_0^+ \to \mathbb{R}^n$, defined as $\|z\|_\infty = \sup\{\|z(t)\| : t \geq 0\}$ and $\chi_\mathcal{A}(s) = 0$ otherwise
$A \backslash B$	set of all the elements in A which do not belong to B

Abbreviations

LHS	Left Hand Side
RHS	Right Hand Side
LTI	Linear Time-Invariant
TC	Triggering Condition
ISS	Input-to-State Stability
ZOH	Zero-Order Hold
ETC	Event-Triggered Control
ETM	Event-Triggered Mechanism

Chapter 1

Introduction

This thesis explores cyber-physical security of control systems under attacks. The purpose of this research is to analyze stability and performance of a cyber-physical system subject to denial-of-servie (DoS) attack. In this chapter, we provide an overview of the subject along with some preliminary background, overview of the literature, define the research motivations, and summarize the main contributions.

1.1 Literature review

Different from the faults that randomly happen in the system, attacks may have access to the system model and data through eavesdropping, faults or leaked information, and so on. By means of this knowledge, more intelligent and harmful attacks can be designed [1]. In an attempt to put cyber attacks into the perspective, they can be broadly classified into three major groups, discloser attacks, deception attacks, and disruption attacks [1]. Disclosure attack corresponds to interferences that involve eavesdropping of the data [2]. Deception attack manipulates the trustworthiness of the data and corrupts the signals (e.g. false-data injection [3]), and disruption attacks refer to the intrusion which cause delay or blockage in the signal (e.g. Denial of service [4]). Mapped to the attacker perspective mentioned above, comes the defender perspective in which the security goals can be viewed as three general classes of confidentiality, integrity and availability. [5–8] .

The defender's perspective is of high importance in cyber-security notion. Guaranteeing desired overall security of a system is complex. In an ideal case, the most complete mechanism for security of the overall system consists of three stages. In the first place, if feasible, it is better to prevent the occurrence of the attack. In this stage, attacks can be postponed or inhibited. Using prevention methods, still some attacks can happen. Thus, during the attack, "resiliency" helps to maintain the performance of the system close to

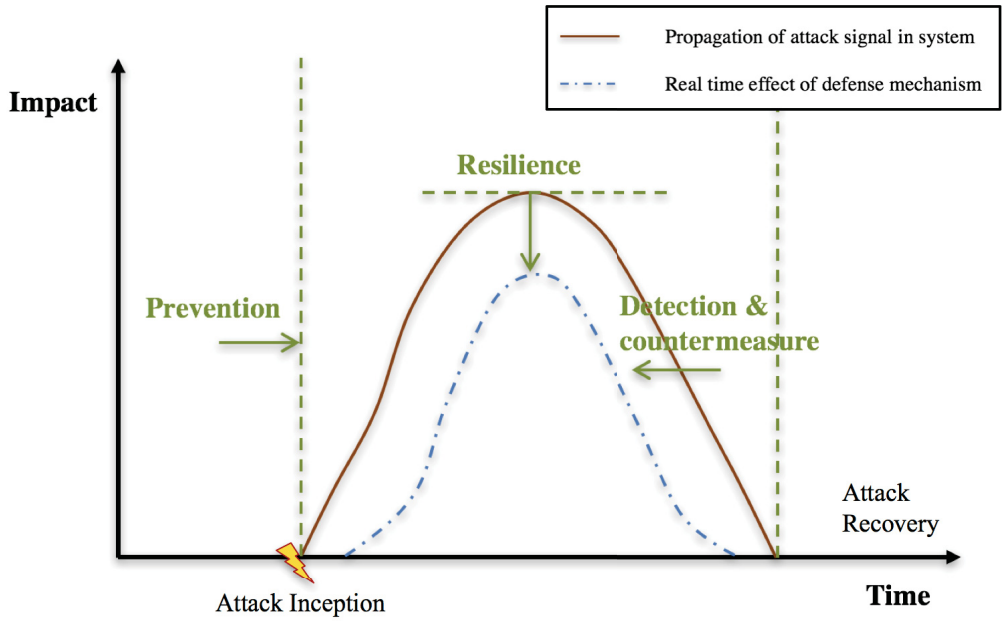

Figure 1.1: Different phases of an overall defense mechanism in security of CPS, which includes prevention, resilience and detection and countermeasure.

normal (in a reasonable level) in the interval between the start of attack and detection and recovery mechanism. Therefore, significant impacts on the system can be minimized in the occurrence of attacks. By the latter, the source of the attack can be identified and the system can be recovered into the normal mode by corresponding recovery actions [9]. Figure 1.1 illustrates these three phases of defense mechanism in an overall defense scheme for a cyber-physical system. In what follows, the tools and results represented in the literature under this three main category is discussed.

1. **Prevention:** In this stage, approaches are targeting against disclosure attacks that start from penetration in the system to steal information and use them in future attacks. The defense mechanism in this group can be classified into Cryptography and Randomization. The former has been comprehensively studied in the computer-science notion [10]. But the latter is rooted in control theory and has a strong history in robust control [11]. Here, we focus on the results presented in randomization. Randomization is a method based on confusing potential attackers and prevent them from predicting the deterministic rules and gaining access to the vital information of the system. It is proven to be useful as a robust control technique [11, 12]. Ran-

domization of data is a very prevalent method whenever confidentiality is aimed to be kept. In [13], the private data is masked in the presence of a malicious agent. The non-adversarial agents use the masked data with a noise and gain the correct states and compute the average consensus. In [14], a random gain selection method is suggested to guard the closed loop control system against disclosure attacks targeting the control rule.

2. **Resilience:** Resilience is defined as a property that enables the system to tolerate severe conditions resulted from natural faults or deliberate attacks [15]. Resilience of a system against adverse conditions usually needs to be strengthen via proper design of the control system. There are numerous methods in literature for increasing the resilience. Below, is the main three groups of approaches used in cyber-physical security literature for increasing the resilience of systems.

   (a) Game-Theory Methods: The goal in game theory methods is to minimize the impact of an attack on the system. In game theory, two or multiple players interact to optimize their own objective function and this optimization depends on the choices made by each player and cannot be done separately. Game theory has a rich literature in security of the systems. This method addresses two main perspective regarding the structure of the cyber-physical system or the type of attack on cyber layer. In the former, security game is modeled based on the cyber and physical structure of the system [16–20]. It consist of two interconnected games in the physical layer and the cyber layer.

   Another perspective corresponds to the type of the attack on the system [21–23]. Specifically speaking, suitable game strategy is chosen with regards to whether the malicious behavior is either active or passive. The Stackelberg game is well suited for the case of a jammer and a passive defender. Whereas, when there is an active defender, Nash equilibrium is a reasonable choice [24, 25]. Another passive attacker example is when an eavesdropper gains access to information from a communication channel leakage. Here, the eavesdropper can be modeled as a follower in a Stackelberg game with an active defense [26]. Moreover, in [27, 28] a game framework for networks with unknown topology is considered in which the defender tries to reach synchronization and while mitigating the attack signal from malicious agents.

(b) Mean Square Reduced (MSR) Algorithms: In MSR approach, the control input is computed at each update time in order to ignore doubtful values to attenuate the effects of attack on the system. A famous application of MSR method is against Byzantine threats where malicious information is sent to the neighbor nodes by byzantine nodes [29, 30]. This algorithm have been used in distributed computational problems, such as synchronization [31], state estimation [32],consensus [33, 34], and optimization [35]. In MSR approach, each node ignores a certain number of largest and and smallest values from neighbors and therefore the global topology knowledge is not needed. Hence, unlike detection-based approach, it does not require heavy computation load in each node [36].

(c) Event-triggered Control: In event-triggered approach, in contrast to time triggered techniques, data is sent to communication channels only when it is needed and generating new control input is based on a triggering function which depends on the errors of state variables. Event-triggered schemes are used to increase the resiliency based on the frequency of attacks occurrence. [37] is an introduction to event-triggered control. It is a suitable approach to mitigate the impact of disruption attacks (e.g. jamming or DoS) in networked control systems. Event-triggered technique is used in order to guarantee the input to state stability of the closed-loop systems in the presence of attack, whose frequency and length is limited [4]. In [38–41] more application of event-triggered control for resiliency of the networked control systems has been studied. Several references deal with resilient control under DoS attack implemented in an event-triggered fashion, [4, 38, 39, 42–45]. In [42] and [43] a method is proposed to improve the scheduling time of control updates by means of avoiding the DoS periods. This method is effective when the DoS attack is structured over time, e.g., pulse-width or periodic jamming signals. In [38, 39], a more realistic model of DoS attack is considered based on the frequency and duration of denial intervals. By adopting the ETC framework, these references propose a scheme that guarantee system stability in the presence of DoS attack. In [4], input-to-state stability in the presence of a bounded disturbance is analyzed. In [44] and [45], output feedback control of systems in the presence of DoS attack is considered with a focus on $\mathcal{L}_\infty$ stability analysis under DoS attack.

3. **Detection and isolation:** The other important constituent of defense mechanism is detection and isolation which focuses on detecting the attacks and recovering the system during occurrence of attacks. Detection is usually based on monitoring the impact of attacks on output of the system. When the effect of attack is not evident in the output, it is called stealthy [46] or covert attack [1]. Majority of methods proposed for detection and isolation in the literature can be classified into three groups as follows:

   (a) Observer-based techniques: The goal of observers is to estimate inaccessible states. By comparing the resulted state estimates in normal and attacked situations-termed residue- detection can be done whenever the residue surpass a certain threshold. [47] provides a unified model for deception and disruption attacks based on linear algebraic conditions for detection and identification of the attacked sets. This idea is extended to the multi-agent systems in the presence of malicious nodes in [36, 48, 49]. In these methods, considerable amount of computational complexities and memory is taken due to different matrices for prediction and detection.

   A subset of observers when the model is static is prevalent in power systems where measurements of current and voltage needs to be estimated. References, [50–53] provide robust signal processing technique such as Least Trimmed Squares (LTS) for minimizing the residue.

   (b) Watermarking: Watermarking is a well known concept in authentication of entities. This approach has been very successful in detecting replay attacks. When an attacker records the sensor data in a time period and replays it again, the attack is referred to as replay attack. Therefore, since the normal data is sent back to monitors, the operator is tricked to think that system is working normally [54]. The idea here is to add a perturbation to the optimal input of the system and by monitoring the output for traces of the perturbation, the replay attack would be detected. This idea extended to the SCADA networks and multi-agent systems for detecting replay attacks respectively in [55] and [56]. In contrast to the additive perturbation, in [57], a sensor multiplicative watermarking technique is applied to detect replay attacks. The same approach is used in [58] to detect routing attack where an intentional swapping between sensors wires happens.

(c) Learning-based Detection and signal reconstruction: This method roots in computer networks for anomaly detection. However, due to its efficiency, its utilization in control systems has been significantly increased. This technique has been introduced in power systems in [59]. Anomaly detection in the presence of attack has been investigated by the means of Neural Networks(NNs) and Bayesian learning in [60–62]. In [63, 64] methods for localizing attacks in power systems is proposed. In [65, 66] a recursive distributed kalman filter is developed in the presence of sensor attacks. Alongside, in [67] , a new technique which is a combination of data-driven methods and traditional resilient estimation is proposed in which signals are reconstructed to remove the effects of attack.

1.2 Research Motivation and Objectives

Control systems have traditionally been designed assuming that the information flow coming from the sensors can be used to make decisions that affect plant operation. More recently, however, Networked Control Systems (NCSs) have replaced classical hard wired systems with more flexible and easy to reconfigure networked interconnections between subsystems. Networked control systems eliminate unnecessary wiring reducing the complexity and the overall cost in control implementations. One important problem that has emerged as a consequence of the massive use of computer networks in control, however, is the possibility of cyber threats, particularly in safety-critical areas such as power networks and intelligent transport systems, forcing designers to incorporate control strategies that guarantee stability and possibly some level of performance in the presence of cyber attacks [68, 69].

