Security Allocation in Networked Control Systems

Anh Tung Nguyen
Security Allocation in Networked Control Systems

Anh Tung Nguyen
anh.tung.nguyen@it.uu.se

October 2023

Division of Systems and Control
Department of Information Technology
Uppsala University
Box 337
SE-751 05 Uppsala
Sweden

http://www.it.uu.se/

Dissertation for the degree of Licentiate of Philosophy in Electrical Engineering with specialization in Automatic Control

© Anh Tung Nguyen 2023
ISSN 1404-5117
Printed by the Department of Information Technology, Uppsala University, Sweden
Abstract

Sustained use of critical infrastructure, such as electrical power and water distribution networks, requires efficient management and control. Facilitated by the advancements in computational devices and non-proprietary communication technology, such as the Internet, the efficient operation of critical infrastructure relies on network decomposition into interconnected subsystems, thus forming networked control systems. However, the use of public and pervasive communication channels leaves these systems vulnerable to cyber attacks. Consequently, the critical infrastructure is put at risk of suffering operation disruption and even physical damage that would inflict financial costs as well as pose a hazard to human health. Therefore, security is crucial to the sustained efficient operation of critical infrastructure.

This thesis develops a framework for evaluating and improving the security of networked control systems in the face of cyber attacks. The considered security problem involves two strategic agents, namely a malicious adversary and a defender, pursuing their specific and conflicting goals. The defender aims to efficiently allocate defense resources with the purpose of detecting malicious activities. Meanwhile, the malicious adversary simultaneously conducts cyber attacks and remains stealthy to the defender. We tackle the security problem by proposing a game-theoretic framework and characterizing its main components: the payoff function, the action space, and the available information for each agent. Especially, the payoff function is characterized based on the output-to-output gain security metric that fully explores the worst-case attack impact. Then, we investigate the properties of the game and how to efficiently compute its equilibrium. Given the combinatorial nature of the defender’s actions, one important challenge is to alleviate the computational burden. To overcome this challenge, the thesis contributes several system- and graph-theoretic conditions that enable the defender to shrink the action space, efficiently allocating the defense resources. The effectiveness of the proposed framework is validated through numerical examples.
Acknowledgments

First of all, I would like to express my sincere appreciation toward my main advisor André Teixeira who provided me with a remarkable opportunity to commence my academic journey in Sweden, even though I had not completed my Master’s program yet. Your guidance and unwavering support are invaluable to me in dealing with research questions. Despite your busy schedule, you consistently make time on Monday mornings to carefully read my research notes, my manuscripts, and even this thesis, and hold weekly meetings with me. I highly value the way we discuss research problems, an experience I have never had during my years of study across Eastern Asia.

I also extend my gratitude to my co-advisor Alexander Medvedev who even did not meet me before my arrival in Sweden. Thank you for agreeing to guide me on this challenging journey. Although we do not have scientific discussions frequently, you silently provide reflections on my research notes and edit my manuscripts and even this thesis.

I am particularly thankful for the fantastic environment at the Division of Systems and Control, at Uppsala University. It is truly amazing how many exciting discussions and collaborations started during coffee breaks, or on the way to lunch. I would like to thank all my colleagues at the Division of Systems and Control and the Division of Signals and Systems for all the Fika breaks, discussions, and shared memories over the last two years.

A special thanks to Tuan Anh Dao, Sribalaji Coimbatore Anand, and Fatih Emre Tosun for carefully reviewing parts of this thesis.

This work has been financially supported by the Swedish Research Council and the Swedish Foundation for Strategic Research. Their support is greatly acknowledged.

None of this would have been possible without the support from my family and friends. Luckily, I have a great group of Vietnamese who make me feel at home in Uppsala. Thank you all anh Nam, anh Tuan Anh, Luong, Thuan, Son, Huy, and Duc Anh. Special thanks to my parents Tuan Anh and Thu Hang and my sister Minh Ngoc for their support and nurturing throughout my life. My dearest gratitude to my partner Nga for her steadfast support and encouragement throughout this challenging journey and, most of all, ready to be married to a PhD candidate. Nga not only provided me with the mental and emotional support I needed but also offered valuable and constructive suggestions for various parts of this thesis. She dedicated her time to editing figures, and her creative touch extended to crafting the beautiful cover of this thesis.

Tùng
List of Papers

This thesis is based on the following papers


The author has also contributed to the publication below that is not covered in the thesis.

Contents

Notation 2

1 Introduction 3
  1.1 Motivation ................................................. 4
  1.2 Problem Formulation ....................................... 11
  1.3 Outline .................................................. 12
  1.4 Included Papers .......................................... 13

2 Networked Control Systems 17
  2.1 Graph Theory .............................................. 19
  2.2 Modeling and Control of Networked Systems .............. 19
  2.3 Performance .............................................. 23

3 Security in Control Systems 27
  3.1 Control Theory Perspective ................................ 27
  3.2 Security Triad and Potential Threats ...................... 30
  3.3 Attack Strategies .......................................... 33
  3.4 Mitigation Strategies ...................................... 35
  3.5 Research Gaps ............................................. 38

4 Game Theory 39
  4.1 Introduction to Non-cooperative Games .................... 39
  4.2 Nash Equilibrium .......................................... 43
  4.3 Stackelberg Games and Equilibrium ....................... 47

5 Security Allocation 51
  5.1 Networked Control Systems under Stealthy FDI Attacks ... 51
  5.2 Defense and Attack Actions ................................ 52
  5.3 Worst-case Impact of Stealthy FDI Attacks ............... 54
  5.4 Game-theoretic Framework for Security Allocation ........ 57
  5.5 Contributions of the Thesis .............................. 58
6 Concluding Remarks 63
  6.1 Conclusion ................................................. 63
  6.2 Future Work .............................................. 63

References 65

Paper I 83
  1 Introduction ................................................. 83
  2 Problem Formulation ......................................... 86
    2.1 Networked Control System under Attacks ............... 86
    2.2 Optimal Stealthy Data Injection Attack ............. 87
    2.3 Game-theoretic Approach to Monitor Vertex Selection 88
  3 Characterization of Feasible Monitor Vertices .......... 89
  4 Numerical Examples .......................................... 92
  5 Conclusion .................................................. 96

Paper II 99
  1 Introduction ................................................. 100
  2 Problem Description ......................................... 102
    2.1 Networked Control System Description ............... 103
    2.2 Adversary Description .................................. 104
  3 Problem Formulation ......................................... 105
    3.1 Stealthy Data Injection Attack Policy ............... 105
    3.2 Game-theoretic Approach to Sensor Placement ....... 106
  4 Evaluating the Game Payoff .................................. 107
    4.1 Worst-case Attack Impact for a Sampled Uncertainty 107
      Point ...................................................... 108
    4.2 Approximate Game Payoff Function ...................... 108
    4.3 Feasibility Analysis .................................... 110
  5 Numerical Examples ........................................... 112
    5.1 Computing the Approximate Game Payoff .............. 113
    5.2 Examining the Saddle-point Equilibrium .............. 113
    5.3 Computing Mixed-strategy Nash Equilibrium ........... 115
  6 Conclusion .................................................. 116

Paper III 121
  1 Introduction ................................................. 122
  2 Problem Formulation ......................................... 123
    2.1 Networked Control System under Cyber-attacks ....... 123
    2.2 Resources of the Adversary and the Defender ........ 124
    2.3 Strategies of the Adversary and the Defender ........ 125
    2.4 Worst-case Attack Impact on the Local Performance ... 128

viii
3 Optimal Detector Placement ........................................ 129
  3.1 Boundedness of the Worst-case Attack Impact on the
    Local Performance ............................................ 129
  3.2 Game-theoretic Approach to Optimal Detector Place-
    ment ............................................................. 132
4 A Case Study ...................................................... 133
5 Conclusion .......................................................... 135

Paper IV ............................................................. 141
  1 Introduction .................................................... 141
  2 Problem Formulation .......................................... 145
    2.1 Networked Control System under Stealthy Attacks .. 146
    2.2 Worst-case Impact of Stealthy Attacks ............... 147
  3 Characterizing the Set of Monitor Vertices ............... 150
    3.1 Evaluating the Worst-case Impact of Stealthy Attacks 150
    3.2 Infinite Invariant Zeros .................................. 152
    3.3 Dominating Sets ........................................... 153
  4 Stackelberg Security Game .................................... 156
    4.1 Game Setup ................................................ 156
    4.2 Stackelberg Optimal Action .............................. 158
  5 Computational Complexity ..................................... 158
  6 Numerical Example ............................................. 161
    6.1 Computing Stackelberg Optimal Action ................. 162
    6.2 Computational Complexity ................................. 162
  7 Conclusion ...................................................... 164
<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{R}$</td>
<td>Set of real numbers</td>
</tr>
<tr>
<td>$\mathbb{C}$</td>
<td>Set of complex numbers</td>
</tr>
<tr>
<td>$\mathbb{R}_+$</td>
<td>Set of real positive numbers</td>
</tr>
<tr>
<td>$\mathbb{R}^n$</td>
<td>Set of $n$-dimensional vectors with entries in $\mathbb{R}$</td>
</tr>
<tr>
<td>$\mathbb{R}^{n \times m}$</td>
<td>Set of matrices with $n$ rows, $m$ columns, and entries in $\mathbb{R}$</td>
</tr>
<tr>
<td>$\otimes$</td>
<td>Kronecker product</td>
</tr>
<tr>
<td>$t$</td>
<td>Continuous-time instant</td>
</tr>
<tr>
<td>$x(t)$</td>
<td>Continuous-time vector-valued variable</td>
</tr>
<tr>
<td>$A^\top$</td>
<td>Transpose of matrix $A$</td>
</tr>
<tr>
<td>$e_i$</td>
<td>Canonical basis vector where its $i$-th entry is 1 and the other entries are zero</td>
</tr>
<tr>
<td>$\Sigma \triangleq (A, B, C, D)$</td>
<td>Continuous LTI system with its state-space model $\dot{x}(t) = Ax(t) + Bu(t)$, $y(t) = Cx(t) + Du(t)$</td>
</tr>
<tr>
<td>$|x|_{\mathcal{L}_2[0,T]}^2$</td>
<td>$\mathcal{L}_2$-norm of signal $x(t)$ in time horizon $[0,T]$</td>
</tr>
<tr>
<td>$\frac{1}{T} \int_0^T |x(t)|_2^2 , dt$</td>
<td>Given by $\frac{1}{T} \int_0^T |x(t)|_2^2 , dt$</td>
</tr>
<tr>
<td>$|x|_{\mathcal{L}_2}^2$</td>
<td>Shorthand notation for $|x|_{\mathcal{L}_2[0,T]}^2$ if the interval $[0,T]$ is clear from the context</td>
</tr>
<tr>
<td>$\mathcal{L}_2$</td>
<td>The space of square-integrable functions ${f : \mathbb{R}<em>+ \to \mathbb{R} \mid |f|</em>{\mathcal{L}_2[0,\infty]}^2 &lt; \infty}$</td>
</tr>
<tr>
<td>$\mathcal{L}_{2e}$</td>
<td>The extended space of $\mathcal{L}<em>2$ ${f : \mathbb{R}</em>+ \to \mathbb{R} \mid |f|_{\mathcal{L}_2[0,T]}^2 &lt; \infty, \forall 0 &lt; T &lt; \infty}$</td>
</tr>
<tr>
<td>$\mathcal{V}$</td>
<td>Set of vertices associated with a graph</td>
</tr>
<tr>
<td>$\mathcal{E}$</td>
<td>Set of edges associated with a graph</td>
</tr>
<tr>
<td>$N_i$</td>
<td>Set of neighbors of vertex $i$</td>
</tr>
<tr>
<td>$V_{-i}$</td>
<td>$\mathcal{V} \setminus {i}$</td>
</tr>
<tr>
<td>$L$</td>
<td>Laplacian matrix associated with a graph</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

Control technology is a critical aspect of contemporary society due to its deep integration into a large variety of critical infrastructures including but not limited to power systems, transportation networks, and water distribution networks [1–3]. The broad acceptance of automatic control is attributed to the advancements in computation, actuation, and sensing, as well as significant theoretical advancements in the field over the past few decades [4]. At its simplest, a feedback control system involves two fundamental components: a physical plant equipped with sensors to provide measurements of the plant variables, actuators to steer its behavior, and a controller that, based on the measurements, computes the control signal to be applied to the plant through the actuators. This model was ubiquitous in describing feedback control systems until the 1960s when feedback controllers mainly relied on mechanical or analog electronic devices with dependable sensor-to-controller and controller-to-actuator connections (see Figure 1.1a for the illustration).

![Classical control systems with wired communications](Figure 1.1a)

![Modern control systems with wireless communications](Figure 1.1b)
The digital age that began in the 1960s brought with it significant technological developments, including digital controllers and communication networks, resulting in the emergence of networked control systems (NCSs) [5], as illustrated in Figure 1.1b. The advent of information technology (IT) infrastructure allows for the incorporation of low-level control components, such as digital controllers, sensors, and actuators, with high-level supervisory layers, resulting in supervisory control and data acquisition (SCADA) systems that have been widely utilized in industrial control systems (ICSs), as depicted in Figure 1.2. The lower layers of SCADA systems usually include sensors and actuators interfaced with programmable logic computers (PLCs) at local stations or with remote terminal units (RTUs) at remote locations, which generally transmit measurement data to higher layers of the SCADA system through insecure communication networks. The PLCs and RTUs can implement low-level control, receive set points from higher levels, and facilitate communication between different hierarchical layers. The aforementioned SCADA systems also offer other functionalities including human-machine interfaces, workstations, historical databases, and integration with corporate IT systems. This integration has been playing a crucial part in modern ICSs, enabling efficient and flexible operation of the physical systems. However, the integration of IT infrastructure in control systems and the use of ubiquitous telecommunication technologies, such as the Internet and wireless communication, pose new challenges. These challenges include issues such as data packet losses and communication delays, which necessitate the development of novel theoretical foundations [6, 7]. Network interruptions are often regarded as accidental occurrences that lack any deliberate intention. On the other hand, malicious adversaries intentionally emulate those performance issues in networks [8], in order to disrupt communication channels and degrade the system performance. Hence, the security and resilience of control systems against such malicious activities have emerged as significant concerns [4,9,10].

1.1 Motivation

Naively, one might assume that cyber attacks on our critical infrastructures are a hypothetical scenario that belongs to a fictitious future. Unfortunately, these cyber attacks have been already occurring in reality. Hemsley and Fisher provided a list of already launched cyber threats and incidents in ICSs with valuable insights into their vulnerabilities [12]. Surprisingly, they noticed that the first cyber attack was conducted in the demonstration of Marconi’s secure wireless communication with Morse code in 1903. Even though the communication channels were encrypted by Morse code, an in-
1.1. Motivation

Figure 1.2: Systematic of a typical ICS architecture with the SCADA and corporate IT systems. (This figure is adapted from [11])

telligent malicious adversary was able to learn Morse code and manipulate the transmitted data, resulting in the failure of Marconi’s demonstration. Almost 100 years after the first reported attack, Maroochy Water Services
witnessed an incident on its wireless communication channels in 2000, leading to the discharge of more than 1.2 million liters of untreated sewage into local rivers. In 2010, a very well-known cyber attack called Stuxnet was identified after its successful damage to one-fifth of Iran’s uranium hexafluoride centrifuges. Stuxnet could be considered the most advanced malware ever discovered after it infected over 200,000 computers and physically degraded 1,000 machines. Besides the above threats on ICSs, the first successful cyber attack on a power grid was recorded in Ukraine just two days before Christmas 2015. One year later, this attack was relaunched in its second phase to shut off power at 30 substations, leading to power inaccessibility for nearly 230,000 people for up to six hours. This sophisticated malware is now known under the name CRASHOVERRIDE or Industroyer. At the end of 2017, a novel attack framework developed toward ICSs, called TRITON, was reported by FireEye and subsequently confirmed by Symantec and ICS-CERT. This malware targeted Schneider Electric’s Triconex safety instrumented system by modifying in-memory firmware to add malicious functionality, allowing attackers to execute custom code and disable safety processes.