This, in turn, have brought up the necessity of investigation of various aspects of cyber-physical systems' security; from attack models to methods for ensuring the resilience of the system. There are many attacks reported in the industrial systems in the last few years such as, stuxnet [70] and Maroochy attack [71] . Cyber attacks in Networked control systems can be broadly classified as *deception attacks* and *denial-of-service* (DoS) attacks. While the former manipulate the trustworthiness of the data transmitted over the network [1, 3, 72], the later affect the timeliness of the data transmission to cause packet losses or preventing communication over time intervals of random duration over the network channels [1], [73–75]. In this thesis, we focus on DoS attacks.

Our starting point is the universal property that a control network must have *integrity*, *i.e.* it should have some resilience to the effect of cyber attacks and remain operational during their occurrence. Remaining operational imply not only retaining *stability*, but

also some level of acceptable performance that allows the network to operate during the attack and to recover post attack. Consistent with current trends and to maintain network communication as low as possible, we cast our analysis and solution in the context of event-triggered control (ETC) which limits the transmission of the data by proposing triggering rules dependent on sensor measurements. Several reference deal with resilient controls under DoS attacks implemented in an event-triggered fashion, [4, 38, 39, 42–45].

1.3 Thesis Outline

The rest of this thesis is organized as follows.

Chapter 2: This chapter Provides an overview on denial-of-service (DoS) attacks in networked control systems. Different types of DoS existed in different forms of networks are introduced. We discuss the recent works have been done on control of cyber-physical systems under DoS attacks. There are also different approaches on modeling the denia-of-service in order to capture the uncertainty nature of these attacks. The model used in this thesis would be discussed in details.

Chapter 3: In this chapter, we consider input-output stability and performance of networked control systems under Denial-of-Service (DoS) attack. We show that under certain conditions on the DoS attack, input-output stability is preserved at the expense of a deterioration of the $\mathcal{L}_2$ gain. The scheme is resilient enough to present a good perspective of various implementation options and enable the designer to balance the trade-off between performance and the duration of the attack into consideration. At last, the results are illustrated by a numerical example.

Chapter 4: A summary and conclusion is provided along with research plan for future works.

Chapter 2

Denial-of-Service Attack

Communication networks are inevitable components of many industrial control systems. The necessity of data transmission to remote locations in control systems has led to an enormous increase in using wireless networks and the Internet. Recent rapid growing developments in the Internet of Things is an indication to expect even more increase in utilization of the wireless technologies in the control systems. Although these new developments are improving the efficiency of control systems, they are also making them more vulnerable towards cyber attacks. Widespread utilization of control systems in various safety-critical infrastructures such as power grids and transportation demands guaranteed reliability and availability of the networks. Attacks against these systems in the absence of proper security mechanism can lead to real-world damage to environment, safety and health of the people and substantial financial losses [76].

There are different security issues concerned with network control systems as investigated in [5–8], [72], [7]. Attacks are performed with different approaches on control systems based on the purpose and amount of knowledge of the attacker. As investigated in aforementioned works, the content of the control or measurement data can be changed during the attack. Also attackers may be able to inject false data into the system and remain stealthy. These attacks requires knowledge on the system dynamics as well as communication protocol. The more an attack becomes smarter, the more information and knowledge of the system is required. On the other hand, denial-of-service (DoS) can prevent transmission of the data while it requires least amount of information about the system. Therefore, DoS can be one the most common and at the same time severe source of damage and performance issues for the systems. DoS attacks can occur differently in different networks. Here, two types of Denial-of-service including packet drops by malicious nodes in multi-hop networks and jamming attacks in wireless networks is discussed.

In a healthy multi-hop network, data packets are transmitted to the remote nodes by means of intermediate ones as routers. Whereas by introducing malicious nodes to the network, it can face packet drops in various forms such as *blackhole* and *grayhole* DoS attacks. In blackhole attack, the malicious node introduces itself as having a shortest route to the destined node. Therefore, by creation of a path through the malicious node for transmission of the packets, it drops the packets instead of forwarding them the remote node. An extension to blackhole attack is grayhole attack in which the behavior of the malicious node is very unpredictable. In this scenario, malicious node acts in a way that makes its detection very difficult. It may drop packets received from certain nodes while forward all other packets. Furthermore, the node may behave maliciously for certain amount of time and then switch back to healthy behavior afterwards. The combination of these two types is also possible, i.e. the malicious node would drop packets from certain nodes in a certain time [77], [78].

Another type of denial-of-service is jamming attack in wireless channels. Jamming attacker tend to prevent the transmission of packets by emitting strong interference signals into a wireless network. Because of the easiness of generating jamming attack and its ability to target various wireless technologies such as GPS, Wi-Fi and mobile communication, it can be a main concern in control systems security. Jamming attack can operate in both the physical layer and medium access control layer (MAC) [78]. In physical layer the jammer do not have to follow any rules of the protocol, by simply emitting radio signals on the wireless medium it tend to corrupt the packets at the receiver or by making a legitimate transmitter sense the channel busy and thus inhibit it to gain obtain access to the channel. [79]. In the case of MAC layer, by exploiting the vulnerabilities of current standards, such as the popular IEEE 802.11, the attacker would be able to corrupt a single bit with sending just enough power and as a result the received packet would fail the cyclic redundancy checks (CRC).

DoS attack have been investigated in different problems such as feedback control, state estimation and consensus. Here, we discuss DoS attack in feedback control problems.

2.1 Control Problem

In the context of networked control problems, plant and controller communicate over a network which is exposed to DoS attack in the form of malicious packet-drops and jamming. The dynamic of the system would be described by linear-continuous system as

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t), \quad x(0) = x_0, \quad t \geq 0 \\ y(t) &= Cx(t) \end{aligned} \tag{2.1}$$

In [4,39], the control scheme is implemented in the context of event-triggered systems. The measured states are transmitted over the network in time instants of $t_j, j \in \{0, 1, 2, ...\}$. Since the network may be exposed to DoS attack, some of the transmission attempts may be unsuccessful. Thus, the control input of the system is given by

$$u(t) = Kx(t_{j(t)}) \tag{2.2}$$

where $j(t)$ is the index for the last successful transmission time. In [4, 39], the control input is held constant between two successful control updates and is not assumed to be zero during the failure of data transmission.

Several reference deal with resilient controls under DoS attacks implemented in an event-triggered fashion, [4, 38, 39, 42–45]. In [42] and [43] a method is proposed to improve the scheduling time of control updates by means of avoiding the DoS periods. This method is effective when the DoS attack is structured over time, e.g., pulse-width or periodic jamming signals. In [4,39], a more realistic model of DoS attack is considered based on the average duration and frequency of the attack. In these works the strategy of the attack is considered to be unknown. This model is further discussed in section 2.2 . By adopting the ETC framework, these references propose a scheme that guarantee system stability in the presence of DoS attack. In [4], input-to-state stability in the presence of a bounded disturbance is analyzed.

In the context of output feedback control, there are approaches investigated in [44, 45, 80–82] . In [44] and [45], output feedback control of systems in the presence of DoS attack is considered with a focus on $\mathcal{L}_\infty$ stability analysis under DoS attack. In [80, 81] by using a predictor and an impulsive observer at the controller side, an approach is provided to mitigate the capabilities of the attack. In [82], it is assumed that the outputs are measured by multiple sensors and transmitted over multiple channels.

In [45,83], the system is considered to be nonlinear. In [83], the state feedback control of the system under DoS attack is investigated. Output feedback control of nonlinear system in event-triggered scheme is explored in [45]. Moreover, by developing a linearization approach in [84], stabilization of the nonlinear system is achieved. In this case, if the DoS attack gets very strong, it can make the states leave the linearization region and thus, cause instability

in the system. In [85], an adaptive controller is proposed to guarantee the stability of a system that contains unknown nonlinear function.

In the domain of distributed systems, a method is proposed in [86] to mitigate the effect of DoS by switching the strategy of transmission between round-robin protocol and event-triggered.

Contrary to previous references, in this work our focus is on $\mathcal{L}_2$ stability and performance. Our interest is in establishing conditions under which (i) $\mathcal{L}_2$ stability is preserved, and (ii) the closed loop $\mathcal{L}_2$ gain of the system remain within certain limits. With respect to the second objective, our interest is to better understand the tradeoff between the duration of the attack and the deterioration of the control properties, measured in $\mathcal{L}_2$ gain sense. Some work related to our objectives were reported in reference [87]. In this reference the authors consider an event-triggered $\mathcal{H}_\infty$ load frequency control for power systems with energy-limited DoS attacks. The disturbance in this work, is assumed to be upper bounded by a linear function of the state norm.

2.2 Deterministic Modeling of DoS attack

There are various modeling approaches for denial-of-service attacks in the literature. We can divide the methods into two main categories of probabilistic and deterministic approaches. The former is extended along of the probabilistic modeling of data transmission failures in networked control system due to non-malicious issues. These failures are usually modeled with stochastic processes such as Bernoulli and Markov processes. In [40], non-malicious data transmission failures and DoS attack is modeled using probabilistic methods.

In this Section, our attention is focused on deterministic modeling approach of DoS attack which is also the basis of modeling in this thesis. As shown in [39], proposed deterministic model allows the denial-of-service to occur in an arbitrary fashion. In this approach, the total duration of the attack in a certain amount of time interval is upper-bounded with a deterministic function of that interval's length.

In the continuous-time context, the modeling is as follows. For denoting the starting time and the duration of each attack interval, two sequences are considered respectively such as $\{h_n \geq 0\}_{n\in\mathbb{N}_0}$ and $\{\tau_n \geq 0\}_{n\in\mathbb{N}_0}$. At the nth attack interval, DoS attack transition from off to on occurs at the time h_n and lasts for τ_n. For avoiding overlapping of consecutive attack intervals, it is assumed that $h_{n+1} > \tau_n + h_n$. In Figure 2.1, a sample of sequence of DoS attack intervals is illustrated.

This model is very well compatible with the jamming scenario, in which the communi-

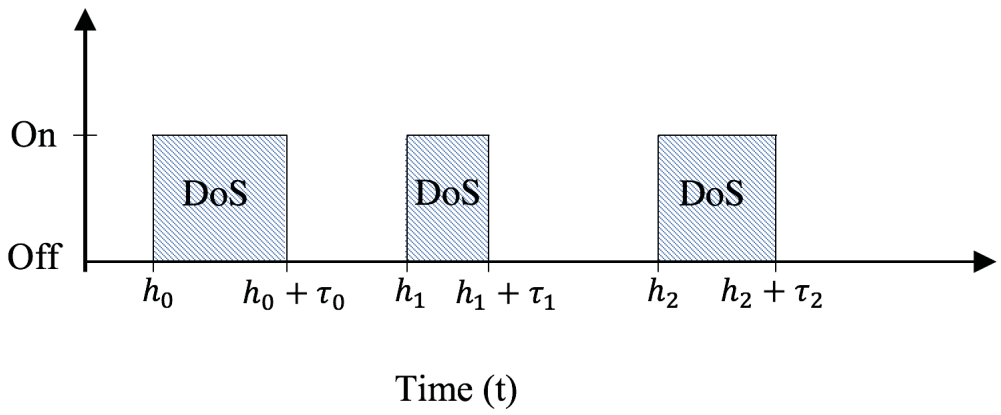

Figure 2.1: Example of a DoS attack sequence.

cation channels may be exposed to a very strong jamming radio signals in the intervals of $[h_n, h_n + \tau_n]$. When a data transmission time occurs in any of the attack intervals, a data transmission failure happens at that time.

It is also helpful to define a notation for total attack duration. For any time interval of $[\tau, t]$, the set of DoS attack occurring times is denoted by

$$\mathcal{A}(\tau, t) = \bigcup_{n \in \mathbb{N}_0} [h_n, h_n + \tau_n] \bigcap [\tau, t]. \tag{2.3}$$

Also, the total duration of the attack in the same interval is denoted by $|\mathcal{A}(\tau, t)|$.

If the DoS attack cover the whole time span, it would be $|\mathcal{A}(0, t)| = t$ for all $t \geq 0$. In these cases, the communication is not possible in the networks. In practice, attackers face some constraints that limit their capabilities and prevent them from attacking continuously at all times. For instance, emitting strong jamming signals are costly [78]; thus, due to the energy resources limitations that attackers may face, they typically cannot attack at all the time span. Moreover, attacking without any constraints would reveal the presence of attack in the system. Therefore, strategic attackers avoid attacking continuously to be able to remain stealthy.

These practical constraints are taken into account in [39] by considering the following assumptions.

Assumption 1. There exist scalars $\kappa_D \geq 0$ and $\rho_D \in [0, 1)$ such that

$$|\mathcal{A}(0, t)| \leq \kappa_D + \rho_D t, \tag{2.4}$$

for $t \geq 0$. Equation (2.4) implies that scalar ρ_D performs as an upper-bound for average ratio of the total attack duration to the total time interval in the long run, since

$lim sup_{t\to 0}|\mathcal{A}(0,t)|/t \leq \rho_D$. The scalar κ_D is used to model the ability of the attacker at the initial time. When the first attack interval starts at $h_0 = 0$, Equation (2.4) imposes an upper-bound on the first attack interval τ_0 as $\tau_0 \leq \kappa_D/(1-\rho_D)$.

In stability analysis of networked control systems in [39], assumption 1 is considered. In [4], an additional constraint is also assumed on the frequency of the attack. The assumption is as follows.

Assumption 2. There exist scalars $\kappa_F \geq 0$ and $\rho_F \in [0,1)$ such that

$$n(0,t) \leq \kappa_F + \rho_F t, \tag{2.5}$$

for $t \geq 0$, where $n(\tau,t) \in \mathbb{N}_0$ is the number of attacks in the time interval of $[\tau,t]$.

In Equation 2.5, scalar ρ_F serves an upper-bound for frequency of the attack in the long run. In networked control systems with periodic transmission, the frequency of attacks requires to be upper-bounded by a small enough scalar ρ_F. It would become more clear if assuming to have a transmission period such as δ. An attacker aware of δ, can set the attacks to locate periodic transmission times with even short duration of attack intervals. In such cases, if $\rho_F \geq \frac{1}{\delta}$, all data transmission attempts can fail and stability of the system can not be achieved.

When there is disturbance in the system dynamics, Assumptions 1 and 2 are not sufficient [4]. The reason is, Assumptions 1 and 2 allows the attack to be activated continuously for long period of time until Equations (2.4) and (2.5) are not violated. For achieving this scenario the attacker can wait for a long duration of time and start attacking continuously afterwards. In such cases, data is transmitted successfully in the initial attack-free period, however because of the presence of disturbance, states never reach to zero. After onset of the attack, it can be continuously active until it cause the states to grow to very large values. Therefor, for avoiding such scenarios, more restricted version of Assumptions 1 and 2 are considered in [4], in which the maximum length of continuous attack would be bounded. Following are the new inequalities

$$\begin{aligned} |\mathcal{A}(\tau,t)| &\leq \kappa_D + \rho_D(t-\tau) \\ n(\tau,t) &\leq \kappa_F + \rho_F(t-\tau) \end{aligned} \tag{2.6}$$

for all $\tau, t \in \mathbb{R}_{\geq 0}$ and $t \geq \tau$.

Average duration and frequency in Equation (2.6) are used in [4, 80, 81] to model DoS attacks in networked control systems. In [4], a sufficient condition is achieved to guarantee asymptotic stability of control systems under attacks which satisfy Assumptions 1 and 2

with Equation 2.6 in event-triggered control scheme. The condition is as follows

$$\Delta^* \rho_F + \rho_D \leq \omega \tag{2.7}$$

in which scalar $\omega \geq 0$ depends on system dynamics parameters and the scalar $\Delta^* \geq 0$ is an upper-bound for intervals between data transmission instants. In [4], Input-to-state stability of networked control system in the presence of disturbance is shown to be guaranteed under conditions with equations (2.6). In [80, 81], authors have shown that by using predictors and buffers in the control system, the condition on DoS 2.7 can get more relaxed. It is worth to mention that the scalars κ_D and κ_F in Equations (2.4) and (2.5) or (2.6) does not affect stability of the linear systems. They only play a role in state trajectory bounds and performance of the system. However, in nonlinear case, they also affect on stability properties of the system.

There are also other deterministic methods for modeling DoS attack. For instance, in [42], DoS attack is modeled as a pulse-width modulated (PWM) signal. It consists of periodic sleeping and jamming cycles. In this case, each cycle of the DoS signal consists of T_j seconds of jamming followed by T_s seconds of sleeping. Since the modeling approach in [4] allows more generality for the DoS attack, we proceed our work by considering that method as our bases for stability analyses of the system.

2.3 Event-Triggered Control

Event-triggered control is one of the most prevalent approaches in control of networked systems under DoS attack. In [4], the event-triggered control approach is utilized to obtain asymptotic stability under any DoS attacks that satisfy Assumptions 1 and 2. When the error between the last transmitted state and current state exceeds a threshold, the transmission of state is triggered. In this approach, for checking the event-triggered condition, state of the system needs to be continuously monitored. Self-triggering is a method to avoid monitoring continuously. In [4], a self-triggering approach is also proposed to in which the predicted value of the state is used to determine the next transmission time. Some of the transmissions may fail due to the presence of DoS attack in communications channels. By using Lyapunov function techniques, the global asymptotic stability of the overall system in [4] is guaranteed under sufficient conditions related to event-triggering and DoS characteristic parameters.

Our approach will be cast in the context of event-triggered control. Several references have studied the event-triggered $\mathcal{L}_2$-gain control problem. In [88], finite gain $\mathcal{L}_2$ stability of

event-based LTI systems is investigated using a full information $\mathcal{H}_\infty$ controller. Reference [89] extends the results of [88] and derives explicit lower bounds for the sampling periods. The disturbance in this reference is assumed to be bounded by the norm of the state. In [90], this assumption is relaxed. In references [91] and [92], event-triggered output feedback controller is proposed to guarantee finite gain $\mathcal{L}_2$ stability of the closed-loop system. Reference [93] considers the nonlinear $\mathcal{L}_2$ problem. More recently, references [94–96] study the event-based $\mathcal{L}_2/\mathcal{L}_p$ stability of general nonlinear systems. As previously mentioned, most of the literature on stability of NCS under DoS attack deals with disturbances which belong to $\mathcal{L}_\infty$ and are bounded. In contrast, this paper considers $\mathcal{L}_2$ disturbances that are only bounded in energy and no assumptions are made on the boundedness of their magnitude. Our main contribution is the analysis of finite $\mathcal{L}_2$ gain of the closed loop system under Denial-of-Service attack. By deriving an explicit finite $\mathcal{L}_2$ gain, one can get a better understanding of impact of DoS attacks on system performance.

Most of the aforementioned works so far in ETC of systems under DoS attack, are based on emulation approach. In this method, the controller or observer gain is designed in advance, hence the design would be restricted to the initial choice of this parameters. In [87] and [40] co-design method for designing control law and the event-triggered condition under DoS attack is proposed. In [97] the effect of quantization errors is also considered in a NCS system under periodic DoS attack. This work has been extended to a more general type of DoS attack in [98].

Chapter 3

$\mathcal{L}_2$ Stability Analysis of Event-Triggered Control Systems Under DoS Attack

3.1 Preliminaries

We first introduce the notation used throughout the rest of the paper. $\mathbb{R}$ represents the field of real numbers and $\mathbb{R}^n$ the n-dimensional vectors with elements in $\mathbb{R}$. Given $\alpha \in \mathbb{R}$, $\mathbb{R}_{>\alpha}$ ($\mathbb{R}_{\geq\alpha}$) represents the set of real numbers greater than (greater than or equal) to α. $\mathbb{N}$ and $\mathbb{N}_0$ represent the set of natural numbers and nonnegative integers, respectively. $\|.\|$ is Euclidean norm of a vector in $\mathbb{R}^n$. Given sets A and B, $A\backslash B$ indicates the set of all the elements in A which do not belong to B.

3.1.1 System Dynamics

Throughout this paper we will consider a linear time-invariant system described as follows

$$\dot{x}(t) = Ax(t) + B_1u(t) + B_2w(t) \tag{3.1}$$

where $t \in \mathbb{R}_{\geq 0}$, $x \in \mathbb{R}^n$ is the state and $u \in \mathbb{R}^m$ is the control signal. $w \in \mathbb{R}^n$ is an external disturbance that is assumed to belong to $\mathcal{L}_2$. A and B are matrices with appropriate dimensions.

The control law is implemented in an event-based fashion over a network. The basic mechanism is represented in Figure 3.1. When the event condition is satisfied, event detector updates the control signal and the actuator receives the updated control input.

Assume the event time instants are denoted by the sequence $\{t_j\}_{j\in\mathbb{N}_0}$, starting from $t_0 = 0$. The control signal is held constant between two successive updates. Thus, the control input can be defined as follows:

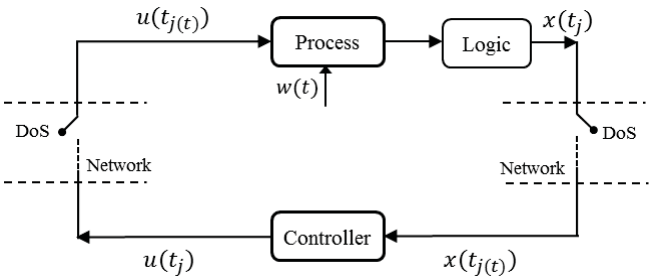

Figure 3.1: Event-triggered mechanism of the closed-loop system and DoS attack.

$$u(t) = kx(t_j) \qquad t \in [t_j, t_{j+1}). \tag{3.2}$$

3.1.2 DoS and Control

Denial-of-service can interrupt communication between system components by preventing (3.2) from being updated at the desired times. We consider a scenario in which DoS attacks simultaneously affect measurement and control channels. Thus, in the presence of DoS, data cannot be sent or received. We consider a more general framework describing DoS attack [38]. Let $\{h_n\}_{n\in\mathbb{N}_0}$ represent the time instants of DoS off/on transitions. Then

$$H_n = \{h_n\} \cup [h_n, h_n + \tau_n[$$

represents the nth DoS interval with the length of τ_n over which communication is denied.

Thus, the attack and non-attack intervals can be represented as follows

$$A(\tau, t) = \bigcup_{n\in\mathbb{N}_0} H_n \bigcap [\tau, t]$$
$$N(\tau, t) = [\tau, t] \backslash A(\tau, t)$$

where for each interval $[\tau, t]$, $A(\tau, t)$ and $N(\tau, t)$ represents the time intervals in which communication is not possible and is allowed, respectively. Therefore, the control input in the presence of attack can be stated as follows:

$$u = kx(t_{j(t)}) \tag{3.3}$$

where $j(t)$ represents the last successful control update, defined as follows:

$$j(t) = \begin{cases} -1, & \text{if } N(0,t) = \emptyset \\ \sup\{j \in \mathbb{N}_0 | t_j \in N(0,t)\}, & \text{otherwise} \end{cases} \tag{3.4}$$

As mentioned, $j(t)$ represents the last successful control update for any $t \in \mathbb{R}_{\geq 0}$.
Note that definition (3.4) covers the scenario that the attack is applied continuously in $(0, t)$.

i.e. when $N(0,t) = \emptyset$, there are no communication period from 0 to t and therefore never triggering occurs. In these cases, we can define $j(t) = -1$ and the corresponding $u(t) = 0$ and $x(t_{-1}) = 0$.

3.1.3 Control Objectives

The goal is to find a controller and a sampling logic that ensure finite gain $\mathcal{L}_2$-stability of the closed loop control system in the presence of the DoS attack. This goal can be stated as follows

Definition 3.1 *The closed-loop system comprised as the system (3.1) with the control signal (3.3) is said to be finite gain $\mathcal{L}_2$-stable if there exists positive real constants γ and η such that*

$$\|x(t)\|_{\mathcal{L}_2} \leq \gamma \|w(t)\|_{\mathcal{L}_2} + \eta$$

for $t \in \mathbb{R}_{\geq 0}$ and $w \in \mathcal{L}_2$.