One of the primary factors contributing to the increased prevalence of cyber attacks on ICSs is the relatively low cost of execution. Adversaries with malicious intent can exploit public and unprotected communication channels to maliciously manipulate transmitted data, as opposed to causing physical damage such as actuator faults or sensor malfunctions. Further, they do not need to be physically present at the same location as the target to launch their attack strategies. Even novice hackers lacking comprehensive system knowledge possess the capability to conduct stealthy attacks that can evade traditional fault detection schemes. A notable example occurred in 2008 when a group of Polish teenagers launched a cyber attack to hack the train network [13]. In the following, we elaborately present how the aforementioned cyber attacks on Australia, Iran, and Ukraine were conducted and their catastrophic consequences, which hopefully motivate research on safety and security in ICSs.

Example 1 (Maroochy Water Services).

The Maroochy Water Services cyber attack, which occurred in 2000, stands as a significant milestone in the history of cyber attacks targeting critical infrastructure. Initiated by a disgruntled former employee, who had been fired from his position, the attack exploited his insider knowledge of the Maroochy Water Services’ computerized SCADA system. Around two months, the attacker remotely manipulated the system, wreaking havoc on the water distribution network. By tampering with chemical dosages, di-
verting raw sewage, and disabling alarms, he caused extensive environmental damage, including the release of 1.2 million liters of untreated sewage into local rivers and parks. This event massively caused substantial harm to aquatic organisms, including fish, invertebrates, and plant lives.

**Example 2 (Stuxnet).**

Stuxnet was a specific type of computer worm created with the intention of disrupting Iran’s nuclear program. It gained significant attention from the media, industry, and research community after its discovery in 2010. Unofficially, it is believed to have been jointly developed by the United States and Israel as a covert operation aimed at sabotaging Iran’s nuclear program. The attack can be divided into three stages, as illustrated in Figure 1.3.

1. Initially, Stuxnet infiltrated a uranium enrichment facility by utilizing a USB drive. It then targeted and compromised the localized controllers responsible for operating the uranium enrichment centrifuges (see Figure 1.3a).

2. Subsequently, Stuxnet began to record normal sensor measurements during regular operations (see Figure 1.3b).

3. In the final stage, Stuxnet implemented malicious control actions while sending the previously recorded measurements to the control center (see Figure 1.3c).

This deceptive approach led the operators to falsely believe that the centrifuges were functioning correctly, while the harmful control signals were actually causing damage to the centrifuges. The ultimate consequences of Stuxnet corrupted over 200,000 computers and physically degraded roughly a thousand industrial machines. According to a report provided in [14], the financial damage caused by Stuxnet would be estimated at up to $1 Trillion.

**Example 3 (BlackEnergy & CRASHOVERRIDE).**

Just two days before Christmas 2015, hackers gained access to the computer systems of three regional power distribution companies in Ukraine. Instead of physically accessing the system as Stuxnet in Example 2, they used a combination of phishing emails and malware to remotely infiltrate the power network. The malware used in the attack is known as BlackEnergy, which is a well-known cyber weapon believed to have originated from Russia.
How did this attack work? The hacker first sent several malicious emails, which contained BlackEnergy, to employees of those companies. Through deceptive means, the employees were convinced to install BlackEnergy on their management systems, thereby granting the attackers access to the networks of those companies. Once inside the systems, the attackers launched a coordinated and sophisticated attack, systematically disabling critical infrastructure components and disrupting the power supply. They remotely issued commands to the control systems, causing circuit breakers to open and effectively cutting off the electricity to thousands of homes and businesses. As a consequence, approximately 230,000 customers were left without power for several hours. The affected regions included parts of Kyiv, the capital city, and several other areas in western Ukraine. After almost two years, the electric utility operations in the same area witnessed the second cyber attack, called CRASHOVERRIDE. This attack interrupted the flow of electricity by maliciously manipulating industrial control equipment and delayed recovery operations to prolong its malicious impact. Further, with the purpose of significantly improving its attack impact from itself in
1.1. Motivation

Figure 1.4: The electricity transmission grid in the Baltic Sea Region, including Norway, Sweden, Finland, Denmark, and a part of Eastern Europe [17]. An example of a SCADA system managing the power networks with possible threats.

2015, CRASHOVERRIDE disabled protective relay devices involved in the targeted operations through a Denial-of-Service attack [15].

The aforementioned incidents in Australia, Iran, and Ukraine have served as a wake-up call for managers of other large-scale networked control systems. Attention to safety, security, and resilience in those systems should be paid. Particularly, very large-scale networked control systems such as multinational power networks should be specially focused on since their electricity inaccessibility might cause a significant financial cost [16]. It is therefore essential to place heightened attention on safeguarding these systems. The following example provides insights into potential threats that may manifest in the foreseeable future.

**Example 4** (Potential threats).

Let us take the electricity transmission grid in the Baltic Sea Region
as an example of very large-scale networked control systems, as depicted in Figure 1.4. This grid is characterized by both national and international interconnections that enable the exchange of electricity across borders, encompassing many European countries such as Norway, Sweden, Finland, Denmark, Estonia, Latvia, Lithuania, and parts of Poland and Germany. These interconnections play an important role in guaranteeing a reliable and efficient supply of electricity to those countries. Due to the importance of the power grid, an Energy Management System (EMS) is essential to ensure its safety, security, and resilience, which is depicted in Figure 1.4. One of its most important virtues is to detect the appearance of anomalies in the system. Those anomalies might come from equipment failures (A0), the direct tampering of RTUs (A1 and A2), communication links between the RTUs and SCADA centers (A3 and A4), and malware installed in SCADA centers (A5 and A6). Anomalies, which have their sources at one of those vulnerable points (A0-A6) can be detected by the Bad Data Detector (BDD) of the EMS (see Figure 1.4). However, malicious adversaries, who have been becoming more intelligent, are able to first learn the system behaviors and then exploit multiple risky points to conduct coordinated attacks, such as perfectly undetected attacks and covert attacks [15], on the network. These attacks are capable of obfuscating anomalies in the coming signals of the BDD, leading to their stealthiness. These stealthy attacks may potentially inflict substantial damage to the network before being detected. To address these potential threats, security and resilience solutions have been receiving much attention in recent days.

Motivated by the above observation on past incidents and foreseeable threats, securing critical infrastructure and industrial processes is of utmost importance in countering cyber attacks. Various governments have formulated strategies to safeguard critical infrastructure, including Sweden [18], the United States of America [19], and Germany [20]. The utilization of security measures based on IT like authentication and encryption could still be effective in guaranteeing the integrity of industrial processes. Nonetheless, given the real-time demands and outdated equipment in CPS, relying solely on IT measures may not always be practical, especially to guarantee the confidentiality and availability of ICSs. Furthermore, these measures alone may not be sufficient in facing all intelligent adversaries. Hence, a multi-pronged approach that integrates physical and cyber security measures is necessary to comprehensively secure critical infrastructure and industrial processes.
1.2 Problem Formulation

This thesis addresses the security problem in a networked control system under cyber attacks in which the system is comprised of multiple subsystems, referred as to vertices. Throughout the thesis, we consider a reference architecture of networked control systems, as depicted in Figure 1.5, with the following four components: the physical plant with sensors and actuators, represented by circles; the wireless communication networks, represented by cloud symbols; the physical links connecting plants; and the digital feedback controllers. Digital feedback controllers play a crucial role in fulfilling certain global control objectives. To do that, each digital feedback controller receives the sensor measurement sent by the corresponding physical plant and computes a suitable control signal that is sent back to the actuators of the physical plant over the wireless communication network. Among the physical plants, one plant is selected to represent the local performance of the entire network. The security problem arises when two strategic agents,
namely a malicious adversary and a defender, appear to take their actions toward their specific and conflicting goals. The malicious adversary wants to select a single attack vertex on which to conduct a cyber attack on its input to disrupt the local performance of the entire network while remaining stealthy to the defender. Meanwhile, the defender desires to select several vertices on which to monitor their outputs with the aim of detecting malicious activities caused by the malicious adversary. To fulfill the purposes of the two strategic agents, the thesis focuses on how they find their best actions.

1.3 Outline

The remainder of this thesis will give a deeper introduction to research gaps and all the concepts utilized to fill them. To motivate the importance of NCSs, they are introduced across various applications in Chapter 2. The research gaps are identified through an overview of the literature in Chapter 3. The literature reviews existing attack policies that can be utilized by adversaries and existing mitigation strategies that can be implemented by defenders. Upon the literature review, it is worth noting that the secure control problem is considered from either the defender’s or the adversary’s side. Thus, a framework that encompasses both strategic agents, namely a defender and a malicious adversary, is needed. Clearly, the conflicting objectives of the two agents make cooperation between them infeasible, enabling us to fit the decision-making problem of the two agents into non-cooperative game-theoretic frameworks. Chapter 4 presents a general introduction to a multi-player non-cooperative game and its equilibrium, followed by several classical examples. In Chapter 5, we first present the mathematical description of an NCS under cyber attacks involving the two strategic agents. How the two agents delve into the system modeling and take action on the system is described with greater elaboration. We stand in the middle of the two agents and provide an analysis of the worst-case attack impact. Subsequently, the actions of the two agents are determined through the game-theoretic framework presented in Chapter 4. Based on this analysis, the contributions of included papers are briefly introduced at the end of the chapter. In Chapter 6, we draw a conclusion of the thesis and provide several future research directions.
1.4 Included Papers


**Summary:** The paper considers the security problem in a networked control system comprised of linear first-order subsystems with certain system parameters. We provide a necessary and sufficient condition to assist the defender in efficiently allocating the defense resources. Then, through a zero-sum game-theoretic framework, the paper shows how the defender and the malicious adversary find their best actions with the purpose of fulfilling their conflicting goals.

**Contribution:** The underlying idea came from scientific discussions about numerical results between André M. H. Teixeira and me. After getting key explanations from André M. H. Teixeira, I did the theoretical derivations and the implementations. The writing was mainly my work, with some help from André M. H. Teixeira and Alexander Medvedev in emphasizing the main results.


**Summary:** The paper considers the security problem in a networked control system comprised of linear first-order subsystems with uncertain system parameters. To deal with the presence of uncertainties, the paper shows how the defender and the malicious adversary evaluate the worst-case risk based on the notion of Value-at-Risk. Then, through a zero-sum
game-theoretic framework with the proposed graph-theoretic conditions, the paper shows how the defender and the malicious adversary find their best actions with the aim of fulfilling their conflicting goals.

**Contribution:** The underlying idea came from existing results of Sribalaji C. Anand and André M. H. Teixeira. Theoretical derivations were done by Sribalaji C. Anand and me equally while the implementations were done by me, with some help from André M. H. Teixeira in designing local controllers. The writing was done by Sribalaji C. Anand and me equally.

**Paper III: Optimal Detector Placement in Networked Control Systems under Cyber-attacks with Applications to Power Networks**


**Summary:** The paper considers the security problem in power networks comprised of linear second-order subsystems with certain system parameters. We provide a local control design scheme and a necessary and sufficient condition to assist the defender in efficiently allocating the defense resources. Then, through a zero-sum game-theoretic framework, the paper shows how the defender and the malicious adversary find their best actions with the purpose of fulfilling their conflicting goals.

**Contribution:** Inspired by Alexander Medvedev’s questions on applications of my research, I came up with the underlying idea for this paper, which was then refined and extended in discussions with Sribalaji C. Anand, André M. H. Teixeira, and Alexander Medvedev. Theoretical derivations and the implementations were done by me. The writing was mainly my work with some help from André M. H. Teixeira in emphasizing the results.

**Paper IV: Security Allocation in Networked Control Systems under Stealthy Attacks**

Anh Tung Nguyen, André M. H. Teixeira, and Alexander Medvedev

Summary: The paper considers the security problem in a networked control system comprised of linear first-order subsystems with certain system parameters. We provide a necessary and sufficient condition based on graph-theoretic properties to assist the defender in efficiently allocating the defense resources. By employing a Stackelberg game-theoretic framework with the defender as the leader and the malicious adversary as the follower, we show how the two agents find their best actions with the aim of pursuing their conflicting goals.

Contribution: The underlying idea for this paper was due to André M. H. Teixeira when we expected to extend our existing results in a more practical sense. Theoretical derivations and the implementations were done by me with some help from André M. H. Teixeira in pointing out graph-theoretic properties. The writing was mainly my work with some help from André M. H. Teixeira and Alexander Medvedev in emphasizing the results.
Chapter 2

Networked Control Systems

Network science has been extensively explored across various scientific disciplines, encompassing domains ranging from biological networks and social networks over telecommunication networks and robotic networks to neuroscience and atomic networks (see examples in Figure 2.1). To deal with the complexity of these systems, network science offers a well-designed framework that decomposes these systems into smaller entities (vertices) and links (edges) connecting entities. The decomposition allows us to thoroughly investigate and study how these systems work. However, human demands never stop especially once the operation of these systems is fully understood. We desire to manage these complex systems such that they work for our purposes to achieve certain global objectives. How we study and control these complex systems is introduced in this chapter.
Figure 2.1: Examples of networked systems. a) School of fish; b) Social network; c) Telecommunication network; d) A formation flight of unmanned aerial vehicles; e) An illustration of human neurons; and f) A visualization of the network of carbon atoms.
2.1 Graph Theory

The interaction topology of a networked system is naturally modeled by a graph. More specifically, entities can be described as vertices or nodes of a graph and interactions such as communication and power transmission lines can be represented as edges of the graph. We call the graph associated with the interaction topology of a networked system the interaction graph. In the following, we briefly review basic graph theory which will be utilized throughout this thesis. Readers are encouraged to find more notation and interesting results in [21].

Let $G = (V, E, \tilde{A})$ be a graph with the set of $N$ vertices $V = \{1, 2, ..., N\}$, the set of edges $E \subseteq V \times V$, and the adjacency matrix $\tilde{A} = [\tilde{a}_{ij}]$. For any $(i, j) \in E$, $i \neq j$, the element of the adjacency matrix $\tilde{a}_{ij}$ is positive, and with $(i, j) \notin E$ or $i = j$, $\tilde{a}_{ij} = 0$. The degree of vertex $i$ is denoted as $\Delta_i = \sum_{j=1}^{n} \tilde{a}_{ij}$ and the degree matrix of graph $G$ is defined as $\Delta = \text{diag}(\Delta_1, \Delta_2, \ldots, \Delta_N)$, where $\text{diag}$ stands for a diagonal matrix. The Laplacian matrix is defined as $L = [\ell_{ij}] = \Delta - \tilde{A}$. Further, $G$ is called an undirected connected graph if and only if matrix $\tilde{A}$ is symmetric, the algebraic multiplicity of zero as an eigenvalue of $L$ is one, and the other eigenvalues of $L$ are real positive. The set of all neighbours of vertex $i$ is denoted as $N_i = \{j \in V \mid (i, j) \in E\}$. We denote the subset of $V$ excluding a vertex $i$ as $V_{-i} = V \setminus \{i\}$.

2.2 Modeling and Control of Networked Systems

In this section, we review the modeling and control methodologies of networked systems across various applications. The following examples illustrate several representative control systems that can be efficiently decomposed into interconnected subsystems. Further, how these systems are controlled to reach their global objective will be also described.

Example 5 (Electric power transmission).

An electric power transmission is an interconnected network for electricity delivery from producers to consumers, encompassing various elements such as electricity generators, electrical buses, consumers, and power transmission lines. Figure 2.2 shows the IEEE 14-bus system, which is an example of electric power transmission. In the network, each bus can be considered as a vertex and transmission lines can be considered as edges connecting buses. The purpose of the network is to ensure the synchronization of buses, leading to the stability of the network. To obtain this goal, the swing equations,
which represent the dynamics of buses [22], need to be considered. For bus $i$, let us denote $V_i(t) = |V_i|e^{j\theta_i(t)}$ and $\theta_i(t)$ as the complex voltage and the phase angle of bus $i$, in which the phase angle is governed by the following dynamics:

$$m_i \ddot{\theta}_i(t) + d_i \dot{\theta}_i(t) = \sum_{k \in \mathcal{N}_i} b_{ik} \sin (\theta_k(t) - \theta_i(t)) + P_i(t), \quad (2.1)$$

where $m_i$, $d_i$, and $b_{ik}$ are the inertia, damping coefficients, and the susceptance of the transmission line connecting bus $i$ with bus $k$, respectively. In the dynamics (2.1), $P_i(t)$ stands for the power injection.

In regular operation, the difference between the phase angles of buses is relatively small, allowing us to linearize the nonlinear term in (2.1) to obtain the following linear dynamics:

$$m_i \ddot{\theta}_i(t) + d_i \dot{\theta}_i(t) = \sum_{k \in \mathcal{N}_i} b_{ik} (\theta_k(t) - \theta_i(t)) + P_i(t). \quad (2.2)$$

The linear dynamics (2.2) enables us to design the power injection $P_i(t)$, which can be considered as a control input, with the purpose of achieving synchronization. For example, the power injection can be designed as follows:

$$P_i(t) = -c_i \dot{\theta}_i(t), \quad (2.3)$$
where \( c_i \) is a positive tuning control parameter. Then, the synchronization of the network is achieved, i.e., \(|\theta_i(t) - \theta_j(t)| \to 0\) for all buses \( i \) and \( j \), if the graph representing the network is connected.

**Example 6** (Flocking control).

Flocking is a behavior observed from the natural activities of animals such as birds and fish when they move as a group to efficiently consume their energy (see an example in Figure 2.1a). The effectiveness of flocking motivates researchers to study how they work and imitate flocking in artificial entities [23–26]. Each entity is considered as a vertex and the communication between entities is considered as an edge of the interaction graph. Most existing studies on flocking aim to fulfill the three flocking rules of Reynolds [27]: 1) Flock Centering: attempt to stay close to nearby flockmates; 2) Collision Avoidance: avoid collisions with nearby flockmates; and 3) Velocity Matching: attempt to match velocity with nearby flockmates.

We take the flocking of unmanned aerial vehicles as an example to illustrate how a group of artificial entities imitates a biological behavior. Let us consider nano-quadrotors as unmanned aerial vehicles, depicted in Figure 2.3a. The dynamics of vehicle \( i \) can be described by Euler–Lagrange equations as follows:

\[
\begin{align*}
\dot{p}_{x,i}(t) &= T_i(t) \left[ \cos(\psi_i(t)) \sin(\theta_i(t)) \cos(\phi_i(t)) + \sin(\psi_i(t)) \sin(\phi_i(t)) \right], \\
\dot{p}_{y,i}(t) &= T_i(t) \left[ \sin(\psi_i(t)) \sin(\theta_i(t)) \cos(\phi_i(t)) - \cos(\psi_i(t)) \sin(\phi_i(t)) \right], \\
\dot{p}_{z,i}(t) &= -g + T_i(t) \cos(\theta_i(t)) \cos(\phi_i(t)),
\end{align*}
\]

(2.4)

![Figure 2.3: a) Crazyflie, which is an example of nano-quadrotors used as an educational tool; and b) an illustration of flocking of multiple nano-quadrotors.](image)
where \( p_{x,i}(t), p_{y,i}(t), \) and \( p_{z,i}(t) \in \mathbb{R} \) are the positions, \( \phi_i(t), \theta_i(t), \) and \( \psi_i(t) \in \mathbb{R} \) are the Euler angles of vehicle \( i \) in the Earth frame. The gravitational acceleration is denoted as \( g \) while \( T_i(t) \) stands for thrust force per one mass unit. In engineering applications, quadrotors are controlled by a cascade structure where the Euler angles and thrust force are normally controlled through the speeds of rotors in the inner loop and the positions are managed in the outer loop. Thus, the dynamics (2.4) can be rewritten as follows:

\[
\ddot{p}_i(t) = u_i(t), \tag{2.5}
\]

where

\[
\begin{align*}
p_i(t) &= [p_{x,i}(t), p_{y,i}(t), p_{z,i}(t)]^\top, \\
u_{x,i}(t) &= T_i(t) \left[ \cos(\psi_i(t)) \sin(\theta_i(t)) \cos(\phi_i(t)) + \sin(\psi_i(t)) \sin(\phi_i(t)) \right] , \\
u_{y,i}(t) &= T_i(t) \left[ \sin(\psi_i(t)) \sin(\theta_i(t)) \cos(\phi_i(t)) - \cos(\psi_i(t)) \sin(\phi_i(t)) \right] , \\
u_{z,i}(t) &= -g + T_i(t) \cos(\theta_i(t)) \cos(\phi_i(t)).
\end{align*}
\]

The control input \( u_i(t) \) can be properly designed to achieve the above three flocking rules of Reynolds as follows:

\[
u_i(t) = f_i(t) + h_i(t) + \sum_{j \in N_i} (\dot{p}_j(t) - \dot{p}_i(t)), \tag{2.6}\]

where \( f_i(t) \) and \( h_i(t) \) are the attractive force and the repulsive force, respectively. These forces enable vehicles to satisfy the first two flocking rules of Reynolds (see [24] for more detail). Meanwhile, the last term of input (2.6) enables vehicles to fulfill the last flocking rule and maintain the three rules during the flight, as depicted in Figure 2.3b, if the graph representing the network is connected.

**Example 7** (Formation control and platooning).

Formation control and platooning refer to the control of multiple artificial entities such as robotics and vehicles to efficiently consume resources in completing complicated tasks [23,28–32] (see an example in Figure 2.4a). In the following, nano-quadrotors, as depicted in Figure 2.3a, are still utilized to illustrate how we can control multiple vehicles to obtain desired formation shapes, as depicted in Figure 2.4b. Each vehicle is considered as a vertex and the wireless communication between vehicles is considered as an edge of the interaction graph. In many engineering applications, the positions of the vehicles can be controlled by sending desired velocities [33]. Thus, the dynamics of vehicles can be described as follows:

\[
\dot{p}_i(t) = u_i(t), \tag{2.7}
\]
where $p_i(t) \in \mathbb{R}^3$ is the position of vehicle $i$ in the Earth frame and $u_i(t) \in \mathbb{R}^3$ is the control input of vehicle $i$. The main purpose is to steer vehicles to desired spots which form given shapes for all the vehicles. Let us denote $f_i$ as the desired spot and $e_i(t) \triangleq p_i(t) - f_i$ as the position error of vehicle $i$. The control input can be properly designed as follows:

$$u_i(t) = \sum_{j \in \mathcal{N}_i} (e_j(t) - e_i(t)).$$

(2.8)

The group of vehicles reaches a given formation shape if the graph representing the network is connected.

### 2.3 Performance

In an engineering context, the most crucial objective of a control system is to achieve certain performance specifications as well as ensure the internal stability. One ubiquitous way to describe the performance specifications of a control system is in terms of the size of certain signals of interest. Take a tracking control system as an example where its performance could be measured by the size of the tracking error signal. In this section, we look at several ways of defining the performance specifications of a control system. Naturally, the selection of these approaches to portray the performance is contingent upon the specific applications at hand.

Let us consider a general control system described by the following state-space model:

$$\begin{cases}
    \dot{x}(t) = Ax(t) + Bu(t), \\
y(t) = Cx(t) + Du(t),
\end{cases}$$

(2.9)
where $x(t)$, $u(t)$, and $y(t)$ are the state, the input, and the output of the system, respectively. The output $y(t)$ is the variable that can be measured by sensors. Describing the performance of the system based on such a measured variable might not be enough to fully formulate the performance requirement. Take a quadruple-tank process as an example (see Figure 2.5). The water levels of the four tanks are controlled by two pumps. Only water levels of Tanks 1 and 2 are measured by sensors. Although the water levels of Tanks 3 and 4 are unmeasured, they still belong to our interests. Thus, we need another signal that fully represents the performance of the system. Generally, this performance signal is comprised of measured and unmeasured states, e.g.,

$$y_p(t) = [h_1(t), h_2(t), h_3(t), h_4(t)]^\top,$$

(2.10)

where $h_i$ is the water level of Tank $i$. This output performance $y_p(t)$ is comprised of two measured water levels (Tanks 1 and 2) and two unmeasured water levels (Tanks 3 and 4). After formulating the performance signal, the performance of the system can be fully represented by minimizing the following cost function:

$$J_q = \int_0^T y_p(t)^\top Q y_p(t) \, dt,$$

(2.11)

where $Q \in \mathbb{R}^4$ is a given constant weighting matrix and $[0, T]$ is the considered time horizon. The basic idea is to estimate the unmeasured water levels
through the inputs and the measured water levels by using conventional observers such as Luenberger and high-gain observers [35]. The measured and estimated water levels are then used to find the optimal input signal that minimizes the cost (2.11).

The idea of using performance signals in conventional control systems to describe the performance specifications, as the example above, is adapted in an NCS which is comprised of interconnected subsystems. Let us revisit Examples 5-7. These examples consider $N$ subsystems in which subsystem $i$ has its output $y_i$. The performance specification of the NCS can be considered in the global sense, i.e., outputs of all the subsystems are involved:

$$y_p(t) = [y_1(t), y_2(t), \ldots, y_N(t)]^T.$$  

(2.12)

Optimizing the global performance of the NCS can be translated into minimizing the cost function (2.11) with the performance output given in (2.12), subject to the global dynamics of the NCS. For instance, the global performance of the IEEE bus system is to synchronize all the buses in Example 5.

In other applications of NCSs, not all the subsystems belong to our interests with respect to performance. Only a portion of subsystems might be considered to represent the performance requirement. Let us assume that we apply the flocking control, introduced in Example 6, to a military application where the group of vehicles is required to deliver an important item between locations A and B. The item is kept in the storage of vehicle $i$ while the other vehicles play disguised roles to cover vehicle $i$. Thus, the performance specification of the NCS is considered in the local sense, i.e., the output of vehicle $i$:

$$y_p(t) = y_i(t).$$  

(2.13)

Then, optimizing the local performance of the NCS can be translated into minimizing the cost function (2.11) with the performance output given in (2.13), subject to the global dynamics of the NCS.
Chapter 3

Security in Control Systems

A tight connection between uncertainties and attacks motivates this chapter to first survey the literature on control systems subject to uncertainties. We first briefly review control theory results that are utilized to deal with uncertainty issues such as disturbances and physical faults. Subsequently, we introduce the security triad as a framework to classify potential threats encountered in control systems. Furthermore, we conduct an extensive review of the existing literature concerning the design and implementation of representative attacks targeting control systems. To counter such malicious activities, recent mitigation strategies, which alleviate the malicious impact on control systems, are also reviewed. Finally, we identify research gaps existing in the literature that will be addressed in this thesis.

3.1 Control Theory Perspective

Feedback control systems subjected to uncertainties such as uncertain system parameters, disturbances, stochastic noises, and faults have been receiving much attention from a vast number of researchers in the control system society [36–47]. To efficiently deal with every type of the aforementioned uncertainties, several specific control topics have been categorized, including robust control for uncertain system parameters and disturbances [36–38], fault-tolerant control for physical faults [39–44], and stochastic control [45–47].

• In robust control [36–38], Figure 3.1 shows an example of a control system subjected to uncertainties, in which one desires to design a controller that assists the plant in meeting given performance requirements in case its system modeling is uncertain. One of the most efficient approaches is the well-established $\mathcal{H}_\infty$ controller design [36]. This control design tech-
nique enables us to minimize the worst-case impact of disturbances and uncertainties on the system performance. Its design procedure results in a Riccati-like equation that can be solved offline to shape a control law. This control law affords the system to be robust with respect to unintentional uncertainties. However, in case of crafted uncertainties made by intelligent malicious entities, those robust control laws might be inefficient, which will be discussed at the end of this subsection.

- **In fault-tolerant control** [39–44], one deals with performance degradation problems in control systems caused by physical faults such as actuator faults, sensor faults, and process faults. In a simplistic explanation, those faults alter executing input/measurement signals from their true values, resulting in the degradation of the system performance. Illustrations of those additive faults in control systems are given in Figure 3.2. Assuming that physical faults occur in a control system, a conventional fault-tolerant control scheme is expected to perform three phases interacting with the faults:
3.1. Control Theory Perspective

Figure 3.3: An example of fault-tolerant schemes where
a) detection phase: a residual signal is generated from
the input and the sensor measurement. This signal is
then compared with a predefined threshold to determine
whether an anomaly occurs. If there exists an anomaly,
an alarm is raised to notify the presence of the anomaly;
b) isolation phase: with the same procedure, a bank of
residual signals is generated from different selections of
inputs and measurements. By observing raised and silent
alarms, one knows the location of faulty components.

i) detection; ii) isolation; and iii) response.

1. In the detection phase, the desired mechanism generates a so-called
residual signal based on the system modeling and the sensor measure-
ments. This residual signal is designed such that it is distinguishable
when a fault occurs. In more detail, a norm of the residual signal is
compared with a predefined threshold to determine whether a fault
exists in the system [40] (see Figure 3.3a).

2. In the isolation phase, a group of residual signals is generated in which
each residual signal is computed from a different combination of sen-
sor measurements. By checking those residual signals with predefined
 corresponding thresholds, faulty components can be isolated (see Fig-
3. Once the faulty components are identified, we proceed to the last phase to respond to them. For instance, information from faulty sensors should be discarded in computation or a reconfiguration of the input allocation can be utilized to eliminate the contributions of faulty actuators.

Regrettably, despite the effectiveness of the aforementioned techniques in dealing with disturbances and physical faults, they may prove impractical when confronted with deliberate attacks [48–50]. While disturbances and physical faults are generally considered accidental events without any specific motives and objectives, attacks are meticulously crafted with malicious intent. Moreover, adversaries might gain access to the system management with the purpose of learning the mechanism of anomaly detectors. Armed with this knowledge, they design a coordinated attack that can evade those detection schemes and disrupt the system simultaneously. Given the escalating intelligence of these malicious adversaries, the development of innovative tools becomes imperative to safeguard control systems, particularly large-scale networked control systems. Prior to this development, the following section gives us an analysis of potential threats in networked control systems.

3.2 Security Triad and Potential Threats

The problem of cyber-security has been receiving much attention from researchers in Information Technology society. Its solutions assist the system to hold the classic triad of Confidentiality, Integrity, and Availability (CIA) [51] for data and IT services, which are defined as follows:

**Confidentiality**: requires that stored, transmitted, and processed data is concealed and can be only accessed by authorized parties.

**Integrity**: requires that data is trustworthy, i.e., they cannot be altered by unauthorized methods.

**Availability**: requires that the system provides data in a timely way when they are requested.

Through the above three properties of IT services, attacks are defined as malicious actions against one or a combination of the properties. Malicious actions against the Confidentiality are called eavesdropping attacks. The eavesdropping attacks gain access to communication channels with the purpose of acquiring data that are being stored, transmitted, and processed (see Figure 3.4). They do not cause malicious impacts on the system immediately. However, disclosed data enables hackers to learn the system behaviors with the aim of later launching sophisticated attacks whose consequences are unforeseeable.
Figure 3.4: An illustration of eavesdropping attacks. Alice and Bob are benign agents and share information through unprotected communication channels. Meanwhile, Charlie, who is a malicious agent, accesses the communication network and discloses the shared data of Alice and Bob.