3.2 Control Policies

In this section, we define the control law, ignoring the cyber attack. Our interest is in a control law, implemented using an event-triggered approach, that attenuates the effect of disturbances, in $\mathcal{L}_2$-sense. The effect of the DoS attack will be discussed in the next section. Consider the dynamical system (3.1) along with the control signal (3.3) and define the following *triggering error*:

$$e(t) = x(t_{j(t)}) - x(t). \tag{3.5}$$

Thus, $e(t)$ represents the gap between the value of the state at the last successful update of the controller, and the actual state at the current time.

Theorem 3.1 *Consider the system (3.1) and the control input (3.3). Assume there is a positive definite function $V : \mathbb{R}^n \to \mathbb{R}$ that satisfies the following hamilton-jacobi inequality (HJI) for a real constant $\gamma > 0$,*

$$\frac{\partial V}{\partial x} A x + \frac{1}{2} \frac{\partial V}{\partial x} \frac{1}{\gamma^2} \frac{\partial V^T}{\partial x} - \frac{1}{2} \frac{\partial V}{\partial x} B B^T \frac{\partial V^T}{\partial x} + \frac{1}{2} x^T x \leq 0 \tag{3.6}$$

Let the control signal take the special form

$$u = k x(t_{j(t)}) = -B^T \frac{\partial V(x(t_{j(t)}))^T}{\partial x} \tag{3.7}$$

Defining the following event-triggered rule

$$\|e(t)\|^2 \leq \frac{(1-\zeta^2)}{\|k\|^2}\|x(t)\|^2 \tag{3.8}$$

with user defined parameter constant $\zeta \in \mathbb{R}$ *satisfying*

$$0 \leq \zeta \leq 1 \tag{3.9}$$

The control system is finite gain $\mathcal{L}_2$ *stable from external disturbance* w *to the output with* $\mathcal{L}_2$ *gain of equal or less than* γ/ζ.

Proof. The proof follows closely reference [93]. Taking the derivative of $V(x)$ along the system trajectories and substituting the control signal (3.7), we have

$$\dot{V} = \frac{\partial V}{\partial x}Ax(t) + \frac{\partial V}{\partial x}Bkx(t_{j(t)}) + \frac{\partial V}{\partial x}w(t)$$

Substituting $kx(t) = -B^T\frac{\partial V^T}{\partial x}$, we obtain

$$\dot{V} = \frac{\partial V}{\partial x}Ax(t) - x(t)^T k^T kx(t_{j(t)}) + \frac{\partial V}{\partial x}w(t).$$

Completing now squares for $\frac{\partial V}{\partial x}w(t)$, we get

$$\begin{aligned}\dot{V} = \frac{\partial V}{\partial x}Ax(t) - x(t)^T k^T kx(t_{j(t)}) + \frac{\gamma^2}{2}\|w(t)\|^2 \\ + \frac{1}{2\gamma^2}\|\frac{\partial V^T}{\partial x}\|^2 - \frac{1}{2}\|\gamma w(t) - \frac{1}{\gamma}\frac{\partial V^T}{\partial x}\|^2.\end{aligned}$$

Applying now the HJI (3.6),we obtain

$$\begin{aligned}\dot{V} \leq -x(t)^T k^T kx(t_{j(t)}) + \frac{\gamma^2}{2}\|w(t)\|^2 - \frac{1}{2}\|x(t)\|^2 \\ - \frac{1}{2}\|\gamma w(t) - \frac{1}{\gamma}\frac{\partial V^T}{\partial x}\|^2 + \frac{1}{2}\frac{\partial V}{\partial x}BB^T\frac{\partial V^T}{\partial x}.\end{aligned}$$

Substituting $kx(t) = -B^T\frac{\partial V^T}{\partial x}$,

$$\begin{aligned}\dot{V} \leq -x(t)^T k^T kx(t_{j(t)}) + \frac{\gamma^2}{2}\|w(t)\|^2 \\ - \frac{1}{2}\|x(t)\|^2 + \frac{1}{2}(kx(t))^T kx(t).\end{aligned}$$

We can now complete squares for $x(t)^T k^T kx(t_{j(t)})$, to obtain

$$\dot{V} \leq -\frac{1}{2}\|x(t)\|^2 + \frac{\gamma^2}{2}\|w(t)\|^2 + \frac{1}{2}\|k\|^2\|e(t)\|^2 - \frac{1}{2}\|kx(t) + ke(t)\|^2$$

Which implies that

$$\dot{V} \leq -\frac{1}{2}\|x(t)\|^2+\frac{\gamma^2}{2}\|w(t)\|^2+\frac{1}{2}\|k\|^2\|e(t)\|^2 \tag{3.10}$$

Introduce now a design parameter $0 \leq \zeta < 1$. We have:

$$\begin{aligned}\dot{V} \leq & -\frac{\zeta^2}{2}\|x(t)\|^2+\frac{\gamma^2}{2}\|w(t)\|^2 \\ & + (-\frac{1-\zeta^2}{2}\|x(t)\|^2+\frac{1}{2}\|k\|^2\|e(t)\|^2)\end{aligned}$$

Thus, defining the control update rule

$$\|e(t)\|^2 \leq \frac{(1-\zeta^2)}{\|k\|^2}\|x(t)\|^2$$

we conclude that

$$\dot{V} \leq -\frac{\zeta^2}{2}\|x(t)\|^2+\frac{\gamma^2}{2}\|w(t)\|^2.$$

Integrating both sides of the above inequality, we obtain

$$\zeta\|x(t)\|_{\mathcal{L}_2} \leq \gamma\|w(t)\|_{\mathcal{L}_2}+\sqrt{2V(x(0))}$$

which implies that the closed loop system is $\mathcal{L}_2$ stable with gain γ/ζ from the external disturbance w to the state x.

■

3.3 $\mathcal{L}_2$ Stability Under Denial-Of-Service

In this section, we consider the effect of DoS attacks. In the presence of an attack, the control update rule (3.8) may be violated since control updates may be interrupted thus affecting stability and performance. It is therefore important to understand the effect of the attack on system performance, according to the attack characteristics.
We begin our discussion by defining our assumptions on the DoS attacks. Then, based on these assumptions, we derive $\mathcal{L}_2$ stability conditions under DoS attacks.

3.3.1 Assumptions

(i) Given the dynamical system (3.1) with control input (3.3), there exist a posivive definite function P such that the Lyapunov function $V(x) = x^T Px$ satisfies the HJI (3.6).

Remark 3.1 *Note that since $V(x) = x^T Px$ is positive definite, then there exist $\alpha_1, \alpha_2 > 0$ such that $\alpha_1\|x(t)\|^2 \leq V(x) \leq \alpha_2\|x(t)\|^2$.*

(ii) We assume that the DoS attacks are limited in duration and frequency as follows:

DoS duration: For any given $t, \tau \in \mathbb{R} \geq 0$ that $t \geq \tau$, there exist $k_0 \geq 0$, $T > 0$ such that

$$|A(\tau, t)| \leq \frac{t - \tau}{T} + k_0 \tag{3.11}$$

The above assumption, adopted from [4], is based in the concept of *average dwell-time* in switching systems, introduced in [99]. The expression provides a criteria to express the length and overall distribution of the attack interval with respect to the time span.

DoS frequency: Let $n(\tau, t)$ indicate the number of attacks occurring on the interval $[\tau, t)$. There exist $N_0 \geq 0$ and $\tau_D \in \mathbb{R} \geq 0$ such that

$$n(\tau, t) \leq N_0 + \frac{t - \tau}{\tau_D} \tag{3.12}$$

for all $\tau, t \in \mathbb{R} \geq 0$ with $t \geq \tau$.

Remark 3.2 *In the concept of average dwell time, the assumptions of duration and frequency are defined to characterize the switching system. In this article we adapt similar assumptions in the characterization of DoS attack. The assumptions provides realistic bounds that will enable us to characterize stability and system performance, and are general enough to include a wide range of possible DoS attacks. In particular, assumption (3.11) provides an upper bound on the attack duration. Similarly, (3.12) defines the dispersion of the attack intervals over a time span.*

3.3.2 $\mathcal{L}_2$ Stability Under Denial of Service

In this section we study closed loop $\mathcal{L}_2$ stability in the presence of DoS attacks, under assumptions (3.11) and (3.12). Note that these assumptions do not depend on the system dynamics and/or information that might be available to the attacker. The closed-loop dynamics under attack can be considered as a switching system that may contain stable and unstable modes.

The set of integers indicating the time instants of control update attempts under DoS can be defined as follows

$$\psi = \{j \in \mathbb{N}_0 | t_j \in \bigcup_{n \in \mathbb{N}_0} H_n\}$$

We can now state our main result:

Theorem 3.2 *Consider the control system (3.1) along with the control input (3.2) and control update rule as (3.8). Let assumption (3.11) be satisfied, and assume that any DoS sequence satisfies assumption (3.12) with*

$$\frac{1}{T} + \frac{\Delta_*}{\tau_D} \leq \frac{w_1}{w_1 + w_2} \tag{3.13}$$

where $\Delta_* \geq 0$ *is a constant satisfying* $sup_{j\in\psi}\Delta_j \leq \Delta_*$ *and* $\Delta_j = t_{j+1} - t_j$*. In this expression,* $w_1 = \beta^2/\alpha_2$ *and* $w_2 = (\frac{\sqrt{1-\zeta^2}}{\|k\|}+2)^2/\alpha_1$ *and* θ *and* β *are design parameters satisfying* $\beta^2 + \theta^2 \leq \zeta^2$*. Then, under these conditions, the closed loop system is* $\mathcal{L}_2$ *stable with the gain of* $\frac{\gamma}{\theta}$*.*

Before proving the Theorem, we notice that the time axis can be separated into two types of intervals, namely; (i) intervals with no attack during which transmission of information is possible and thus, (3.8) holds, and (ii) intervals where the flow of information is prevented by a DoS attack. In these intervals, the systems is essentially in open loop and the control law (3.8) is not applied and therefore not valid.

Moreover, we should note that DoS attack cause actuation delay in the system. To explain, assume that sampling time t_j belongs to some DoS interval H_n, then the transmission would fail at t_j. Since transmission rate is finite, when the DoS interval is over, there would be a delay from when DoS interval finishes (i.e. $h_n + \tau_n$) and the next successful transmission attempt. Thus, it is necessary to consider this delay into characterization of the intervals in which event-triggering rule (3.8) holds and may not hold.

Consider the control update sequence $\{t_j\}$ and the DoS sequence $\{h_n\}$, let the set $S_n := \{j \in \mathbb{N}_0 | t_j \in H_n\}$ denote the integers corresponding to attempts for control updates occurring in the DoS interval. Define

$$\lambda_n := \begin{cases} \tau_n, & \text{if } S_n = \emptyset \\ t_{\sup\{j\in\mathbb{N}_0 : j\in S_n\}} - h_n, & \text{otherwise} \end{cases}$$

$$\Lambda_n := \begin{cases} 0, & \text{if } S_n = \emptyset \\ \Delta_{\sup\{j\in\mathbb{N}_0 : j\in S_n\}}, & \text{otherwise} \end{cases}$$

Therefore, the nth time interval in which (3.8) may not hold would be

$$\bar{H}_n = \{h_n\} \cup [h_n, h_n + \lambda_n + \Lambda_n[$$

which is the union of the DoS interval H_n and corresponding actuation delay. Note that next attack interval may occur in the DoS induced delay and thus h_{n+1} may belong to $\bar{H}_n$

and cause an overlap between intervals of $\bar{H}_n$ and $\bar{H}_{n+1}$. To address this concern for analysis purpose, it is more convenient to consider the overlapping intervals as a single interval [4]. By using an auxiliary sequence $\{z_m\}_{m\in\mathbb{N}_0}$ and defining it recursively from $\{h_n\}_{n\in\mathbb{N}_0}$ as follows

$$z_0 := h_0$$
$$z_{m+1} := \inf\{h_n > z_m | h_n > h_{n-1} + \lambda_{n-1} + \Lambda_{n-1}\}$$

for all $m \in \mathbb{N}_0$. Let v_m be the duration of mth attack interval in this new definition as

$$v_m := \sum_{\substack{n\in\mathbb{N}_0 \\ z_m \le h_n < z_{m+1}}} |\bar{H}_n \backslash \bar{H}_{n+1}|$$

for all $m \in \mathbb{N}_0$.