False data injection (FDI) attacks are malicious actions against the Integrity property. In such attacks, adversaries exploit vulnerabilities in communication channels to inject falsified data into genuine data, as depicted in Figure 3.5. These attacks can be perceived as replicas of actuator faults or sensor faults (see Figure 3.2) where input data or observation data is altered with falsified data. Analogously to those physical faults, FDI attacks might cause damage to the system immediately. However, the injected false data is typically crafted with sophistication to evade conventional BDDs, leading to the stealthiness of adversaries. The less system knowledge adversaries have, the simpler one can detect FDI attacks. Several effective methods, which gain uncertainties of system dynamics to adversaries, have been extensively studied such as physical watermarking [52] and multiplicative watermarking [53]. By lessening the system knowledge on the adversaries’ side, those techniques lead to the failure of stealthiness conditions, unmasking malicious adversaries.

Malicious actions that target the Availability property are referred to as Denial-of-Service (DoS) attacks. These attacks neither access communication channels nor acquire trustworthy data from benign agents. Instead, their primary purpose is to disrupt the access of benign agents to the communication network, preventing data from being transmitted over the network,
Figure 3.5: An illustration of false data injection attacks. Alice and Bob are benign agents and share information through unprotected communication channels. Meanwhile, Charlie, who is a malicious agent, accesses the communication network and injects falsified data into the dialogues between Alice and Bob.

as illustrated in Figure 3.6. Consequently, control actions are not reachable from the plant, or observation data does not come to the control center, resulting in prompt degradation in the system performance. Numerous solutions have been proposed to alleviate the malicious impacts of the DoS attacks on the system performance. For instance, techniques such as variable bit rate quantization for quantized control systems [54] and multi-channel transmissions [55] have been proposed as means to mitigate the malicious impacts caused by DoS attacks.
3.3 Attack Strategies

Exploiting various resources such as the disclosure resource, disruption resource, and system knowledge of ICSs, a wide range of attack types aim to compromise the essential properties of the CIA. Notably, the notorious Stuxnet attack [56] serves as a well-known example of replay attacks (see Example 2 for a detailed exposition). This attack unfolds in two distinct phases. In the first phase, adversaries infiltrate the management system with the purpose of recording data, thereby undermining the principle of Confidentiality. In the subsequent phase, the recorded data is replayed into the management system while concurrently injecting malicious actions into physical infrastructure, resulting in a breach of the Integrity property. The immense success achieved by Stuxnet has served as a catalyst, prompting the emergence of a multitude of sophisticated and advanced attacks. This attack has garnered considerable attention among researchers, underscoring the paramount importance of addressing safety and security concerns within the realm of control systems.

Naturally, the resounding triumph of Stuxnet [56] (see Example 2) as an exemplary case of replay attacks on ICSs promotes numerous researchers to delve into the realm of advanced replay attack methodologies. Detection techniques such as watermarking [53, 57] have emerged as highly effective
tools in unveiling the occurrence of replay attacks. However, in the pursuit of evading watermarking detection schemes in control systems, Zhang et al. [58] have ingeniously combined the zero-dynamics property inherent in dynamic systems with traditional replay attack techniques, thereby giving rise to a novel breed of attacks known as generalized replay attacks. Notably, these insidious attacks manage to not only maintain their stealthiness in the face of watermarking detection schemes but also pose catastrophic consequences for non-minimum phase systems. Furthermore, concerted efforts have been directed toward the development of replay attacks tailored specifically for Internet of Things (IoT) applications [59–61]. These endeavors aim to exploit vulnerabilities in IoT systems, thereby amplifying the significance of addressing replay attack concerns in the context of IoT-enabled environments.

The idea of exploring the zero-dynamics property through unstable invariant zeros of dynamical systems was not only utilized in designing generalized replay attacks in [58], but also promoted in [62] where Zhang and Ye showed a useful design of an attack signal. The signal falls into the category of output-zeroing inputs, which leave no trace at the detection output. This characteristic allows malicious adversaries to be stealthy to conventional detection schemes. To design such a stealthy attack, malicious adversaries need to know system knowledge and alter data transmitted over communication channels. This unauthorized data manipulation compromises the Integrity property of the system. With the similar purpose of leaving minimal traces at the detection output, malicious adversaries disclose real-time data of the system to construct optimization problems that yield stealthy attack signals [49,63]. Those adversaries require unauthorized access to communication channels and the ability to alter data, violating the Confidentiality and Integrity properties of the system. Considering conventional detection schemes in designing stealthy attacks might leave adversaries risky to be detected [49,62,63]. To address this concern, several authors have incorporated the Kullback-Leibler divergence in their work [64–66], aiming to minimize the distinction between healthy and attacked detection outputs. The technique requires no additional resources beyond those outlined in [49,63] but enables adversaries to be stealthy to ubiquitous anomaly detection schemes, which consider residual signals between healthy and attacked detection outputs. By specifically targeting the central state estimation in distributed sensor networks, Lu and Yang [67] proposed a sparse sensor attack that replicates the true system modeling to generate fake measurement data. Furthermore, a captivating avenue of research emerges with the integration of machine learning techniques for the design of stealthy attack signals [68].

Considering more practical system modeling is one possible extension to the idea of utilizing the zero-dynamics property of dynamic systems in
designing stealthy data injection attacks. Zhang et al. [69] adopted the concept of controlled invariant subspace, which results from geometric control theory and is decoupled with the system outputs and the nonlinear function, to propose a stealthy attack on a class of nonlinear systems. Tackling nonlinear systems poses significant challenges, requiring adversaries to delve into system knowledge and disclose real-time transmitted data. Instead of considering nonlinear system modelings, Park et al. [48] focused their study on potential threats in linear systems subjected to uncertainties. The attack signals in [48] were designed based on the zero-dynamics property of the nominal linear system in the first phase. Nonetheless, due to uncertainties in system modeling, the attack may fail short of satisfying the stealthiness condition derived from linear system modeling, resulting in the presence of detectable traces at the detection output. To overcome this limitation, they introduced an adaptive mechanism-based scheme to properly adjust the attack signals based on real-time control and measurement data. Clearly, the above attacks designed for two examples of practical system modeling necessitate system knowledge, disclosure, and disruption resources, breaking down the Confidentiality and Integrity properties of the system.

Deliberately compromising the Availability property of systems presents a viable means of degrading the system performance. The typical attack scheme is DoS attacks that interrupt communication channels, as illustrated in Figure 3.6. Obviously, malicious adversaries are unable to perform communication interruption for a very long period of time due to energy constraints. In this regard, Zhang et al. [70] proposed an optimal schedule for DoS attacks on remote sensor networks where sensor measurement data needs to be sent to a remote estimator. This schedule empowers adversaries to maximize the estimation errors of the remote estimator through consecutive jamming attacks. Subsequently, the same group of authors, then, developed this idea for DoS attacks on wireless networked control systems to maximize the Linear Quadratic Gaussian control cost [71]. The idea of the optimal DoS schedule was also extended by considering different communication scenarios such as packet-dropping networks [72], round-robin protocol [73], and adapting system behaviors [74].

3.4 Mitigation Strategies

Standing on the defense side, we desire to have mitigation strategies against malicious activities that violate the triad of the CIA properties introduced earlier. The mitigation strategies are normally classified into three different categories, which are Detection, Prevention, and Resilience [75].

Detection refers to techniques that can notify the presence of an attack,
identify its attacking location, and actively mitigate its malicious impact.

**Prevention** encompasses techniques that can dodge an attack or suspend the beginning of an attack.

**Resilience** assists the system to operate as close as possible to regular situations while involving the effect of an attack.

The expensive lesson learned from the catastrophic consequences of Stuxnet [14] (see Example 2) remains its value to this day. After remarkably succeeding in Stuxnet, replay attacks have served as a wellspring of inspiration for numerous researchers in finding effective detection schemes. Digital watermarking, which originated in 1993 [76], is one of the most popular techniques used to identify the ownership of noise-tolerant signals, images, and audio by embedding discreet markers in them. Inspired by the use of digital watermarking, Mo and Sinopoli were among the pioneers to bring the idea of watermarking to detect replay attacks on control systems [57]. They added a low-energy noisy signal, which we know its distribution, to the control input before sending it to actuators. Subsequently, traces of the added noisy signal are observed at the output, which enables us to detect replayed data. The added noisy signal is called physical watermarking. The idea of utilizing physical watermarking to detect replay attacks on control systems has been extended across various domains, encompassing topics such as optimal watermarking schedule [77], detecting generalized replay attacks [78], replay attacks on multi-agent systems [79], quickest detection requirement [80], and sequential detection [81].

Although physical watermarking has proven effective in detecting replay attacks on control systems [57,77–79], two drawbacks come with it. Since the additive watermark is a noisy signal, it basically degrades the performance of the system and burdens actuators. To overcome such shortcomings, multiplicative watermarking has been introduced as an alternative approach for detecting replay attacks [82]. Basically, this method consists of two steps, which are encoding and decoding. At each step, signals, which need to be transmitted, are fed to an SISO filter with time-varying piecewise constant parameters. It is noteworthy that the encoding filter is the inverse of the decoding filter. Switching the parameters of those filters might fool adversaries into replaying data that bypassed the old filter, making the difference between the replayed data and the true data. This difference allows us to detect the replay attack by utilizing conventional detection schemes. Due to the utmost importance of the switching, this multiplicative watermarking was, then, equipped with an automatic switching mechanism by the same group of authors, Ferrari and Teixeira [53].

In addition to replay attacks, eavesdropping attacks have been also receiving much attention due to their potential risks. Interestingly, the eavesdropping attacks perform the first stage of replay attacks to collect true data
from operating control systems. However, they abandon the second stage of replay attacks, so their attack policies and consequences are unforeseeable. Consequently, preventing such attacks is of paramount importance. Drawing inspiration from the concept of multiplicative watermarking [53, 82], encoding and decoding have been also employed to dodge the eavesdropping attacks with the aim of ensuring the Confidentiality property of the processed data in the entire control loop [83–91]. The underlying principle revolves around a bijective mapping that enables the transformation of true data into ciphertext, with the critical distinction that only a single legitimate entity possesses the inverse mapping. This design ensures that even if malicious adversaries manage to intercept and access communication channels transmitting the ciphertext, they lack the necessary resources to retrieve the original, unencrypted data.

DoS attacks that interrupt data transmission through communication channels have been extensively studied across various computer science domains. In the realm of computer security, Carl et al. [92] introduced several ubiquitous detection techniques, such as activity profiling, sequential change-point detection, and wavelet analysis to detect DoS attacks. However, the integration of physical layers, encompassing dynamical plants, actuators, and sensors, within cyber layers presents a fresh set of challenges for networked control systems in the face of DoS attacks. To enhance the resilience of control systems, Amin, Cárdenas, and Sastry proposed optimal control problems against DoS attacks to minimize their malicious impacts [93]. By considering the worst-case scenario of DoS attacks with the maximum attack duration, Feng and Tesi [94] guaranteed that the system states do not go to infinity before network recovery through a robust design framework, maintaining the resilience of the system. Another potential countermeasure against DoS attacks is to increase the data bit rate, as it enables senders to transmit information more frequently, thereby mitigating the detrimental effects of attacks [54, 95, 96]. Moreover, the utilization of multiple communication channels to transmit the same information enhances the likelihood of data reaching its intended destination, thereby bolstering system resilience [55].

Beyond those above attacks, stealthy FDI attacks have been gaining popularity in the control system society due to their significant malicious impacts. Adversaries adeptly exploit their profound understanding of system knowledge and data eavesdropping techniques, rendering them stealthy to conventional and even modern detection methods. Consequently, more advanced detection schemes are demanded. Physical watermarking, originally developed for detecting replay attacks, has been adapted to notify the presence of FDI attacks in [52, 97]. This idea has been recently developed to reduce the average detection delay time in [80]. As discussed above, physical
watermarking often worsens the control cost and the lifetime of actuators in control systems. One of the neat solutions to such issues is multiplicative watermarking [50, 53, 98]. Reallocating defense sources also assists us in mitigating the malicious impact of adversaries [99], obtaining the resilience of the system under stealthy FDI attacks. However, it is crucial to recognize that current intelligent adversaries have the potential to learn and adapt to these mitigation strategies, thereby refining their attack policies to regain their stealthiness. Consequently, the intelligence and adaptability of adversaries necessitate a thorough investigation of networked control systems under the influence of stealthy FDI attacks in this thesis.

3.5 Research Gaps

Upon review of the above existing studies [8, 48–50, 52–55, 57–74, 77–101], it becomes evident that the literature has primarily focused on secure estimation and control from the viewpoint of either the defender or the adversary. However, it is important to acknowledge that both parties encounter similar challenges. While the defender confronts resource limitations in countering malicious activities, the adversary also faces energy constraints during attack execution. Therefore, it is highly pertinent to address this matter within a comprehensive framework that encompasses both the defender and the adversary.

Fortunately, the security allocation problem between the defender and the malicious adversary fits well within the framework of game theory, which is one of the most efficient frameworks addressing the challenge of optimal decision-making among non-cooperative parties [102]. A general introduction to non-cooperative games and how they address the security allocation problem will be provided in the following chapter. Furthermore, the objectives of both the defender and the malicious adversary have not been adequately formulated in the existing literature. This deficiency will be addressed in Chapter 5.
Chapter 4

Game Theory

In this chapter, we first present the general introduction to multi-player non-cooperative games in which each player puts an effort to find an optimal strategy with the aim of obtaining the best game payoff. What shapes the optimal strategies for the players is called the equilibrium of the game. In the second section, after assuming that the players make their decisions at the same time, we analyze the equilibrium of the game through the concepts of the Nash equilibrium (NE) in deterministic and mixed strategies. While the former tells us the deterministic strategies of the players, the latter shows us the probabilistic strategies of the players. The assumption that the players are forced to make their decisions at the same time might be impractical in many contexts [103–109]. To address such an issue, we relax the assumption by introducing the Stackelberg game where one player acts as the leader and the other players act as the followers. In the Stackelberg game, the leader has the power to move first with knowing that the followers will base their strategies on the leader’s decision.

4.1 Introduction to Non-cooperative Games

In the realm of game theory, the focus lies on the strategic interactions that occur among multiple decision-makers, known as players. Each player possesses a preference ordering regarding various alternatives, which is captured within an objective function specifically tailored for that player. This objective function aims to either maximize the player’s outcomes (where it takes the form of a utility or benefit function) or minimize them (in which case it is referred to as a cost or loss function).

In the context of a non-trivial game, the objective function of a player is contingent upon the choices made by at least one player, often involving all players in the game. Consequently, a player cannot simply optimize their
own objective function in isolation from the decisions made by other players. This interdependency establishes a linkage between the actions taken by all the players, binding them together in the decision-making process, even within a non-cooperative setting. If the players are allowed to cooperate with each other to take the final actions, those actions are fully trusted by all the players, resulting in the highest benefits for them without any inefficiency. This interaction is also known as cooperative games, which are not covered in this thesis.

On the other hand, in the absence of any possibility or allowance for cooperation among players, we enter the domain of non-cooperative game theory, where the establishment of a satisfactory solution concept becomes crucial. Setting aside the matter of how players can reach such a satisfactory solution, we demand to figure out the minimum characteristic of the satisfactory solution through the following question: Why are all the players happy to stay at the satisfactory solution? A straightforward answer should be: If a player unilaterally moves away from his satisfactory position, he does not increase his incentive. Consequently, this player does not have any motivation to move away from his satisfactory position. It is important to note that allowing two or more players to collectively deviate from the satisfactory solution would require cooperation among players, which is explicitly prohibited in the non-cooperative game setting. Hence, a solution point where no player can enhance their benefit through a unilateral move is termed a non-cooperative equilibrium or Nash equilibrium, named after John Nash, who introduced and demonstrated its existence in finite games (where each player has only a finite number of alternatives) nearly seventy years ago [110].

The games can be defined with four components, consisting of the players, the set of possible actions for each player (so-called action space), the payoff corresponding to each possible action for each player, and the information structure of the games [111]. To be simplistic, we mainly focus on two-player games in the non-cooperative setting. Each player has a finite number of possible actions, i.e., the players pick their actions out of finite action spaces, so it is called finite games or matrix games. We say that a two-player game is a zero-sum game, if the gain of a player is exactly the same as the loss of the other player and vice versa. Otherwise, it is called a non-zero-sum game. In this thesis, the concept of zero-sum games is applied in Papers I-III, while the notion of non-zero-sum games is considered in Paper IV. To offer readers, who are unfamiliar with game theory, a better grasp of non-cooperative games, we present two classical examples which consist of a zero-sum game and a non-zero-sum game in the following.
4.1. Introduction to Non-cooperative Games

Table 4.1: Components of the Matching Pennies game

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Players</td>
<td>Even and Odd</td>
</tr>
<tr>
<td>Action Space</td>
<td>Each player chooses Head or Tail</td>
</tr>
<tr>
<td>Game Payoff</td>
<td>Given in Table 4.2</td>
</tr>
<tr>
<td>Information Structure</td>
<td>Actions taken secretly</td>
</tr>
</tbody>
</table>

Table 4.2: The game payoff matrices for Even (left table) and for Odd (right table)

<table>
<thead>
<tr>
<th></th>
<th>Odd</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Head</td>
<td>Tail</td>
</tr>
<tr>
<td>Even</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td></td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Odd</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Head</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>Tail</td>
<td>1</td>
<td>-1</td>
</tr>
</tbody>
</table>

Example 8 (Matching Pennies).

This is a simple game commonly used in the introduction to game theory. It involves two players, named Even and Odd. Each player possesses a penny and must secretly decide whether to turn it into Head or Tail, which are his two possible actions. Due to the secret action, the players do not know the true action of the opponent. Once both players have taken their actions, they reveal them simultaneously. If the outcomes match (both heads or both tails), Even retains both pennies, resulting in a gain of one from Odd (+1 for Even, -1 for Odd). Conversely, if the outcomes differ (one head and one tail), Odd keeps both pennies, receiving one from Even (-1 for Even, +1 for Odd). To conveniently follow the game, let us summarize the components of the game in Table 4.1. By observing the game payoff matrices in Table 4.2, the gain of a player is exactly the loss of the other player. Thus, this competition is categorized as a zero-sum game.

Example 9 (Prisoner’s’ Dilemma).

This is a classic example of a non-zero-sum game that illustrates the tension between individual rationality and collective cooperation. In the Prisoners’ Dilemma, two individuals are arrested for a crime, and they are held separately without the ability to communicate and offered the standard deal: help with the investigation, one will be treated with leniency. The offer is described elaborately in three possibilities:
Table 4.3: Components of the Prisoners’ Dilemma

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Players</td>
<td>Prisoner A and Prisoner B</td>
</tr>
<tr>
<td>Action Space</td>
<td>Each Prisoner defects or remains silent</td>
</tr>
<tr>
<td>Game Payoff</td>
<td>Given in Table 4.4</td>
</tr>
<tr>
<td>Information Structure</td>
<td>Actions given secretly</td>
</tr>
</tbody>
</table>

Table 4.4: The game payoff matrices for Prisoner A (upper table) and Prisoner B (lower table).

<table>
<thead>
<tr>
<th>Prisoner A</th>
<th>Silent</th>
<th>Defect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silent</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Defect</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prisoner A</th>
<th>Silent</th>
<th>Defect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silent</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Defect</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

1. If both prisoners remain silent, they will both receive a reduced sentence for a lesser charge (payoff of 3);

2. If one prisoner remains silent while the other defects, the defector will receive a greatly reduced sentence (payoff of 4), while the other prisoner will receive a harsher sentence (payoff of 0); and

3. If both prisoners defect, they will both receive a moderately reduced sentence, but still longer than if they had both remained silent (payoff of 1).

To improve the reading experience, let us summarize the components of the game in Table 4.3 in which the game payoff matrices are given in Table 4.4. From the game payoff matrices in Table 4.4, the gain of a prisoner is not the same as the loss of the other prisoner. Therefore, this competition is categorized as a non-zero-sum game.

After showing the importance of the satisfactory solution of a non-cooperative game, also known as NE, we introduce general formulations of a non-cooperative game and how to find its NE in the following section.
4.2 Nash Equilibrium

In this section, we desire to characterize the satisfactory solution to the non-cooperative game where all the players take their actions secretly. First, we make use of the following notation used for an $M$-player non-cooperative game. The player set $\mathcal{P} = \{1, 2, \ldots, M\}$. The action variable of Player $i$ is denoted by $\omega_i \in \Omega_i$, where $\Omega_i$ is the finite action space of Player $i$. For convenience, let us denote $\omega$ as the $M$-tuple of action variables of all the players, $\omega = (\omega_1, \omega_2, \ldots, \omega_M)$ and $\Omega$ as the $M$-product of the action spaces. Consequently, one has $\omega \in \Omega$. The objective function of Player $i$ is denoted by $J_i(\omega_i, \omega_{-i})$, where $\omega_{-i}$ stands for the action variables of all the players except the one of Player $i$.

Now, we are ready to denote an $M$-tuple of action variables $\omega^* \in \Omega$ as an NE of the non-cooperative game. Suppose that Player $i$ is a maximizer, whose objective function is the utility function or benefit function. The definition of NE in the previous section tells us that a unilateral deviation made by Player $i$ does not gain his benefit, resulting in the following condition:

$$ J_i(\omega^*_i, \omega_{-i}) \geq J_i(\omega_i, \omega^*_i), \quad \forall \omega_i \in \Omega_i \text{ such that } (\omega_i, \omega^*_i) \in \Omega. \quad (4.1) $$

We have a similar condition for Player $k$, who is a minimizer, as follows:

$$ J_k(\omega^*_k, \omega_{-k}) \leq J_k(\omega_k, \omega^*_k), \quad \forall \omega_k \in \Omega_k \text{ such that } (\omega_k, \omega^*_k) \in \Omega. \quad (4.2) $$

In the case of a non-cooperative two-player game ($M = 2$) and $J_1(\cdot) = -J_2(\cdot) = J(\cdot)$, we have a two-player zero-sum game where Player 1 is a maximizer and Player 2 is a minimizer. The NE of this game $(\omega^*_1, \omega^*_2)$ is formulated as follows:

$$ J(\omega_1, \omega^*_2) \leq J(\omega^*_1, \omega^*_2) \leq J(\omega^*_1, \omega^*_2), \quad \forall (\omega_1, \omega_2) \in \Omega. \quad (4.3) $$

The optimal solution $J(\omega^*_1, \omega^*_2)$ can be found through the following optimization problem if it is feasible.

$$ \max_{\omega_1 \in \Omega_1} \min_{\omega_2 \in \Omega_2} J(\omega_1, \omega_2) = \min_{\omega_2 \in \Omega_2} \max_{\omega_1 \in \Omega_1} J(\omega_1, \omega_2) = J(\omega^*_1, \omega^*_2). \quad (4.4) $$

Next, we are going to revisit Examples 8-9 to examine their NE in deterministic strategies.

Recall the zero-sum Matching Pennies game in Example 8, both players in this game desire to maximize their game payoffs which are given in Table 4.2. Since it is a zero-sum game, we only need to consider the left table in Table 4.2 where Even is a maximizer and Odd is a minimizer. We observe that no deterministic action for a player can be selected to surely win over...
the opponent (get the payoff of 1) in all the scenarios. Alternatively, for any pair of actions taken by the two players, a unilateral deviation made by the loser (payoff of −1) always promotes him as the winner (payoff of 1), which conflicts with the definition of NE (4.3). Consequently, no NE exists in the Matching Pennies game.

Let us revisit the Prisoners’ Dilemma in Example 9 where both players strive to maximize their game payoffs given in Table 4.4. For any action taken by Prisoner B, taking a Defect always gives Prisoner A a better game payoff. A similar scenario is also true for Prisoner B. If both Prisoners are taking Defect, a unilateral deviation made by a Prisoner from Defect to Silent surely decreases his/her game payoff from 1 to 0. Therefore, the strategy (Defect, Defect) selected by the two Prisoners satisfies the NE (4.3).

From the above analyses of NE in deterministic strategies, we basically grasp the concept of a pure NE in a non-cooperative game. Unfortunately, the zero-sum Matching Pennies game (Example 8) does not admit a pure NE. Indeed, a matrix game does not necessarily exhibit a pure NE in general [112]. Intuitively, the absence of a pure NE for a non-cooperative game, for example, Example 8, raises a natural question: Are the players trapped in the dilemma of decision-making? They need to find the other way to determine their strategies. An alternative solution is the mixed strategy or randomized strategy.

In the mixed strategy, the players randomize their strategies over their entire action spaces. More specifically, let us denote $p_i \in P_i$ as the probability distribution of Player $i$ where $P_i$ is the set of all probability distributions on his action space $\Omega_i$. We denote $P$ as the $M$-product of probability distributions on the action space of all the players $\Omega$. The pure objective function $J_i(\cdot)$ is replaced with the expected objective function with respect to the probability distributions of all the players, which is denoted as $\bar{J}_i(p_1, p_2, \ldots, p_M)$. The NE in mixed strategies is denoted as $(p_1^*, p_2^*, \ldots, p_M^*)$. If Player $i$ is a maximizer, the mixed-strategy NE satisfies

$$\bar{J}_i(p_i^*, p_{-i}^*) \geq \bar{J}_i(p_i, p_{-i}^*), \quad \forall p_i \in P_i, \text{ such that } (p_i, p_{-i}^*) \in P.$$  \hspace{1cm} (4.5)

This implies that a unilateral deviation of the probability distribution made by Player $i$ does not gain his incentive. Analogously, if Player $k$ is a minimizer, the mixed-strategy NE satisfies

$$\bar{J}_k(p_k^*, p_{-k}^*) \leq \bar{J}_k(p_k, p_{-k}^*), \quad \forall p_k \in P_k \text{ such that } (p_k, p_{-k}^*) \in P.$$  \hspace{1cm} (4.6)

In the case of zero-sum two-player games where Player 1 is a maximizer
and Player 2 is a minimizer, the mixed-strategy NE is formulated as follows:

\[ J(p_1, p_2^*) \leq J(p_1^*, p_2^*) \leq J(p_1^*, p_2), \quad (p_1, p_2) \in P, \]  

(4.7)

where

\[ J(p_1, p_2) = p_1^\top [J(\omega_1, \omega_2)] p_2, \]  

(4.8)

and \([J(\omega_1, \omega_2)]\) represents the game payoff matrix. Here, the value of the zero-sum two-player game in mixed-strategy is \( J^* = J(p_1^*, p_2^*) \). To be more illustrative, we apply the concept of the mixed-strategy NE (4.7) to the zero-sum Matching Pennies game in the following.

Followed by the discussion above, we have already known that the Matching Pennies game does not admit an NE in deterministic strategies, affording us to analyze its mixed strategies. Let us denote the probability distribution over the action space of the players in the following: Even chooses Head with a probability \( p_1 \) and Tail with a probability \( 1 - p_1 \). Meanwhile, Odd chooses Head with a probability \( p_2 \) and Tail with a probability \( 1 - p_2 \). Consequently, we denote \( p_1 = (p_1, 1 - p_1) \) and \( p_2 = (p_2, 1 - p_2) \) as the mixed strategies of Even and Odd, respectively. Denote \((p_1^*, p_2^*)\) as the NE in mixed strategies. To be more convenient, we rewrite the game payoff matrix of Even with the corresponding probability distribution in Table 4.5.

By mainly considering the game payoff matrix of Even in Table 4.5, the zero-sum Matching Pennies game tells us that Even is the maximizer and Odd is the minimizer of the game. Assuming that Even chooses the mixed-strategy NE (say \( p_1^* = (p_1^*, 1 - p_1^*) \)) and Odd chooses an arbitrary strategy (say \( p_2 = (p_2, 1 - p_2) \)), the expected game payoff for Even is computed based on the game payoff matrix given in Table 4.5 as follows:

\[
J(p_1^*, p_2) = p_1^* \times 1 \times p_2 + p_1^* \times (-1) \times (1 - p_2) \\
+ (1 - p_1^*) \times (-1) \times p_2 + (1 - p_1^*) \times 1 \times (1 - p_2) \\
= (4p_1^* - 2)p_2 - 2p_1^* + 1. 
\]  

(4.9)

The concept of the mixed-strategy NE (4.7) tells us that a unilateral deviation of the probability distribution taken by Odd does not decrease the expected game payoff for Even. Consequently, the expected game payoff in (4.9) should be independent of \( p_2 \), resulting in the following equation:

\[ 4p_1^* - 2 = 0 \iff p_1^* = 0.5. \]  

(4.10)

Conversely, assuming that Odd chooses her mixed-strategy NE (say \( p_2^* = (p_2^*, 1 - p_2^*) \)) and Even chooses an arbitrary strategy (say \( p_1 = (p_1, 1 - p_1) \)),
Table 4.5: Game payoff matrix of Even in the zero-sum Matching Pennies game with the probability distributions where Even is the maximizer and Odd is the minimizer.

<table>
<thead>
<tr>
<th>Even</th>
<th>Head</th>
<th>Tail</th>
<th>Probability</th>
<th>mix-str. NE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>-1</td>
<td>$p_1$</td>
<td>0.5</td>
</tr>
<tr>
<td></td>
<td>-1</td>
<td>1</td>
<td>$1 - p_1$</td>
<td>0.5</td>
</tr>
<tr>
<td>Probability</td>
<td>$p_2$</td>
<td>$1 - p_2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mix-str. NE</td>
<td>0.5</td>
<td>0.5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

the expected game payoff for Even is computed as follows

$$
\bar{J}(p_1, p_2^*) = p_1 \times 1 \times p_2^* + p_1 \times (-1) \times (1 - p_2^*) \\
+ (1 - p_1) \times (-1) \times p_2^* + (1 - p_1) \times 1 \times (1 - p_2^*) \\
= (4p_2^* - 2)p_1 - 2p_2^* + 1. \tag{4.11}
$$

Analogously, based on the definition of the mixed-strategy NE (4.7), a deviation of the probability distribution of Even does not gain his expected game payoff, resulting in the following equation:

$$
4p_2^* - 2 = 0 \iff p_2^* = 0.5. \tag{4.12}
$$

The above analysis gives us the NE in mixed strategies for the two players, Even and Odd, which is $p_1^* = (0.5, 0.5)$, $p_2^* = (0.5, 0.5)$. By choosing the mixed-strategy NE, the expected game payoff for both players is the same at $\bar{J}(p_1^*, p_2^*) = 0$.

In summary, the above non-cooperative game well describes how the players determine their optimal strategies in order to obtain their suitable utilities. The first concept of the satisfactory solution of the game, the pure NE, showed the deterministic strategies for the players where they are simultaneously happy with their obtained utilities. However, a pure NE is not guaranteed to exist in general (see Example 8). Consequently, we introduced the second concept of the satisfactory solution of the game, the mixed-strategy NE. This mixed-strategy NE serves as an alternative solution, allowing for a range of strategies that are based on probability distributions over the action spaces of the players.