Now, for any $\tau, t \in \mathbb{R} \geq 0$ with $t \geq \tau$, the interval $[\tau, t]$ can be defined as union of complementary intervals of $|\bar{N}(\tau,t)|$ and $|\bar{A}(\tau,t)|$, where $|\bar{N}(\tau,t)|$ (respectively, $|\bar{A}(\tau,t)|$) is the total time in which (3.8) holds (respectively, is violated) as follows

$$\bar{A}(\tau,t) = \cup_{m\in\mathbb{N}_0} Z_m \cap [\tau,t] \tag{3.14}$$

$$\bar{N}(\tau,t) = \cup_{m\in\mathbb{N}_0} W_{m-1} \cap [\tau,t] \tag{3.15}$$

where

$$Z_m = \{z_m\} \cup [z_m, z_m + v_m[\tag{3.16}$$

$$W_m = \{z_m + v_m\} \cup [z_m + v_m, z_{m+1}[\tag{3.17}$$

As mentioned earlier, $\{z_m\}_{m\in\mathbb{N}_0}$ and $\{v_m\}_{m\in\mathbb{N}_0}$ are two sequences of non-negative real numbers where $z_{-1} = v_{-1} := 0$. As it can be seen, by construction, $\bar{A}(\tau,t)$ is union of sub-intervals if $[\tau,t]$ in which (3.8) may not hold. Note that since the union of sets $\bar{A}(\tau,t)$ and $\bar{N}(\tau,t)$ equals to $\bar{N}(\tau,t)$ and their intersection is empty, they are complementary. Also, the union of sub-intervals in which (3.8) satisfies is $\bar{N}(\tau,t)$. Specifically, by construction, for each $m \in \mathbb{N}_0$, the successful control update occurs exactly on at $z_m + v_m$ and there is no denial-of-service over W_m. The Equations (3.14),(3.3.2),(3.16) and (3.17) would be used in the proof of Theorem 3.2.

To proceed with the proof of Theorem 3.2 we also require the following lemma. Here, we denote $\mu_m = z_m + v_m$ for ease of use.

Lemma 3.1 *Let $t, \tau \in \mathbb{R} \geq 0$ with $t \geq \tau$, and assume that every DoS attack of duration $|A(\tau, t)|$ satisfies assumption (3.11) for some $k_0 \geq 0$, $T > 0$. Then we have that:*

$$e^{-w_1|\bar{N}(\mu_m,t)|}e^{w_2|\bar{A}(z_m,t)|} \leq e^{-\rho_*(t-z_m)}e^{(w_1+w_2)k_*}$$

where $\rho_* = w_1 - \frac{(w_1+w_2)}{T_*}$, $T_* = \tau_D T/(\tau_D + T\Delta_*)$ and $k_* = k_0 + (1 + N_0)\Delta_*$.

Proof. *As defined before, $|\bar{A}(\tau, t)|$ is the total time during which the control update rule (3.8) may not hold because of the presence of DoS attack. This time equals the total length of DoS interval over $[\tau, t]$ plus the delay caused by the DoS. The actuation delay can be upper bounded by considering it happen $n(\tau, t)$ times during the interval $[\tau, t]$ and once at the beginning of the interval. Thus, the upper bound of $|\bar{A}(\tau, t)|$ for any $\tau, t \in \mathbb{R} \geq 0$ is as follows:*

$$|\bar{A}(\tau, t)| \leq |A(\tau, t)| + (1 + n(\tau, t))\Delta_*$$

Then we have

$$\begin{aligned} |\bar{A}(\tau, t)| &\leq \frac{t-\tau}{T} + k_0 + (1 + N_0 + \frac{t-\tau}{\tau_D})\Delta_* \\ &\leq k_* + \frac{t-\tau}{T_*} \end{aligned}$$

where $k_* = k_0 + (1 + N_0)\Delta_*$ and $T_* = \tau_D T/(\tau_D + T\Delta_*)$.

Since $|\bar{N}(\mu_m, t)| = |\bar{N}(z_m, t)|$, we conclude that $|\bar{N}(\mu_m, t)| = t - z_m - |\bar{A}(z_m, t)|$. Then,

$$\begin{aligned} & e^{-w_1|\bar{N}(\mu_m,t)|}e^{w_2|\bar{A}(z_m,t)|} \\ &\qquad \leq e^{-w_1[(t-z_m)-(k_*+\frac{t-z_m}{T_*})]}e^{w_2(k_*+\frac{t-z_m}{T_*})} \\ &\qquad \leq e^{-(t-z_m)[w_1-\frac{(w_1+w_2)}{T_*}]}e^{(w_1+w_2)k_*} \\ &\qquad \leq e^{-\rho_*(t-z_m)}e^{(w_1+w_2)k_*}. \end{aligned}$$

This completes the proof of Lemma 3.1.

■

Proof of Theorem 3.2. We can now proceed with the proof of Theorem 3.2. In the presence of an attack, communication is prevented and the event triggering rule is not applied to the system, except at the very beginning of the attack, where the triggering rule still holds. Thus,

$$\|e(z_m)\|^2 \leq \frac{(1-\zeta^2)}{\|k\|^2}\|x(z_m)\|^2.$$

To find an upper bound for e(t) in the presence of an attack we proceed as follows:

$$\begin{aligned}\|e(t)\|^2 &= \|x(t_{k(z_m)}) - x(t) + x(z_m) - x(z_m)\|^2 \\ &= \|e(z_m) - x(t) + x(z_m)\|^2 \\ &\leq \|e(z_m)\|^2 + \|x(z_m)\|^2 + \|x(t)\|^2 \\ &+ 2\|e(z_m)\|\|x(t)\| + 2\|e(z_m)\|\|x(z_m)\| \\ &+ 2\|x(t)\|\|x(z_m)\|\end{aligned}$$

Thus, during attacks, the following upper bound on the error is satisfied:

$$\begin{aligned}\|e(t)\|^2 \leq (&\frac{(1-\zeta^2)}{\|k\|^2} + 2\frac{\sqrt{(1-\zeta^2)}}{\|k\|} + 1)\|x(z_m)\|^2 + \|x(t)\|^2 \\ &+ (2 + 2\frac{\sqrt{(1-\zeta^2)}}{\|k\|} + 1))\|x(z_m)\|\|x(t)\|\end{aligned}$$

Substituting the above upper bound in the Lyapunov inequality (3.10) and defining $\xi = \frac{(1-\zeta^2)}{\|k\|^2}$, one obtain

$$\begin{aligned}\dot{V} \leq &- \|x\|^2 + \gamma^2\|w\|^2 + (\xi + 2\sqrt{\xi} + 1)\|x(z_m)\|^2 \\ &+ \|x(t)\|^2 + (2 + 2\sqrt{\xi})\|x(z_m)\|\|x(t)\|.\end{aligned}$$

It follows that

$$\begin{aligned}\dot{V} \leq &- \|x(t)\|^2 + \gamma^2\|w(t)\|^2 \\ &+ (\sqrt{\xi} + 2)^2 \max\{\|x(z_m)\|^2, \|x(t)\|^2\}.\end{aligned} \tag{3.18}$$

The Lyapunov function $V(x) = x^T P x$ is positive definite, and thus satisfies:

$$\alpha_1\|x(t)\|^2 \leq V(x) \leq \alpha_2\|x(t)\|^2 \tag{3.19}$$

Substituting (3.19) in (3.18), we get

$$\begin{aligned}\dot{V} \leq &-\|x(t)\|^2 + \gamma^2\|w(t)\|^2 \\ &+ \frac{1}{\alpha_1}(\sqrt{\xi} + 2)^2 \max\{V(x(z_m)), V(x(t))\}.\end{aligned}$$

Thus, we concluded that

$$\dot{V} \leq -\|x(t)\|^2 + \gamma^2\|w(t)\|^2 + \frac{1}{\alpha_1}(\sqrt{\xi} + 2)^2 V(x(t))$$

Let now $w_2 = \frac{1}{\alpha_1}(\sqrt{\xi} + 2)^2$, $a_2 = \gamma^2$ and $a_3 = 1$. Then, we have

$$e^{-w_2 t}(\dot{V} - w_2 V) \leq -e^{-w_2 t}\|x(t)\|^2 + \gamma^2 e^{-w_2 t}\|w(t)\|^2$$

Thus,

$$\frac{d}{dt}(e^{-w_2 t}V) \leq -e^{-w_2 t}\|x(t)\|^2 + \gamma^2 e^{-w_2 t}\|w(t)\|^2.$$

Integrating both sides of the above inequality and multiplying by $e^{w_2 t}$, we obtain

$$\begin{aligned} V(x(t)) \leq & e^{w_2(t-z_m)} V(x(z_m)) + a_2 \int_{z_m}^{t} e^{w_2(t-\tau)} \|w(\tau)\|^2 d\tau \\ & - a_3 \int_{z_m}^{t} e^{w_2(t-\tau)} \|x(\tau)\|^2 d\tau \end{aligned} \tag{3.20}$$

The above Lyapunov inequality is satisfied for the system in the presence of an attack. When there is no attack occurring in the system, communication network is not interrupted. Hence, as mentioned earlier in section III, the Lyapunov inequality is as follows:

$$\dot{V} \leq -\zeta^2 \|x\|^2 + \gamma^2 \|w\|^2$$

Taking account of the inequality $\beta^2 + \theta^2 \leq \zeta^2$ and replacing in the above equation, we have:

$$\dot{V} \leq -\frac{\beta^2}{\alpha_2} V(x(t)) + \gamma^2 \|w\|^2 - \theta^2 \|x\|^2$$

Let $w_1 = \beta^2/\alpha_2$, $b_2 = \gamma^2$ and $b_3 = \theta^2$. Following the same procedure used to obtain the Lyapunov inequality during the attack interval (3.20), in the absence of an attack we obtain the following inequality:

$$\begin{aligned} V(x(t)) \leq & e^{-w_1(t-\mu_m)} V(x(\mu_m)) \\ & + b_2 \int_{\mu_m}^{t} e^{-w_1(t-\tau)} \|w(\tau)\|^2 d\tau \\ & - b_3 \int_{\mu_m}^{t} e^{-w_1(t-\tau)} \|x(\tau)\|^2 d\tau \end{aligned} \tag{3.21}$$

Substituting $V(x(\mu_m))$ in (3.21) using the upper bound obtained from (3.20), we obtain

$$\begin{aligned} V(x(t)) \leq & \, e^{-w_1(t-\mu_m)} e^{w_2 v_m} V(x(z_m)) \\ & + e^{-w_1(t-\mu_m)} a_2 \int_{z_m}^{\mu_m} e^{w_2(\mu_m-\tau)} \|w(\tau)\|^2 d\tau \\ & - e^{-w_1(t-\mu_m)} a_3 \int_{z_m}^{\mu_m} e^{w_2(\mu_m-\tau)} \|x(\tau)\|^2 d\tau \\ & + b_2 \int_{\mu_m}^{t} e^{-w_1(t-\tau)} \|w(\tau)\|^2 d\tau \\ & - b_3 \int_{\mu_m}^{t} e^{-w_1(t-\tau)} \|x(\tau)\|^2 d\tau. \end{aligned}$$