On the other hand, the non-cooperative game described above assumes that the players investigate their action spaces to determine their optimal
strategies at the same time. Nonetheless, in practice such as security games and competitive pricing [103], one player has the power to take action first. For example, in competitive pricing among several companies where one company is a giant and the others are startups. The giant has the power to make its pricing strategy first with knowing that the others base their pricing strategies on its decision. Subsequently, the other companies have to react to the leader’s strategy. In security games where a defender competes with adversaries, the defender has the power to choose their defense strategies regardless of the appearance of the adversaries. Then, the adversaries have to react to the chosen defense strategy. To address such a practical issue, the next section introduces a different game that better suits the context of security games in this thesis.

4.3 Stackelberg Games and Equilibrium

This section introduces a non-cooperative game with a different information structure, the Stackelberg game. A key distinct point is that a player is called the leader who has the power to take action first. Then, the leader announces his action to the other players who are called the followers. The followers have to react to the leader’s action after fully observing it.

We consider an $M$-player Stackelberg game and use the same notation as the previous section. Without loss of generality, we denote Player 1 as the leader of the game while the other players are the followers. Assuming that the leader is a maximizer who wishes to maximize his objective function $J_1(\omega_1, \omega_{-1})$, the leader has the power to take action first. Let us denote $\omega_1^{\dagger}$ as the best response of the leader that can be found by solving the following optimization problem:

$$\omega_1^{\dagger} = \arg \max_{\omega_1 \in \Omega_1} J_1(\omega_1, \omega_1^{\dagger}(\omega_1)), \quad (4.13)$$

where

$$\omega_1^{\dagger}(\omega_1) = \arg \min_{\omega_{-1} \in \Omega_2 \times \Omega_3 \times \ldots \times \Omega_M} J_1(\omega_1, \omega_{-1}). \quad (4.14)$$

The leader selects $\omega_1^{\dagger}$ as his strategy and announces it to the followers. Subsequently, the followers have to react to the leader’s strategy by optimizing their objective functions $J_i(\omega_i^{\dagger}, \omega_i, \omega_{\{1,-i\}})$ for all $i \in \{2, 3, \ldots, M\}$ where $\omega_{\{1,-i\}}$ stands for the actions of all the players except the ones of the leader and Player $i$. The game among all the followers becomes an $(M - 1)$-player non-cooperative game described in the previous section. Let us give a two-player Stackelberg game as an illustrative example to show how the players determine their strategies in the following.
Example 10 (Smartphone Competition).

Companies A and B enter the smartphone market by introducing a new smartphone model with its pricing strategy. Company A is one of the technology giants while Company B is a startup. Thus, Company A has the power to set its pricing strategy first, knowing that Company B will base its pricing strategy on the leader’s decision.

Suppose that Company A moves first by setting a high price for its product. Company B is aware of the leader’s move before making its strategy. If Company B also sets a high price for its product, it might not sell a good number of smartphones due to its poorer reputation. However, if Company B sets a low price for its product, it captures a different portion of the market share and probably sells more products. On the other hand, suppose that Company A moves first by setting a low price for its product. The obvious strategy for Company B is lowering its price. Setting a high price makes the sales strategy challenging for Company B due to its poorer reputation. To offer readers a better reading experience, the components of this

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Players</strong></td>
<td>Company A and Company B</td>
</tr>
<tr>
<td><strong>Action Space</strong></td>
<td>Each company sets a high price or a low price for its new smartphone</td>
</tr>
<tr>
<td><strong>Game Payoff</strong></td>
<td>Payoff for each company given in Table 4.7</td>
</tr>
</tbody>
</table>
| **Information Structure** | Company A moves first and knows its effect on Company B’s decision  
Company B fully observes and reacts to Company A’s strategy |

<table>
<thead>
<tr>
<th>Company A</th>
<th>Company B</th>
<th>high price</th>
<th>low price</th>
</tr>
</thead>
<tbody>
<tr>
<td>high price</td>
<td>(6, 4)</td>
<td>(3, 7)</td>
<td></td>
</tr>
<tr>
<td>low price</td>
<td>(8, 2)</td>
<td>(5, 5)</td>
<td></td>
</tr>
</tbody>
</table>
competition are summarized in Table 4.6 while the game payoff matrix is given in Table 4.7.

To find the best strategy for Company A, it needs to address the optimization problem (4.13). From the game payoff matrix given Table 4.7, Company A will get the minimum payoff of 3 or 5 by setting a high price or a low price, respectively. Therefore, to obtain a better game payoff, Company A should go for the option of setting a low price for its product. After fully observing the leader’s decision, Company B will also get a payoff of 5, if it sets a low price for its new smartphone. In conclusion, both Companies set low prices for their products to obtain the Stackelberg equilibrium at (5, 5).
Chapter 5

Security Allocation

This chapter first describes a networked control system under stealthy FDI attacks with various modeling representations. We introduce the security allocation problem involving two strategic agents, namely a defender and a malicious adversary. The objectives of the two agents are modeled by the output-to-output gain security metric that represents the worst-case impact of stealthy FDI attacks. The security allocation problem is then tackled through game-theoretic frameworks. In the remainder of this chapter, we present the main contributions of the thesis.

5.1 Networked Control Systems under Stealthy FDI Attacks

Consider an undirected connected graph $G \triangleq (V, E, \tilde{A})$ consisting of $N$ vertices where each vertex $i$ has a state-space model:

$$\dot{x}_i(t) = A_i x_i(t) + b\tilde{u}_i(t), \quad (5.1)$$

$$y_i(t) = c^\top x_i(t), \quad (5.2)$$

where $x_i(t) \in \mathbb{R}^{n_x}$ is the state, $\tilde{u}_i(t) \in \mathbb{R}$ is the healthy/attacked input, $y_i(t) \in \mathbb{R}$ is the output of vertex $i$. This thesis will study two types of state-space models where the dimension of the state of each vertex $n_x$ is either one or two.

If the dimension of the state of each vertex $n_x$ is one, we have the following parameters:

$$A_i = 0, \quad b = 1, \quad c = 1. \quad (5.3)$$

On the other hand, if the dimension of the state of each vertex $n_x$ is two,
the following parameters are utilized:

\[
A_i = \begin{bmatrix} 0 & 1 \\ 0 & -h_i \end{bmatrix}, \quad b = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad c = \begin{bmatrix} 1 \\ 0 \end{bmatrix},
\]

where all the parameters \( h_i \in \mathbb{R}_+ \), \( \forall i \in \mathcal{V} \) are given.

Among all the vertices, a single vertex is selected to represent the local performance of the entire network (say performance vertex \( \rho \)). In more detail, the local performance of the entire network is evaluated via the output energy over a given time horizon of performance vertex \( \rho \in \mathcal{V} \) denoted as \( \|y_\rho\|_{\mathcal{L}_2}^2 \). Since the performance vertex \( \rho \) plays an important role in the network, it is reasonable to employ the following assumption.

**Assumption 1.** Communication channels of the performance vertex \( \rho \) are protected from any cyber attacks.

We assume that each vertex communicates with its own remote local controller through unprotected wireless communication channels, leaving control signals vulnerable to cyber attacks. If the communication channel of vertex \( i \) is not attacked, \( \tilde{u}_i(t) = u_i(t) \), in which \( u_i(t) \) is the healthy control signal. Otherwise, the control signal is manipulated by a malicious adversary, i.e., \( \tilde{u}_i(t) \neq u_i(t) \). For each healthy control input \( u_i(t) \), it can be formulated as a linear function of its state \( x_i(t) \) and their neighborhood states \( x_j(t), \forall j \in \mathcal{N}_i \), i.e., \( u_i(t) = \sum_{j \in \mathcal{N}_i} \phi_{ij}(x_i, x_j) \) where \( \phi_{ij}(\cdot) \) are linear functions for all \( i \in \mathcal{V} \). Although we employ several types of \( \phi_{ij}(\cdot) \) in this thesis (see Papers I-IV for more detail), most of those functions are designed to asymptotically stabilize the entire network, which allows us to introduce the following assumption.

**Assumption 2.** The system states \( x_i(t) \) for all \( i \in \mathcal{V} \) are at the origin before being attacked by malicious adversaries.

After the entire network is asymptotically stable at the origin, a malicious adversary might be present to choose a single attack vertex on which to conduct a stealthy FDI attack on its input with the aim of disrupting the local performance of the entire network. To counter such malicious activities, a defender needs to allocate the defense resources. Those actions will be discussed in the following section.

### 5.2 Defense and Attack Actions

We start this section by introducing how much the malicious adversary and the defender know about the network. Then, the actions of the defender and the malicious adversary are presented.
5.2. Defense and Attack Actions

**System knowledge:** The malicious adversary and the defender know all the parameters of the system, the vertex set \( V \), and the edge set \( E \). We assume that the malicious adversary knows the detection mechanism that will be utilized by the defender.

**Actions:** The defender allocates the defense resources by selecting a monitor set \( M \) containing several monitor vertices \( m_k \in M \) on which to monitor their outputs:

\[
y_M(t) = C_M^T x(t),
\]

where \( C_M = [e_{m_1}, e_{m_2}, \ldots, e_{m_{|M|}}] \).

On the other hand, according to Assumption 1, the malicious adversary selects a vertex \( a \in V_{-\rho} \) on which to conduct an additive time-dependent attack signal \( \zeta(t) \in \mathbb{R} \) on its control input as follows:

\[
\tilde{u}_i(t) = u_i(t) + \begin{cases} 0, & \text{if } i \in V_{-a}, \\ \zeta(t), & \text{if } i \equiv a. \end{cases}
\]

This control input (5.6) affords us to obtain the closed-loop system modeling as follows:

\[
x(t) = Ax(t) + b \otimes e_a \zeta(t),
\]

where \( x(t) = [x_1(t)^\top, x_2(t)^\top, \ldots, x_N(t)^\top]^\top \) represents the network state. Since the linear functions \( \phi_{ij}(\cdot) \) are designed to asymptotically stabilize the entire network, the matrix \( A \) is the function of \( A_i \) and \( \phi_{ij}(\cdot) \) such that \( A \) is Hurwitz, leading to \( \lim_{t \to \infty} x(t) = 0 \) in case of attack-free, i.e., \( \zeta(t) \equiv 0 \).

In the scope of this study, we mainly focus on stealthy FDI attacks conducted at the input of attack vertex \( a \) that will be defined in the following. Consider the structure of the following continuous LTI system \( \Sigma_{\rho,M} \triangleq (A, e_a, [e_\rho, C_M]^\top, 0) \), with the performance output \( y_\rho(t) = e_\rho^\top x(t) \) and the monitor outputs \( y_{m_k}(t) = e_{m_k}^\top x(t), \forall m_k \in M \). The attack input signal \( \zeta(t) \) of the system \( \Sigma_{\rho,M} \) is called stealthy FDI attacks if the monitor outputs satisfy \( \|y_{m_k}\|_{\mathcal{L}_2}^2 \leq \delta_{m_k}, \forall m_k \in M \), in which \( \delta_{m_k} > 0 \) is given for each corresponding monitor vertex \( m_k \) and called an alarm threshold. This definition of stealthy FDI attacks means that the adversary is said to be detected if there exists at least one monitor vertex \( m_k \in M \) whose output energy crosses its corresponding alarm threshold \( \delta_{m_k} \). Further, the impact of stealthy FDI attacks is measured via the energy of the performance vertex \( \rho \) over the horizon \([0, T]\), i.e., \( \|y_\rho\|_{\mathcal{L}_2[0,T]}^2 \). The worst-case impact of stealthy FDI attacks conducted by the malicious adversary on the local performance will be further investigated in the next section.
5.3 Worst-case Impact of Stealthy FDI Attacks

In the literature, several metrics have been utilized to formulate the worst-case impact of attacks on NCSs [113–122]. In the investigation of advanced persistent threats on cloud control systems, the authors in [113] utilized the cost functions, which represent defense plans and attack strategies, to formulate utility functions for the defender and the adversary. These game utility functions facilitate a comprehensive depiction of the level of dedication exerted by the defender and the adversary in their endeavors to counteract their respective opponents. Similar utility functions were developed to deal with DoS attacks in [114, 115] and sensor attacks in [116]. A different approach based on the Kullback-Leibler divergence was proposed in [117] to formulate utility functions for the adversary and the defender where the authors considered an NCS subjected to stochastic noises. In a more thorough manner, the defender finds strategies to maximize the Kullback-Leibler divergence between regular and attacked estimation errors while the adversary conducts the opposite way. However, an aspect that remains uncertain pertains in the aforementioned studies [113–117] to formulating the disruptive impact of the attack strategies on the dynamic system.

To meet the above shortfall, the disruptive impact on the system states has been taken into account in [118–120] where utility functions were indirectly adapted from the well-known linear-quadratic regulator problem. In more detail, the utility function for the adversary considers a trade-off for maximizing the energy of the system states and minimizing the energy of attack signals. Nonetheless, anomaly detectors, which are fundamental elements in NCSs, were overlooked in the above studies. The inclusion of anomaly detectors potentially poses a conundrum for the adversary’s endeavors in disrupting the network.

To close the gap in the above existing studies by incorporating anomaly detectors and considering the disruptive impact on dynamic systems simultaneously, several recent metrics based on $L_2$-gain were proposed to formulate the objectives of the defender and the malicious adversary in [114,121,122]. In more detail, the worst-case attack impact is composed of the maximum $L_2$-gains of multiple outputs, including a monitor output and a performance output, with respect to a single attack signal. More specifically, given performance vertex $\rho$, monitor vertex $m$, and attack vertex $a$, the following objective function is adapted from [121, Sec. 3]:

$$W_\rho(a, m) = \sup_{\|\zeta\|_{L_2} \neq 0} \frac{\|y_\rho\|_{L_2}^2}{\|\zeta\|_{L_2}^2} - \lambda \sup_{\|\zeta\|_{L_2} \neq 0} \frac{\|y_m\|_{L_2}^2}{\|\zeta\|_{L_2}^2}, (\lambda \geq 0).$$

The above objective $W_\rho(a, m)$ also considers two different outputs $y_\rho(t)$ and $y_m(t)$, but note that the output energies are maximized separately, leading to
5.3. Worst-case Impact of Stealthy FDI Attacks

two different optimal input signals $\zeta(t)$ in general cases. Thus, the objective function $W(a, m)$ possibly results in pessimistic worst-case attack impacts that cannot be attained by any admissible input signal. Moreover, the use of a maximum $L_2$-gain for characterizing the detectability corresponds to an optimistic perspective, where the adversary attempts to maximize the energy of the detection output, instead of the opposite.

To deal with the aforementioned critical issue of formulating security metrics against stealthy FDI attacks, this thesis mainly adopts the output-to-output gain security metric, which was first proposed in [123] and then recently developed in [124], to formulate the worst-case impact of stealthy FDI attacks. This metric is designed based on the well-established $H_\infty$ framework for the robustness and the $H_\infty$ index dedicated for the detectability [125]. Thus, this metric allows us to fully explore the worst-case attack impact for multiple outputs with respect to a single input.

In more detail, given a fixed performance vertex $\rho$, the adversary selects an attack vertex $a \in V_{-\rho}$ while the defender selects a set of monitor vertices $M$. The worst-case impact of stealthy FDI attacks on the fixed performance vertex $\rho$ is formulated as follows:

$$J_\rho(a, M) = \sup_{\zeta \in L_{2e}, \; x(0) = 0} \|y_\rho\|_{L_2}^2$$

s.t. $\|y_{m_k}\|_{L_2}^2 \leq \delta_{m_k}, \; \forall m_k \in M$. 

The dual problem of (5.8) is given as follows:

$$\inf_{\gamma_{m_k} > 0} \left[ \sup_{\zeta \in L_{2e}, \; x(0) = 0} \left( \|y_\rho\|_{L_2}^2 - \sum_{m_k \in M} \gamma_{m_k} \|y_{m_k}\|_{L_2}^2 \right) + \sum_{m_k \in M} \gamma_{m_k} \delta_{m_k} \right].$$

The dual problem (5.9) is bounded only if $\|y_\rho\|_{L_2}^2 - \sum_{m_k \in M} \gamma_{m_k} \|y_{m_k}\|_{L_2}^2 \leq 0, \; \forall \zeta \in L_{2e}$ and $x(0) = 0$, which results in the following minimization problem:

$$J_\rho(a, M) = \min_{\gamma_{m_k} > 0} \sum_{m_k \in M} \gamma_{m_k} \delta_{m_k}$$

s.t. $\|y_\rho\|_{L_2}^2 - \sum_{m_k \in M} \gamma_{m_k} \|y_{m_k}\|_{L_2}^2 \leq 0, \; \forall \zeta \in L_{2e}, x(0) = 0.$

The strong duality can be proven by utilizing S-Procedure [126, Ch .4]. Recalling the key results in dissipative system theory for linear systems with quadratic supply rates [127], the constraint of (5.10) can be translated
into a linear matrix inequality [124, Prop. 1] as follows:

\[
J_\rho(a, M) = \min_{\gamma_{mk} > 0, \, P \succcurlyeq P^T \succeq 0} \sum_{m_k \in M} \gamma_{mk} \delta_{mk}
\]

\[
s.t. \begin{bmatrix}
AP + PA & P(b \otimes e_a) \\
(b \otimes e_a)^T P & 0
\end{bmatrix} + \begin{bmatrix}
c \otimes e_\rho \\
0
\end{bmatrix} \begin{bmatrix}
(c \otimes e_\rho)^T & 0
\end{bmatrix} \leq 0.
\]

To guarantee the existence of a solution to the optimization problem (5.11), we need to show the feasibility of the optimization problem (5.8). This feasibility, undoubtedly, hinges upon the system modeling, which has been explicated across various applications within the included papers. The main contributions of the thesis are to provide several system- and graph-theoretic conditions tailored to those applications under which the feasibility of the optimization problem (5.8) is guaranteed. This feasibility assists the defender in dealing with the following security allocation problem.

**Problem 1** (Security allocation). The defender is required to select an optimal monitor set \( M \) that minimizes the worst-case impact of stealthy FDI attacks conducted by the malicious adversary.

To outline the system- and graph-theoretic conditions, as the main contributions of the thesis, in Section 5.5, let us invoke the following formal representations.

**Definition 1** (Invariant zeros). Consider the strictly proper system \( \Sigma \triangleq (\bar{A}, \bar{B}, \bar{C}, 0) \) where \( \bar{A}, \bar{B}, \) and \( \bar{C} \) are real matrices with appropriate dimensions. A tuple \((\bar{\lambda}, \bar{x}, \bar{g})\) \( \in \mathbb{C} \times \mathbb{C}^N \times \mathbb{C} \) is a zero dynamics of \( \bar{\Sigma} \) if it satisfies

\[
\begin{bmatrix}
\bar{\lambda} I - \bar{A} & -\bar{B} \\
\bar{C} & 0
\end{bmatrix}
\begin{bmatrix}
\bar{x} \\
\bar{g}
\end{bmatrix} = \begin{bmatrix}
0 \\
0
\end{bmatrix}, \quad \bar{x} \neq 0.
\]

In this case, a finite \( \bar{\lambda} \) is called a finite invariant zero of the system \( \bar{\Sigma} \). Further, the strictly proper system \( \bar{\Sigma} \) always has at least one invariant zero at infinity [128, Ch. 3].

**Definition 2** (Relative degree [35, Ch. 13]). Consider the strictly proper system \( \tilde{\Sigma} \triangleq (\tilde{A}, \tilde{B}, \tilde{C}, 0) \) with \( \tilde{A} \in \mathbb{R}^{n \times n}, \tilde{B}, \) and \( \tilde{C} \) are real matrices with appropriate dimensions. The system \( \tilde{\Sigma} \) is said to have relative degree \( r \) \( (1 \leq r \leq n) \) if the following conditions satisfy

\[
\tilde{C} \tilde{A}^k \tilde{B} = 0, \quad 0 \leq k < r - 1,
\]

\[
\tilde{C} \tilde{A}^{r-1} \tilde{B} \neq 0.
\]
Lemma 1 ([123, Th. 2]). Suppose that the monitor set $M$ contains only one element (say vertex $m$). Consider the following continuous LTI systems $\Sigma_\rho \triangleq (A, e_\rho, e_\rho^T, 0)$ and $\Sigma_m \triangleq (A, e_m, e_m^T, 0)$ in which the two systems have the same stealthy attack input at vertex $a$ but different output vertices, i.e., $\rho$ for $\Sigma_\rho$ and $m$ for $\Sigma_m$. The worst-case impact (5.8) is bounded if, and only if, unstable invariant zeros of $\Sigma_m$ are also unstable invariant zeros of $\Sigma_\rho$. 

5.4 Game-theoretic Framework for Security Allocation

The non-cooperative game described in Chapter 4 is applied to deal with the security allocation problem in a networked control system under stealthy FDI attacks, as depicted in Figure 1.5. Due to resource constraints, the malicious adversary selects one vertex on which to conduct stealthy FDI attacks on its input. Meanwhile, the defender selects one or several vertices on which to monitor their outputs with the purpose of alleviating the worst-case attack impact. To fit the game-theoretic framework introduced in the previous chapter, the components of the game are presented with further elaboration in the following.

The two players in the game are the defender (with $m$ possible actions) and the malicious adversary (with $n$ possible actions). The competition between the defender and the malicious adversary is a one-shot game where the two players make their decisions once. Henceforth, the security game between one defender and one malicious adversary is shortened as the security game if it is clear from the context.

A core element of the game is the game payoff matrices, which are denoted as $m \times n$-dimensional real-valued matrices $J^d = [J^d_{ij}]$ and $J^a = [J^a_{ij}]$ for the defender and the malicious adversary, respectively. Based on those payoffs, if the gain of the malicious adversary is exactly the same as the loss of the defender and vice versa, this competition is a zero-sum game. Otherwise, this competition is a non-zero-sum game. In this thesis, the former is considered in Papers I-III while the latter is considered in Paper IV. If the defender selects the $i$-th row and the adversary selects the $j$-th column, then the tuple $(J^d_{ij}, J^a_{ij})$ is the outcome of the game in which $J^d_{ij}$ and $J^a_{ij}$ represent the cost of the defense strategy and the worst-case attack impact, respectively. Thus, the defender desires to select an action such that it minimizes the cost $J^d_{ij}$, while the malicious adversary wants to make an attack policy such that it maximizes the worst-case attack impact $J^a_{ij}$.

The information structure of the two-player games is considered in two different cases. In the first case, the players make their decisions simultaneously without knowing the true action of the opponent. This case is
Table 5.1: Components of the security game between a defender and a malicious adversary.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Players</td>
<td>Defender and Adversary</td>
</tr>
<tr>
<td>Action Space</td>
<td>Defender chooses one in ( m ) rows</td>
</tr>
<tr>
<td></td>
<td>Adversary chooses one in ( n ) columns</td>
</tr>
<tr>
<td>Game Payoff</td>
<td>( m \times n )-dimensional matrix ( J^d ) for Defender</td>
</tr>
<tr>
<td></td>
<td>( m \times n )-dimensional matrix ( J^a ) for Adversary</td>
</tr>
<tr>
<td>Information Structure in Papers I-III</td>
<td>Players take action simultaneously</td>
</tr>
<tr>
<td>Information Structure in Paper IV</td>
<td>Defender takes action first</td>
</tr>
<tr>
<td></td>
<td>Adversary fully observes Defender’s action</td>
</tr>
</tbody>
</table>

considered in Papers I-III. The other case is a Stackelberg game where the defender has the power to take action first, with knowing that the malicious adversary bases their action on the defender’s decision. Then, after fully observing the defender’s action, the malicious adversary makes their best response to the defender’s action. This Stackelberg game, where the defender acts as the leader and the malicious adversary acts as the follower, is considered in Paper IV. To facilitate readers in attaining a clear understanding, we summarize the components of the security game in Table. 5.1. Papers I-IV included in this thesis present how the defender and the malicious adversary determine their optimal actions in the competition game.

5.5 Contributions of the Thesis

Among those papers included in this thesis, the system modeling of each vertex is described slightly differently from linear first-order systems with certain system parameters (Papers I and IV) over linear first-order systems with uncertain system parameters (Paper II) to second-order systems with certain system parameters (Paper III). Due to different system modelings, although the monitor outputs and the performance output are formulated differently, the worst-case impact of stealthy FDI attacks is always formulated based on the output-to-output gain security metric introduced in Section 5.3. Then, the contributions of the included papers are made to guarantee the boundedness of the worst-case impact of stealthy FDI attacks (5.8), which enables the defender to deal with Problem 1.
5.5. Contributions of the Thesis

Paper I

At the initial stage of this thesis, Paper I delves into the investigation of an NCS under attacks in which the system consists of linear first-order vertices with certain system parameters to address the security allocation problem. The scenario of the paper allows the defender to select one monitor vertex, i.e., $\mathcal{M} = \{m \mid m \in \mathcal{V}\}$. After formulating the worst-case impact of stealthy FDI attacks based on the output-to-output gain as described in (5.8), the paper discovers the connection between the boundedness of this impact (5.8) and the relative degrees (see Definition 2) of respective systems $\Sigma_\rho$ and $\Sigma_m$, which are defined in Lemma 1. This connection results in a necessary and sufficient condition for the relative degrees of those respective systems under which the boundedness of the worst-case impact of stealthy FDI attacks (5.8) is guaranteed. To offer a more intricate explanation, if, and only if, the relative degree of $\Sigma_m$ is not greater than that of $\Sigma_\rho$, the worst-case impact (5.8) is finite regardless of the location of an attack vertex. This boundedness plays a crucial role in making defense strategies where it enables the defender to restrict his action space into admissible actions that fulfill the above necessary and sufficient condition. Further, given the adjacency matrix $\bar{A}$ representing the network, monitor vertex $m$, and performance vertex $\rho$, the paper also indicates that if the monitor vertex $m$ fulfills the following algebraic sufficient condition $e_\rho^\top \bar{A}(I + \bar{A})e_m = e_\rho^\top \bar{A}^2 e_\rho$, it is admissible. Finally, the security allocation problem is solved through a zero-sum game-theoretic framework.

Paper II

This paper extends the security allocation problem raised in Paper I by introducing uncertain system parameters. The system parameter $A$ in (5.7) becomes $A \triangleq \bar{A} + \Delta$ where $\bar{A}$ is the nominal value and $\Delta$ is uncertainty. The defender and the malicious adversary only know partial information, including nominal value $\bar{A}$ and uncertainty set $\Omega$, which covers all the possibilities of uncertainty $\Delta$, i.e., $\Delta \in \Omega$. Due to this uncertainty problem, formulating the worst-case impact of stealthy FDI attacks is more challenging. To deal with such an issue, a well-established risk metric, called Value-at-Risk, is adopted to describe the worst-case risk of stealthy FDI attacks. This metric allows us to evaluate the worst-case risk with sampled values of the uncertain set $\Omega$. Recall the system $\Sigma_m$ in Lemma 1, the paper proposes a control design scheme for local controllers that guarantees $\Sigma_m$ having no unstable invariant zero. Subsequently, we propose a sufficient condition under which the boundedness of such a worst-case risk is guaranteed, leading to the admissible actions of the defender. Finally, the security allocation problem is
Chapter 5. Security Allocation

dealt with by solving the pure and mixed-strategy Nash equilibria.

The following two papers broaden the conceptual framework of this thesis by extending the security allocation problem in two ways. More extensively, Paper III considers more complicated system modelings that better suit real-world applications. This is challenging to the analysis of the worst-case impact of stealthy FDI attacks. Meanwhile, Paper IV relaxes the assumption about the certain location of the performance vertex by keeping it secret from the malicious adversary. This relaxation requires the defender to find a more comprehensive way to characterize admissible actions instead of the one proposed in Paper I.

Paper III

While the previous papers consider the security allocation problem in NCSs consisting of interconnected linear first-order vertices, this paper contributes to extending the vision of this thesis by studying interconnected linear second-order vertices with certain system parameters. Due to the different modeling descriptions, control laws designed in the previous papers are no longer able to handle unstable invariant zeros of $\Sigma_m$, possibly leading to infinite attack impacts. To overcome such an issue, Paper III proposes a control design to fulfill the performance requirement of the entire network. Given a certain assumption, this control law also assists us in providing a sufficient condition under which the defender ensures that the worst-case impact of stealthy FDI attacks is bounded. This condition enables the defender to identify their admissible actions. After casting the security problem between the defender and the malicious adversary in a zero-sum game framework, the paper presents an algorithm to seek the best actions of the two strategic agents through the concept of the deterministic and mixed-strategy Nash equilibria. Finally, the effectiveness of the proposed security allocation scheme is demonstrated through the IEEE 14-bus system.

Paper IV

The previous papers address the security allocation problem wherein both the defender and the malicious adversary evaluate the worst-case impact of stealthy FDI attacks through assuming a certain location of the local performance. Since the local performance of the entire network is vital, it should
5.5. Contributions of the Thesis

not be revealed publicly. Hence, Paper IV extends the security allocation problem in Paper I by relaxing the assumption on the certain location of the local performance. Given a monitor set $\mathcal{M}$ and an attack vertex $a$, this relaxation requires the defender and the malicious adversary to evaluate the expected worst-case impact of stealthy FDI attacks formulated by $Q(a, \mathcal{M}) \triangleq \sum_{\rho \in \mathcal{V}_{-a}} \pi(\rho|a)J_\rho(a, \mathcal{M})$ where $J_\rho(a, \mathcal{M})$ is the worst-case impact of stealthy FDI attacks (5.8) and $\pi(\rho|a)$ represents the belief in the location of the local performance $\rho$. Toward an analysis of the expected worst-case impact $Q(a, \mathcal{M})$, we need to investigate all the worst-case impacts $J_\rho(a, \mathcal{M})$ for all $\rho \in \mathcal{V}$. To this end, we provide an upper bound for the worst-case attack impact $J_\rho(a, \mathcal{M})$ by considering single monitor vertices separately, i.e., $J_\rho(a, \mathcal{M}) \leq \min_{m_k \in \mathcal{M}} J_\rho(a, m_k)$. This upper bound is guaranteed to be finite through a proposed necessary and sufficient condition for the relative degrees of $\Sigma_m$ and $\Sigma_\rho$, which are defined in Lemma 1, connecting to the key result in Paper I. This condition enables the defender to restrict their admissible actions to a subset of available vertices, called dominating sets. After the action space of the defender is characterized as dominating sets, the security allocation problem is addressed through a game-theoretic framework. While the previous papers let the defender and the malicious adversary decide their actions simultaneously, Paper IV empowers the defender by letting the defender make their decision first, knowing that the malicious adversary bases their action on the defender’s decision. After observing the defender’s action, the malicious adversary selects the best response to maximize the expected worst-case attack impact. Then, we cast the security allocation problem in a Stackelberg game-theoretic framework where the defender acts as the leader and the adversary acts as the follower of the game. An algorithm is presented to seek the Stackelberg optimal action that yields the best actions of the defender and the malicious adversary. Finally, the contributions of Paper IV are highlighted in terms of computational complexity by applying the proposed security allocation scheme in the context of very large-scale networks.
Chapter 6

Concluding Remarks

6.1 Conclusion

In this comprehensive summary, we have considered various aspects of networked control systems under cyber attacks. There are numerous ways for malicious adversaries to launch cyber attacks on systems such as replay attacks, DoS attacks, eavesdropping attacks, and FDI attacks. However, we mainly focused on stealthy FDI attacks since the malicious adversaries are able to delve into system knowledge to manage their stealthiness, enabling them to cause catastrophic consequences without being detected. Given the potent capabilities of these adversaries, this thesis investigated the worst-case impact of stealthy FDI attacks where the adversary maximizes their malicious impact and remains stealthy simultaneously. The investigation provided several crucial system- and graph-theoretic conditions for the defender, enabling him to bound the worst-case impact of stealthy FDI attacks. Subsequently, under those conditions, the solution to the security allocation problem in terms of minimally alleviating the worst-case impact of stealthy FDI attacks was found through the game-theoretic frameworks.