By continuing this procedure, i.e. substitution of initial values of the Lyapunov function in

the inequality with their upper bounds from their previous interval, we obtain

$$
\begin{aligned}
V(x(t)) \leq\ & e^{-w_1(t-\mu_m)}e^{w_2 v_m} \\
& \times e^{-w_1(z_m-\mu_{m-1})}e^{w_2 v_{m-1}}V(x(z_{m-1})) \\
& + e^{-w_1(t-\mu_m)}e^{w_2 v_m}e^{-w_1(z_m-\mu_{m-1})} \\
& \times a_2\int_{z_{m-1}}^{\mu_{m-1}} e^{w_2(\mu_{m-1}-\tau)}\|w(\tau)\|^2 d\tau \\
& - e^{-w_1(t-\mu_m)}e^{w_2 v_m}e^{-w_1(z_m-\mu_{m-1})} \\
& \times a_3\int_{z_{m-1}}^{\mu_{m-1}} e^{w_2(\mu_{m-1}-\tau)}\|x(\tau)\|^2 d\tau \\
& + e^{-w_1(t-\mu_m)}e^{w_2 v_m} b_2\int_{\mu_{m-1}}^{z_m} e^{-w_1(z_m-\tau)}\|w(\tau)\|^2 d\tau \\
& - e^{-w_1(t-\mu_m)}e^{w_2 v_m} b_3\int_{\mu_{m-1}}^{z_m} e^{-w_1(z_m-\tau)}\|x(\tau)\|^2 d\tau \\
& + e^{-w_1(t-\mu_m)} a_2\int_{z_m}^{\mu_m} e^{w_2(\mu_m-\tau)}\|w(\tau)\|^2 d\tau \\
& - e^{-w_1(t-\mu_m)} a_3\int_{z_m}^{\mu_m} e^{w_2(\mu_m-\tau)}\|x(\tau)\|^2 d\tau \\
& + b_2\int_{\mu_m}^{t} e^{-w_1(t-\tau)}\|w(\tau)\|^2 d\tau \\
& - b_3\int_{\mu_m}^{t} e^{-w_1(t-\tau)}\|x(\tau)\|^2 d\tau.
\end{aligned}
$$

Denoting $\gamma_1 = \max\{a_2, b_2\}$, $\gamma_2 = \min\{a_3, b_3\}$ and $\Gamma(\tau) \triangleq \gamma_1\|w(\tau)\|^2 - \gamma_2\|x(\tau)\|^2$, we obtain

$$
\begin{aligned}
V(x(t)) \leq\ & e^{-w_1(t-\mu_m)}e^{w_2 v_m} \\
& \times e^{-w_1(z_m-\mu_{m-1})}e^{w_2 v_{m-1}}V(x(z_{m-1})) \\
& + \int_{z_{m-1}}^{\mu_{m-1}} e^{-w_1(t-\mu_m)}e^{w_2 v_m}e^{-w_1(z_m-\mu_{m-1})} \\
& \times e^{w_2(\mu_{m-1}-\tau)}\Gamma(\tau) d\tau \\
& + \int_{\mu_{m-1}}^{z_m} e^{-w_1(t-\mu_m)}e^{w_2 v_m}e^{-w_1(z_m-\tau)}\Gamma(\tau) d\tau \\
& + \int_{z_m}^{\mu_m} e^{-w_1(t-\mu_m)}e^{w_2(\mu_m-\tau)}\Gamma(\tau) d\tau \\
& + \int_{\mu_m}^{t} e^{-w_1(t-\tau)}\Gamma(\tau) d\tau
\end{aligned}
$$

Continuing the above substituting for all the intervals from 0 to t and using Lemma 2, the

overall Lyapunov inequality is given by:

$$\begin{aligned} V(x(t)) \leq e^{-w_1|\bar{N}(0,t)|}e^{w_2|\bar{A}(0,t)|}V(x(0))+\int_{\mu_m}^{t} e^{-w_1(t-\tau)}\Gamma(\tau)d\tau \\ + \sum_{\substack{m\in\mathbb{N}\\ \mu_m<t}} \int_{z_m}^{\mu_m} e^{-w_1|\bar{N}(\mu_m,t)|}e^{w_2|\bar{A}(\tau,t)|}\Gamma(\tau)d\tau \\ + \sum_{\substack{m\in\mathbb{N}\\ z_m<t}} \int_{\mu_{m-1}}^{z_m} e^{-w_1|\bar{N}(\tau,t)|}e^{w_2|\bar{A}(\mu_{m-1},t)|}\Gamma(\tau)d\tau. \end{aligned} \tag{3.22}$$

Taking account of Lemma 2, we obtain

$$\begin{aligned} V(x(t)) \leq e^{-w_1|\bar{N}(0,t)|}e^{w_2|\bar{A}(0,t)|}V(x(0)) \\ + \int_0^t e^{-\rho_*(t-\tau)}e^{(w_1+w_2)k_*}\Gamma(\tau)d\tau \end{aligned} \tag{3.23}$$

Since $V(x(t)) \geq 0$, from the Lyapunov inequality (3.23) and the definition $\Gamma(\tau) \triangleq \gamma_1\|w(\tau)\|^2 - \gamma_2\|x(\tau)\|^2$, we can get:

$$\begin{aligned} \gamma_2 \int_0^t e^{-\rho_*(t-\tau)}e^{(w_1+w_2)k_*}\|x(\tau)\|^2 d\tau \leq \\ + e^{-w_1|\bar{N}(0,t)|}e^{w_2|\bar{A}(0,t)|}V(x(0)) \\ + \gamma_1\int_0^t e^{-\rho_*(t-\tau)}e^{(w_1+w_2)k_*}\|w(\tau)\|^2 d\tau \end{aligned}$$

By integrating both sides from $t = 0$ to $t = \infty$ and rearraging the double integral area we can obtain:

$$\begin{aligned} \gamma_2\frac{1}{\rho_*}\int_0^\infty e^{(w_1+w_2)k_*}\|x(\tau)\|^2 d\tau \leq \\ \int_0^\infty e^{-\rho_* t}e^{(w_1+w_2)k_*}V(x(0))dt + \gamma_1\frac{1}{\rho_*}\int_0^\infty e^{(w_1+w_2)k_*}\|w(\tau)\|^2 d\tau \end{aligned}$$

Thus one can get

$$\gamma_2 \int_0^\infty \|x(\tau)\|^2 d\tau \leq V(x(0)) + \gamma_1 \int_0^\infty \|w(\tau)\|^2 d\tau$$

which results

$$\|x(t)\|_{\mathcal{L}_2} \leq \sqrt{\frac{V(x(0))}{\gamma_2}} + \sqrt{\frac{\gamma_1}{\gamma_2}}\|w(t)\|_{\mathcal{L}_2}$$

Since, by assumption, $\gamma_1 = \max\{a_2, b_2\}$ and $\gamma_2 = \min\{a_3, b_3\}$. Therefore, $\gamma_1 = \gamma^2$ and $\gamma_2 = \{1, \theta^2\}$. Also $\theta^2 \leq 1$, and thus $\gamma_2 = \theta^2$. Consequently,

$$\sqrt{\frac{\gamma_1}{\gamma_2}} = \frac{\gamma}{\theta}.$$

This completes the proof. ■

Remark 3.3 *In the absence of an attack, the $\mathcal{L}_2$ gain of the system is γ/ζ, as expected from Theorem 1. It is relatively straightforward to recover this result from Theorem 2. In this case $\theta = \zeta$, and the gain becomes γ/ζ.*

3.3.3 Discussion

In this proposed framework, there is a trade off between the length of tolerable attack and the quantitative system performance in $\mathcal{L}_2$ sense. A larger β indicates a larger amount of tolerable attack duration as it corresponds to larger $w_1/(w_1 + w_2)$. On the other hand, a larger β means smaller θ and therefore a larger $\mathcal{L}_2$ gain.
The theorem explicitly shows the trade off between the $\mathcal{L}_2$ gain and the event update rule. Having more frequent update results in higher performance and smaller $\mathcal{L}_2$ gain.
In the next section, we provide a numerical example to better illustrate the analysis.

3.4 Illustrative Examples

In this section, the theory and discussion are illustrated using a numerical example. Consider the following system, and notice that it has an unstable equilibrium point at the origin.

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -2 & 3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u + w \tag{3.24}$$

Using the Lyapunov function $V = x^T P x$, for an $\mathcal{L}_2$ gain of $\gamma = 4$, the stabilizing $\mathcal{L}_2$ feedback controller is $u = -2B_1^T P^T x$, where P is the solution to the HJI (3.6),

$$P = \begin{bmatrix} 27.28 & 6.812 \\ 6.812 & 9.315 \end{bmatrix}$$

Thus, we obtain $\alpha_1 = 7.02$ and $\alpha_2 = 29.57$. Taking $\beta = 0.68$ and $\theta = 0.68$, the allowed duty cycle of the DoS attack is $w_1/(w_1 + w_2) = 0.0501$, which implies a tolerable duty cycle of 5%. Figure 3.2, shows the trajectories of the system under the control feedback (3.3) and above characteristics. Triggering times determined by the event rule (3.8) are shown in Figure 3.3. The disturbance w is a uniform distribution between 0 and 1. DoS attacks are generated randomly. In this example, the generated DoS attack has a duty cycle of 20%. Although the value obtained for the amount of tolerable DoS attack is conservative due to the assumptions used in the stability analysis, it provides an explicit relationship between the system performance, event rule and convergence rate of the closed-loop system.

Table 3.1 shows the trade-off between the $\mathcal{L}_2$ gain of the closed-loop system and the duty cycle of the DoS attack for different values of β and θ for $\zeta^2 = 0.9409$. It is shown that for a predefined γ and the control rule (3.3), the closed-loop system is resilient to attacks

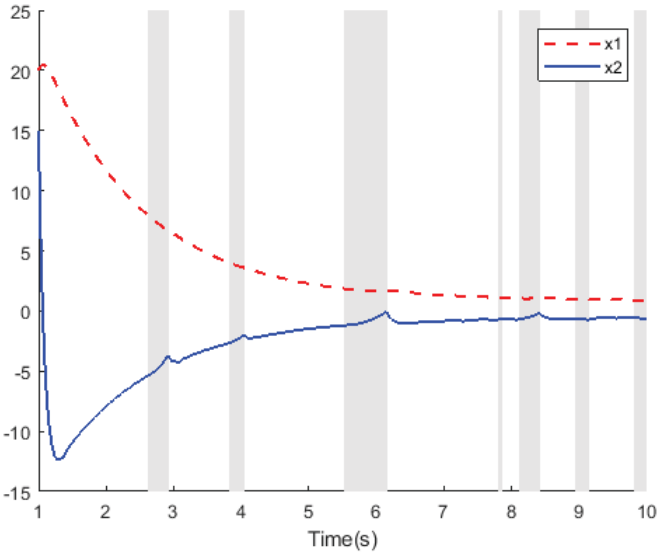

Figure 3.2: Trajectories of closed loop system under $\mathcal{L}_2$ control.

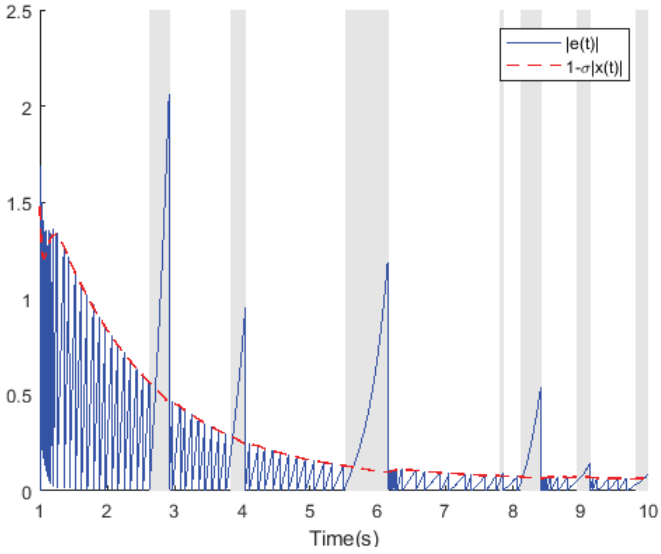

Figure 3.3: The error and the event rule margin trajectories.

with larger duty-cycle up to a threshold, while sacrificing performance.
The amount of duty-cycle of the attack converges to a maximum of nearly 5% for a large $\mathcal{L}_2$ gain.

The gain and the maximum amount of tolerable attack depends on various design parameters such as control rule parameters, γ, α_1, α_2 and ζ. In Figure 3.4, the trade-off between tolerable amount of the attack and $\mathcal{L}_2$ gain of the system is explicitly shown for various values of ζ. It is worth mentioning while as much as it is needed to sacrifice the gain to bring the system to the desired amount of attack tolerance, near 90% of the desired

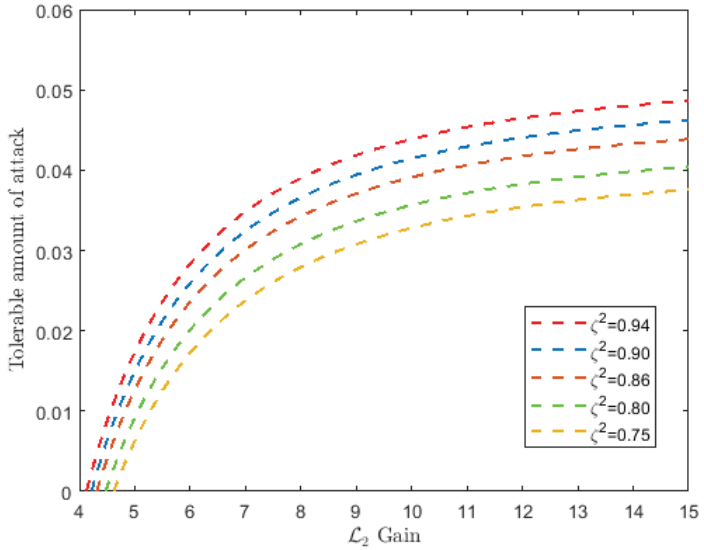

Figure 3.4: Trade-off between tolerable amount of attack $\frac{\omega_1}{\omega_1+\omega_2}$ and $\mathcal{L}_2$ gain of the system for various values of ζ.

tolerance can be obtained without significant deterioration of the gain. Moreover, smaller ζ corresponds to fewer update of the control rule and as a result less transmission of data in the network. Thus, Figure 3.4 gives a good insight of the relative trade-off between these parameters which enables the designer to suitably tune the design parameters with respect to the design goals.

Table 3.1: Trade-off between the $\mathcal{L}_2$ gain and the duty cycle of the attack for $\zeta^2 = 0.94$

$\begin{bmatrix}\boldsymbol{\theta}\\ \boldsymbol{\beta}\end{bmatrix}$	$\begin{bmatrix}0.84\\ 0.48\end{bmatrix}$	$\begin{bmatrix}0.68\\ 0.68\end{bmatrix}$	$\begin{bmatrix}0.56\\ 0.79\end{bmatrix}$	$\begin{bmatrix}0.39\\ 0.88\end{bmatrix}$	$\begin{bmatrix}0.32\\ 0.91\end{bmatrix}$
DoS	1.4%	2.7%	3.5%	4.4%	4.6%
$\boldsymbol{L_2}$ **gain**	4.7	5.8	7.1	10	12.3

3.5 Summary

In this chapter, we investigated $\mathcal{L}_2$ stability of networked systems under DoS attack. We derive an explicit finite $\mathcal{L}_2$ gain to characterize system performance in the presence of disturbance and certain class of DoS attack. Also, tolerable amount of DoS attack with respect to the control law is derived to ensure the closed-loop $\mathcal{L}_2$ stability is preserved. By having

the explicit relation between control and event rule parameters and attack characteristics, a better perspective into designing an event-triggered robust controller is provided. Hence, the $\mathcal{L}_2$ controller is designed to obtain a resilient control system despite of the presence of disturbance and DoS attack. In this regards, several interesting research venues such as deriving an optimal control strategy with respect to a certain class of DoS attack can be followed. Also, the result can be extended to nonlinear networked systems as a future research topic.

Chapter 4

Summary and Conclusions

Traditionally speaking, control systems are usually designed with this assumption that the sensors measurements can be used for controlling the plant operation. By introduction of Networked Control Systems (NCSs) in which the classical hard wiring are replaced with more flexible networked interconnections between subsystems, unnecessary wiring and overall complexity of control systems are reduced. Although the widespread use of computers have brought many privileges into networked control systems, it also introduced an important threat: *cyber attacks*. Various types of cyber attacks have been known and investigated so far. One of the most common and easy to apply attacks in networked control systems is denial-of-service (DoS). Due to the fact that the attacker does not require to know the systems dynamics for performing the attack, DoS becomes one of the primary options between different types of attacks. Therefore, guaranteeing stability and some level of performance in the presence of DoS attack in networked control systems is a must.

In chapter 2, denial-of-service attack is put on perspective based on different types of its origin and methods of modeling. There are different DoS modeling approaches in the attempt to make it compatible with various frameworks and control approaches in networked control systems. Moreover, an overview of methods for guaranteeing and analyzing of stability of networked control systems under DoS attack is provided. Consistent with the recent trend, our focus is on event-triggered implementation of control systems which leads to a significant reduction in data transmission in communication channels.

In chapter 3, input-output stability and performance of the control system under DoS attack is analyzed. While the literature is mainly focused with retaining stability, in this chapter we are also concerned with keeping the performance of the system in a reasonable level. For this purpose, $\mathcal{L}_2$ stability of the system is investigated. In this stability analysis, no constraint was assumed on magnitude of the exogenous disturbance. The model con-

sidered in this thesis for DoS attack is very general and no knowledge is assumed available about the time instants of the attack occurrence and length of each attack interval. We show that under some assumptions on DoS attacks, input-output stability of the system is guaranteed in the expense of deterioration of the $\mathcal{L}_2$ gain. Moreover, explicit relation between $\mathcal{L}_2$ gain of the system and tolerable amount of DoS attack is provided. The scheme is resilient enough to enable the control designer to consider a suitable trade-off point between security of the system (i.e. the amount of tolerable attack) and the performance of the system under attack. At last, the results are illustrated by a numerical example.

4.1 Directions for Future Work

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

- As a further path in this research, stability of the system in model-based periodic event-triggered control scheme can be investigated. It has been shown that using this mechanism significantly decrease the amount of transmissions in NCSs compared to both standard periodic time-triggered controller or periodic event-triggered controller [100]. Using predictors both in controller to actuator (C-S) and in sensor to controller (S-C) channel, enables the ETC system to outperform the conventional ETC systems. Using this scheme, it would be beneficial to investigate the stability and $\mathcal{L}_2$ gain of the control system under denial-of-service attack using this scheme.

- In the next step, previous results and ideas can be extended to decentralized systems. Decentralized systems are suitable for large-scale system in which physical components such as controllers, actuators and sensors are distributed over a wide area. Centralized ETMs and controllers can be very costly due to the fact that event-triggered rules and controllers need access to all plant or controller output in every sampling time. Moreover, by considering a large-scale plant consisting of number of sub-systems instead of a complete plant model, the computational load on ETMs would be reduced. Therefore, extending the previous ideas to decentralized systems would be of a practical importance in stability analyses of control systems under DoS attack.

Bibliography

[1] H. S. A.Teixeira, K. Sou and K. Johansson, "Secure control systems: A quantitative risk management approach," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 24–45, 2015.

[2] P. T. E. Nozari and J. Cortes, "Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design," *Automatica*, vol. 81, p. 221–231, 2017.

[3] F. D. F. Pasqualetti and F. Bullo, "Control-theoretic methods for cyber-physical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 110–127, 2015.

[4] C. D. Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 2930–2944, 2015.

[5] S. A. A. A. Cardenas and S. Sastry, "Research challenges for the security of control systems," *in Proceedings The 3rd USENIX Workshop on Hot Topics in Security (HotSec)*, 2008.

[6] ——, "Secure control: Towards survivable cyber-physical systems," *in Proceedings of 28th International Conference on Distributed Computing Systems Workshops*, p. 495–500, 2008.

[7] A. Cardenas, S. Amin, and S. Sastry.

[8] K. H. J. H. Sandberg and S. A. (guest eds), "Special issue on cyber-physical security in networked control systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, 2015.

[9] S. Dibaji, M. Pirani, D. Flamholz, A. Annaswamy, K. Johansson, and A. Chakrabortty, "A systems and control perspective of cps security," *Annual Reviews in Control*, 2019.

[10] P. C. V. O. J. Katz, A. J. Menezes and S. A. Vanstone, *Handbook of Applied Cryptography.* CRC Press, 1996.

[11] M. Milanese, *Robustness in Identification and Control.* Springer, 2013.

[12] C. R. P. Frasca, H. Ishii and R. Tempo, "Distributed randomized algorithms for opinion formation, centrality computation and power systems estimation: A tutorial overview," *European Journal of Control*, vol. 24, pp. 2–13, 2015.

[13] Y. Mo and R. M. Murray, "Privacy preserving average consensus, ieee transactions on automatic control," *IEEE Transactions on Automatic Control*, vol. 62, no. 2, p. 753–765, 2017.

[14] A. M. A. K. H. J. S. M. Dibaji, M. Pirani and A. Chakrabortty, "Secure control of power systems: Confidentiality and integrity threats," *in Proceedings of IEEE Conference on Decision and Control*, p. 7269–7274, 2018.

[15] D. I. G. C. G. Rieger and M. A. McQueen, "Resilient control systems: Next generation design research," *in Proceedings of 2nd Conference on Human System Interactions*, p. 632–636, 2009.

[16] L. B. Q. Zhu and T. Basar, "Resilient distributed control of multi-agent cyber-physical systems," *in Control of Cyber-Physical Systems*, p. 301–316, 2013.

[17] W. S. A. Sanjab and T. Bas¸a, "Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game," *IEEE International Conference on Communications (ICC)*, pp. 1–6, 2017.

[18] R. P. A. Clark, Q. Zhu and T. Basar, "An impact aware defense against stuxnet," *in Proceedings of American Control Conference*, p. 4140–4147, 2013.

[19] H. T. Q. Zhu and T. Basar, "Network security configurations: A nonzero-sum stochastic game approach," in proceedings of american control conference," *in Proceedings of American Control Conference*, p. 1059–1064, 2010.

[20] A. Sanjab and S. Walid, "On bounded rationality in cyber-physical systems security: Game-theoretic analysis with application to smart grid protection," *In 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG)*, pp. 1–6, 2016.

[21] M. P. F. Miao, Q. Zhu and G. J. Pappas, "A hybrid stochastic game for secure control of cyber-physical systems," *Automatica*, vol. 93, pp. 55–63, 2018.

[22] V. Ugrinovskii and C. Langbort, "Controller–jammer game models of denial of service in control systems operating over packet-dropping links," *Automatica*, vol. 84, p. 128–141, 2017.

[23] Y. L. Y.Wu and L. Shi, "A game-theoretic approach to remote state estimation in presence of a dos attacker," *in Proceedings of IFAC World Congress*, p. 2595–2600, 2017.

[24] M. Felegyhazi and J.-P. Hubaux, "Game theory in wireless networks: A tutorial," *Tech. Rep.*, 2006.

[25] C. L. A. Gupta and T. Basar, "Optimal control in the presence of an intelligent jammer with limited actions," *in Proceedings of IEEE Conference on Decision and Control*, p. 1096–1101, 2010.

[26] T. A. T. B. M. Manshaei, Q. Zhu and J. P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys*, vol. 45, pp. 53–73, 2013.

[27] K. G. Vamvoudakis and J. P. Hespanha, "Cooperative qlearning for rejection of persistent adversarial inputs in unknown networked systems," *IEEE Transactions on Automatic Control*, vol. 63, no. 4, p. 1018 – 1031, 2018.

[28] H. B. P. N. Brown and J. R. Mardenr, "Security against impersonation attacks in distributed systems," *IEEE Transactions on Control of Network Systems*, 2018.

[29] X. K. H. J. LeBlanc, H. Zhang and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, p. 766–781, 2013.

[30] E. F. H. Zhang and S. Sundaram, "A notion of robustness in complex networks," *IEEE Transactions on Control of Network Systems*, vol. 2, no. 3, p. 310–320, 2015.

[31] H. J. LeBlanc and X. Koutsoukos, "Resilient first-order consensus and weakly stable, higher order synchronization of continuous-time networked multiagent systems." *IEEE Transactions on Control of Network Systems*, vol. 5, no. 3, p. 1219–1231, 2018.

[32] E. F. H. Zhang and S. Sundaram, "Distributed observers for lti systems," *IEEE Transactions on Automatic Control*, vol. 63, no. 11, p. 3689–3704, 2018.

[33] ——, "A notion of robustness in complex networks," *IEEE Transactions on Control of Network Systems*, vol. 2, no. 3, p. 310–320, 2015.

[34] H. J. LeBlanc and X. Koutsoukos, "Resilient first-order consensus and weakly stable, higher order synchronization of continuous-time networked multi-agent systems," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 3, p. 1219–1231, 2018.

[35] S. Sundaram and B. Gharesifard, "Secure local filtering algorithms for distributed optimization," *in Proceedings of IEEE Conference on Decision and Control*, p. 1871–1876, 2016.

[36] S. Sundaram and C. N. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Transactions on Automatic Control*, vol. 56, no. 7, p. 1495–1508, 2011.

[37] K. H. J. W. Heemels and P. Tabuada, "An introduction to event-triggered and self-triggered control," *in Proceedings of IEEE Conference on Decision and Control*, p. 3270–3285, 2012.

[38] C. D. Persis and P. Tesi, "On resilient control on nonlinear systems under denial-of-service," *In Proceeding of 53rd IEEE Conference on Decision and Control*, p. 5254–5259, December 2014.

[39] C. D. Persis and P. Tesi., "Resilient control under denial-of-service," *In Proceeding of 19th IFAC World Congress*, p. 134–139, 2014.

[40] H. I. A. Cetinkaya and T. Hayakawa, "Networked control under random and malicious packet losses," ieee transactions on automatic control, vol. 62, no. 5, pp. 2434–2449, 2017." *in Proceedings of IEEE Conference on Decision and Control*, vol. 62, no. 5, p. 2434–2449, 2017.

[41] H. Sun, C. Peng, W. Zhang, T. Yang, and Z. Wang, "Security based resilient event-triggered control of networked control systems under denial of service," *Journal of the Franklin Institute*, 2018.

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

[43] H. S. Foroush and S. Martinez., "On event-triggered control of linear systems under periodic denial-of-service jamming attacks," *IEEE 51st Annual Conference on Decision and Control*, 2012.

[44] C. D. P. V. Dolk, P. Tesi and W. Heemels, "Event-triggered control systems under denial-of-service attacks," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 93–105, 2017.

[45] V. Dolk, P. Tesi, C. D. Persis, and W. Heemels, "Event-triggered control systems under denial-of-service attacks," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 93–105, 2016.

[46] H. S. A. Teixeira, I. Shames and K. H. Johansson, "Revealing stealthy attacks in control systems," *in Proceedings of 50th Annu. Allert. Conf. Commun. Control. Comput. Allert*, p. 1806–1813, 2012.

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

[48] A. B. F. Pasqualetti and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Transactions on Automatic Control*, vol. 57, no. 1, p. 90–104, 2012.

[49] S. K. Y. Chen and J. M. F. Moura, "Dynamic attack detection in cyber-physical systems with side initial state information," *IEEE Transactions on Automatic Control*, vol. 62, no. 9, p. 4618–4624, 2017.

[50] H. S. K. H. J. A. Teixeira, S. Amin and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," *in Proceedings of IEEE Conference on Decision and Control*, p. 5991–5998, 2010.

[51] Y. Chakhchoukh and H. Ishii, "Coordinated cyber-attacks on the measurement function in hybrid state estimation," *IEEE Transactions on Power Systems*, vol. 30, no. 5, p. 2487–2497, 2015.

[52] G. T. H. Y. Chakhchoukh, V. Vittal and H. Ishii, "Lts-based robust hybrid se integrating correlation," *IEEE Transactions on Power Systems*, vol. 32, no. 4, p. 3127–3135, 2017.

[53] P. N. Y. Liu and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, 2011.

[54] S. W. Y. Mo and B. Sinopoli, "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Systems Magazine*, vol. 35, no. 1, p. 93–109, 2015.

[55] R. C. Y. Mo and B. Sinopoli, "Detecting integrity attacks on scada systems," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 4, p. 1396–1407, 2014.

[56] H. K. A. Khazraei and F. R. Salmasi, "Replay attack detection in a multi agent system using stability analysis and loss effective watermarking," *in Proceedings of American Control Conference*, p. 4778–4783, 2017.

[57] R. M. G. Ferrari and A. M. H. Teixeira, "Detection and isolation of replay attacks through sensor watermarking," *in Proceedings of IFAC Workshop on Distributed Estimation and Control in Networked Systems*, p. 7363–7368, 2017.

[58] R. M. Ferrari and A. M. Teixeira, "Detection and isolation of routing attacks through sensor watermarking," *in Proceedings of American Control Conference*, p. 5436–5442, 2017.

[59] J. H. C. W. Ten and C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, p. 865–873, 2011.

[60] G. J. M. Y. He and J. Wei, "Real-time detection of false data injection attacks in smart grids: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, p. 1–12, 2016.

[61] E. K. Reddy, "Neural networks for intrusion detection and its applications," *in Proceedings of the World Congress on Engineering*, vol. 2, no. 5, pp. 3–5, 2013.

[62] Y. S. H. B. Kailkhura and P. K. Varshney, "Distributed bayesian detection in the presence of byzantine data," *IEEE transactions on signal processing*, vol. 63, no. 19, pp. 5250–5263, 2015.

[63] M. Liao and A. Chakrabortty, "Optimization algorithms for catching data manipulators in power system estimation loops," *IEEE Transactions on Control Systems Technology*, no. 99, pp. 1–16, 2018.

[64] T. R. S. Nudell, Nabavi, and A. Chakrabortty, "A real-time attack localization algorithm for large power system networks using graph-theoretic techniques," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, p. 2551–2559, 2015.

[65] D. E. Q. S. D. K. Ding, Y. Li and L. Shi, "A multichannel transmission schedule for remote state estimation under dos attacks," *Automatica*, vol. 78, p. 194–201, 2017.

[66] N. K. S. N. D. S. Mishra, Y. Shoukry and P. Tabuada, "Secure state estimation against sensor attacks in the presence of noise," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 49–59, 2017.

[67] O. A. L.K. Mestha and M. Abbaszadeh, "Cyber-attack detection and accommodation algorithm for energy delivery systems," *In 2017 IEEE Conference on Control Technology and Applications (CCTA)*, pp. 1326–1331, 2017.

[68] A. Cardenas, S. Amin, and S. Sastry, "Secure control: towards survivable cyber-physical systems," *in Proceedings of The 28th International Conference on Distributed Computing Systems Workshops*, pp. 495 – 500, 2008.

[69] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proceedings of IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[70] L. O. M. N. Falliere and E. Chien, "W32. stuxnet dossier: Symantec security response," *https://www.symantec. com, Symantec, Tech. Rep.*

[71] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," *in Proceedings of International Conference on Critical Infrastructure Protection*, p. 73–82, 2007.

[72] P. T. H. Fawzi and S. Diggavi, "Secure state-estimation for dynamical systems under active adversaries," *Annual Allerton Conference on Communication, Control, and Computing*, 2011.

[73] W. T. W. Xu, K. Ma and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Network*, vol. 20, pp. 41–47, 2006.

[74] A. C. S. Amin and S. Sastry, "Safe and secure networked control systems under denial of-service attacks," *In Hybrid systems: Computation and Control*, pp. 31–45, 2009.

[75] A. Gupta, C. Langbort, and T. Basar, "Optimal control in the presence of an intelligent jammer with limited actions," *Proc. of the 49th IEEE Conference on Decision and Control, Atlanta, GA, USA*, 2010.

[76] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *computer*, vol. 35, no. 10, pp. 54–62, 2002.

[77] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "Dos attacks in mobile ad-hoc networks: A survey," *second international conference on advanced computing and communication technologies*, pp. 535–541, 2012.

[78] 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.

[79] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Communications surveys and tutorials*, vol. 13, no. 2, pp. 245–257, 2010.

[80] S. Feng and P. Tesi, "Networked control systems under denial-of-service: Co-located vs. remote architectures," *Systems and Control Letters*, vol. 108, pp. 40–47, 2017.

[81] ——, "Resilient control under denial-of-service: Robust design," *Automatica*, pp. 42–51, 2015.

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

[83] C. D. Persis and P. Tesi, "Networked control of nonlinear systems under denial-of-service," *Systems and Control Letters*, vol. 96, pp. 124–131, 2016.

[84] R. Kato, A. Cetinkaya, and H. Ishii, "Stabilization of nonlinear networked control systems under denial-of-service attacks: A linearization approach," *American Control Conference (ACC)*, pp. 1444–1449, 2019.

[85] L. An and G. Yang, "Decentralized adaptive fuzzy secure control for nonlinear uncertain interconnected systems against intermittent dos attacks," *IEEE transactions on cybernetics*, vol. 49, no. 3, pp. 827–838, 2018.

[86] S. Feng, P. Tesi, and C. D. Persis, "Towards stabilization of distributed systems under denial-of-service," *IEEE 56th Annual Conference on Decision and Control (CDC)*, pp. 5360–5365, 2017.

[87] J. L. Peng, Chen and M. Fei, "Resilient event-triggering h_∞ load frequency control for multi-area power systems with energy-limited dos attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 4110–4118, 2017.

[88] T. C. X. S. H. Lemmon, Michael and M. Zyskowski, "On self-triggered full-information h-infinity controllers," *In International Workshop on Hybrid Systems: Computation and Control*, vol. 38, pp. 371–384, 2007.

[89] X. Wang and M. Lemmon, "Self-triggered feedback control systems with finite-gain l2 stability," *IEEE Transactions on Automatic Control*, vol. 54, no. 3, p. 452–467, 2009.

[90] ——, "Self-triggering under state-independent disturbances," *IEEE Transactions on Automatic Control*, vol. 55, no. 6, p. 1494–1500, 2010.

[91] H. Yu and P. Antsaklis, "Event-triggered output feedback control for networked control systems using passivity: Time-varying network induced delays," *50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC)*, p. 205–210, December 2011.

[92] ——, "Event-triggered output feedback control for networked control systems using passivity: Triggering condition and limitations," *50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC)*, p. 199–204, December 2011.

[93] M. Lemmon, "Networked control systems," A. Bemporad, M. Heemels, and M. Johansson, Eds. Berlin Heidelberg: Springer-Verlag, 2010, ch. Event-triggered Feedback in Control, Estimation, and Optimization, pp. 293–358.

[94] M. Abdelrahim, J. Daafouz, and D. Nesic, "Robust event-triggered output feedback controllers for nonlinear systems," *Automatica*, vol. 75, pp. 96–108, 2017.

[95] V. S. Dolk, D. P. Borgers, and W. P. M. H. Heemels, "Output-based and decentralized dynamic event-triggered control with guaranteed lp-gain performance and zeno-freeness," *IEEE Trans. Autom. Control*, vol. 62, no. 1, pp. 34–49, 2017.

[96] M. Ghodrat and H. J. Marquez, "On the local input-output stability of event-triggered control systems," *IEEE Trans. Autom. Control*, vol. 64, no. 1, pp. 174–189, 2018.

[97] X. Chen, Y. Wang, and S. Hu, "Event-based robust stabilization of uncertain networked control systems under quantization and denial-of-service attacks," *Inform. Sci*, vol. 459, pp. 369–386, 2018.

[98] ——, "Event-triggered quantized h control for networked control systems in the presence of denial-of-service jamming attacks," *Nonlinear Analysis: Hybrid Systems*, vol. 33, pp. 265–281, 2019.

[99] J. Hespanha and A. Morse, "Stability of switched systems with average dwell-time," *In Proceedings of the 38th IEEE Conference on Decision and Control*, vol. 3, p. 2655–2660, 1999.

[100] W. Heemels and M. Donkers, "Model-based periodic event-triggered control for linear systems," *Automatica*, vol. 49, no. 3, p. 698–711, 2013.