6.2 Future Work

The view on the worst-case impact of stealthy FDI attacks through the lens of the output-to-output gain security metric still opens the door to many promising research topics. Here, we outline several intriguing topics that have captured our attention:

Should our hypothesized adversaries be granted increased power? To be more realistic, we might allow adversaries to select more vertices on which to conduct a coordinated stealthy FDI attack. Given multiple attack vertices, if we assume that the maximum number of attack vertices is not more than
that of monitor vertices, the results in Paper IV can be extended. Therefore, we would scale up the scope of this thesis to a multiple-adversary-multiple-defender game in networked control systems.

The idea of characterizing admissible monitor sets as dominating sets, as presented in Paper IV, holds great promise for future investigation. By combining the algebraic testing condition of dominating sets with the output-to-output gain security metric, we can formulate a unified convex optimization problem. Solving this problem would yield an optimal defense strategy applicable to arbitrary networks.

The problem of optimal detector placement, as explored in Paper III, can be extended to incorporate the defender’s ability to adjust detector gains after selecting detection vertices. This adjustment mechanism has the potential to effectively reduce the worst-case impact of stealthy FDI attacks, resulting in a more efficient defense strategy. The selection and adjustment of detection vertices can be elegantly addressed through solving convex optimization problems.

The assumption regarding the information structure, where defenders and malicious adversaries possess knowledge of their competitors, can be relaxed. The relaxation opens up possibilities where they might deal with several types of their competitors, resulting in Bayesian game settings [129]. Dealing with the problem of optimal sensor placement in Bayesian games would be a promising avenue for future exploration.

By studying new security problems, including but not limited to the ones mentioned above, we aim to advance the field and contribute to the growing body of knowledge on networked control systems under cyber attacks. Through our anticipated rigorous investigation and innovative methodologies, we strive to enhance the security and resilience of control systems in the face of sophisticated adversaries.
References


72 References


[85] K. Teranishi, T. Sadamoto, and K. Kogiso, “Input-output history feed-
back controller for encrypted control with leveled fully homomorphic

observer-based control for linear continuous-time systems,” arXiv

[87] B. T. Nguyen, T. X. Nghiem, L. Nguyen, T. T. Nguyen, and
T. Nguyen, “Secure-and privacy-preserving policies for cooperative
control of multiple vehicle systems,” in Autonomous Systems: Sensors,
Processing and Security for Ground, Air, Sea, and Space Vehicles and

“Encrypting controller using fully homomorphic encryption for secu-
ritry of cyber-physical systems,” IFAC-PapersOnLine, vol. 49, no. 22,

control based on structured feedback,” IEEE control systems letters,

[90] C. Murguia, F. Farokhi, and I. Shames, “Secure and private implement-
ation of dynamic controllers using semihomomorphic encryption,”
IEEE Transactions on Automatic Control, vol. 65, no. 9, pp. 3950–

[91] J. Kim, H. Shim, and K. Han, “Dynamic controller that operates
over homomorphically encrypted data for infinite time horizon,” IEEE
Transactions on Automatic Control, 2022.

attack-detection techniques,” IEEE Internet computing, vol. 10, no. 1,

[93] S. Amin, A. A. Cárdenas, and S. S. Sastry, “Safe and secure net-
worked control systems under denial-of-service attacks,” in Hybrid
Systems: Computation and Control: 12th International Conference,


Title
A Single-Adversary-Single-Detector Zero-Sum Game in Networked Control Systems

Authors
Anh Tung Nguyen, André M. H. Teixeira, and Alexander Medvedev

Edited version of
Anh Tung Nguyen, André M. H. Teixeira, and Alexander Medvedev
A Single-Adversary-Single-Detector Zero-Sum Game in Networked Control Systems

Abstract
This paper proposes a game-theoretic approach to address the problem of optimal sensor placement for detecting cyber-attacks in networked control systems. The problem is formulated as a zero-sum game with two players, namely a malicious adversary and a detector. Given a protected target vertex, the detector places a sensor at a single vertex to monitor the system and detect the presence of the adversary. On the other hand, the adversary selects a single vertex through which to conduct a cyber-attack that maximally disrupts the target vertex while remaining undetected by the detector. As our first contribution, for a given pair of attack and monitor vertices and a known target vertex, the game payoff function is defined as the output-to-output gain of the respective system. Then, the paper characterizes the set of feasible actions by the detector that ensures bounded values of the game payoff. Finally, an algebraic sufficient condition is proposed to examine whether a given vertex belongs to the set of feasible monitor vertices. The optimal sensor placement is then determined by computing the mixed-strategy Nash equilibrium of the zero-sum game through linear programming. The approach is illustrated via a numerical example of a 10-vertex networked control system with a given target vertex.

1 Introduction

The notion of networked control systems has gained popularity in the modeling and analysis of real-world large-scale interconnected systems such as power systems, transportation networks, and water distribution networks. Networked control systems, generally employing non-proprietary and pervasive communication and information technology, such as the Internet
Figure I.1: Visualisation of a single-adversary-single-detection zero-sum game in a networked control system.

and wireless communications, may leave the systems vulnerable to cyber-attacks [15] and inflict significant financial and societal costs. Reports on Stuxnet [56], for example, have shown the devastating consequences of this malicious software attack on the nuclear program of Iran. Motivated by the above observations, cyber-physical security has become an increasingly important aspect of control systems in recent years.

This study considers a continuous-time networked control system under attack with two strategic agents: a malicious adversary and a detector. The system consists of multiple one-dimensional subsystems, so-called vertices, in which there exists a single protected target vertex. The purpose of the adversary is to affect the output of the target vertex without being detected. To this end, the adversary chooses one vertex to attack and directly injects attack signals into its input. Meanwhile, the detector chooses one monitor vertex and measures its output, with the aim of unmasking the presence of the adversary. Assuming both agents to be strategic, we investigate the optimal selection of the monitor vertex through a game-theoretic approach. Fig. I.1 visualizes the above-defined game in a networked control system. The game-theoretic approach has been successfully applied to tackle the problem of robustness, security, and resilience of cyber-physical systems [112]. It allows us to deal with the robustness and security of cyber-physical systems within the common well-defined framework of $H_\infty$ robust control design. Further, many other concepts of games describing networked systems subjected to cyber-attacks such as dynamic games [130] and stochastic games [131] have been recently studied.

Although the above games were successful in studying control systems
subjected to cyber-attacks such as denial-of-service attacks, changing the
locations of detectors to increase the detection of such cyber-attacks was
not considered. To address this gap, [121] consider a game-theoretic for-
mulation where the defender chooses the location of sensors in a networked
system, to protect against an adversary that aims at maximally disrupting
the system while remaining undetected. The game payoff in [121] has been
formulated by combining the maximum $L_2$ gains of multiple outputs w.r.t.
a single input representing the attack signal. On the one hand, these multi-
ple $L_2$ gains are evaluated separately and thus may be attained for different
optimal input signals, possibly resulting in pessimistic payoffs that cannot
be attained by any admissible input signal. On the other hand, the use of a
maximum gain for characterizing detectability corresponds to an optimistic
perspective, where the adversary attempts to maximize the energy of the
detection output, instead of the opposite.

In this paper, we consider a game-theoretic approach that is inspired
and related to the one in [121]. However, to address the above-mentioned
limitations, we invoke the output-to-output gain (OOG) proposed in [123,
124] as the game payoff for the adversary and the detector. This game
payoff affords us to fully explore the cyber-attack impact on the monitor
and the target outputs simultaneously with a single input signal. As our
main contributions, we cast the optimal selection of a monitor vertex as
a zero-sum game and investigate the existence of a set of feasible monitor
vertices that, if selected, result in a bounded game-payoff. We show that
the existence of such a set is related to the system-theoretic properties of the
underlying dynamical system, namely its relative degrees. Then, we propose
an algebraic condition to characterize the set of feasible monitor vertices that
guarantee a bounded game payoff for any attack vertex. Finally, a numerical
element is given to demonstrate the effectiveness of the proposed approach.
Further, a mixed-strategy Nash equilibrium of the game is also investigated
in a simulation example.

We conclude this section by providing the notation to be used throughout
this paper. The problem formulation is introduced in Section 2. Thereafter,
Section 3 investigates and characterizes the set of feasible monitor vertices
through the system-theoretic properties of the system. Section 4 presents
a numerical example of the zero-sum game between an adversary and a
detector and computes the optimal monitor selection based on a mixed-
strategy Nash equilibrium. Section 5 concludes the paper.

**Notation:** the set of real positive numbers is denoted as $\mathbb{R}_+$; $\mathbb{R}^n$ and
$\mathbb{R}^{n \times m}$ stand for sets of real $n$-dimensional vectors and $n$-row $m$-column ma-
trices, respectively. Let us define $e_i \in \mathbb{R}^n$ with all zero elements except
the $i$-th element is set as 1. A continuous-time system with the state-
space model $\dot{x}(t) = Ax(t) + Bu(t)$, $y(t) = Cx(t) + Du(t)$ is denoted as
\[ \Sigma \triangleq (A, B, C, D) \]. Consider the norm \( \|x\|_{L_2[0,T]}^2 \triangleq \int_0^T \|x(t)\|_2^2 \, dt \). The space of square-integrable functions is defined as \( L^2_{2} \triangleq \{ f : \mathbb{R}^+ \to \mathbb{R} \mid \|f\|_{L_2[0,\infty]} < \infty \} \) and the extended space be defined as \( L^2_{2e} \triangleq \{ f : \mathbb{R}^+ \to \mathbb{R} \mid \|f\|_{L_2[0,T]} < \infty, \, \forall \, 0 < T < \infty \} \). Let \( G \triangleq (V, E, A) \) be a digraph with the set of \( N \) vertices \( V = \{v_1, v_2, \ldots, v_N\} \), the set of edges \( E \subseteq V \times V \), and the adjacency matrix \( A = [a_{ij}] \). For any \((v_i, v_j) \in E, \, i \neq j\), the element of the adjacency matrix \( a_{ij} \) is positive, and with \((v_i, v_j) \notin E \) or \( i = j, \, a_{ij} = 0 \). The degree of vertex \( v_i \) is denoted as \( d_i = \sum_{j=1}^{n} a_{ij} \) and the degree matrix of graph \( G \) is defined as \( D = \text{diag}(d_1, d_2, \ldots, d_N) \), where \( \text{diag} \) stands for a diagonal matrix. The Laplacian matrix is defined as \( L = [\ell_{ij}] = D - A \). Further, \( G \) is called an undirected graph if \( A \) is symmetric. An edge of an undirected graph \( G \) is denoted by a pair \((v_i, v_j) \in E \). An undirected graph is connected if for any pair of vertices there exists at least one path between two vertices. The set of all neighbours of vertex \( v_i \) is denoted as \( \mathcal{N}_i = \{v_j \in V \mid (v_i, v_j) \in E\} \).

2 Problem Formulation

This section consists of three subsections. Firstly, the networked control system in the presence of a cyber-attack is defined. Then, we introduce the optimal stealthy data injection attack which will be studied throughout the paper. The last subsection describes our game-theoretic approach to selecting feasible monitor vertices.

2.1 Networked Control System under Attacks

Consider a connected undirected network \( G \triangleq (V, E, A) \) with \( N \) vertices, the state-space model of a one-dimensional vertex \( v_i \) is described:

\[ \dot{x}_i(t) = u_i(t), \quad i \in \{1, 2, \ldots, N\}, \quad (I.1) \]

where \( x_i(t) \in \mathbb{R} \) is the state of vertex \( v_i \). Due to the fact that states of all the vertices are not always available, we employ the widely-used displacement-based control law for networked control systems:

\[ u_i(t) = \sum_{v_j \in \mathcal{N}_i} (x_j(t) - x_i(t)). \quad (I.2) \]

For convenience, let us denote \( x(t) \) as the state of the networked control system, \( x(t) = [x_1(t), x_2(t), \ldots, x_N(t)]^\top \). In our setup, the adversary conducts time-dependent malicious action \( a(t) \in \mathbb{R} \) at the input of vertex \( v_a \):

\[ u_a(t) = \sum_{v_j \in \mathcal{N}_a} (x_j(t) - x_a(t)) + a(t). \quad (I.3) \]
The purpose of the adversary is to manipulate the output of a given target vertex \( v_\tau \). On the other hand, the detector places a sensor at the output of vertex \( v_m \) to monitor attack signals. The system model (I.1) under the control law (I.2) can be rewritten in the presence of attack signals at the vertex \( v_a \) (I.3) with two outputs observed at the two vertices \( v_\tau \) and \( v_m \):

\[
\dot{x}(t) = -Lx(t) + e_a a(t), \quad (I.4)
\]

\[
y_\tau(t) = e_\tau^T x(t), \quad (I.5)
\]

\[
y_m(t) = e_m^T x(t). \quad (I.6)
\]

In the scope of this study, we mainly focus on the stealthy data injection attack. This attack will be defined as follows. Consider the above structure of the continuous-time system (I.4)-(I.6), which we denote as \( \Sigma_{\tau,m} \triangleq (-L, e_a, [e_\tau, e_m]^T, 0) \), with target output \( y_\tau(t) = e_\tau^T x(t) \) and monitor output \( y_m(t) = e_m^T x(t) \). The input signal \( a(t) \) of the system \( \Sigma_{\tau,m} \) is called the stealthy data injection attack if the monitor output satisfies \( \|y_m\|_2^2 \leq \delta \), in which \( \delta > 0 \) is called an alarm threshold. Further, the impact of the stealthy data injection attack is measured via the energy of the target output over the horizon \( [0,T] \), i.e., \( \|y_\tau\|_{L_2[0,T]}^2 \). Without loss of generality, let us set the alarm threshold \( \delta = 1 \) in the remainder of this study.

The worst-case impact of the stealthy data injection attack will be further investigated in the next subsection.

### 2.2 Optimal Stealthy Data Injection Attack

The adversary attacks vertex \( v_a \) with the objective of maximizing impact on the output of the target vertex \( v_\tau \) while remaining undetected at the monitor vertex \( v_m \), which can be formulated as the following non-convex optimal control problem [124]:

\[
J_\tau(v_a, v_m) \triangleq \sup_{a \in L_{2e}} \|y_\tau\|_{L_2}^2 \quad \text{s.t.} \quad \|y_m\|_{L_2}^2 \leq 1. \quad (I.7)
\]

Following the details in [124], the above optimal control problem can be equivalently rewritten as the following optimization problem

\[
J_\tau(v_a, v_m) \triangleq \min_{\gamma \in \mathbb{R}_+} \gamma \quad \text{s.t.} \quad \|y_\tau\|_{L_2}^2 \leq \gamma \|y_m\|_{L_2}^2, \quad \forall a \in L_{2e},
\]

\[
x(0) = 0,
\]

where the constraint may in turn be replaced with a convex Linear Matrix Inequality ( [124, Ch. 6.4] and references therein), yielding a convex optimization problem that computes \( J_\tau(v_a, v_m) \).
Remark 1. With a similar scenario, another objective function based on $L_2$-gain for the adversary and the detector has been proposed in [121, Sec. 3]. The objective function in [121] was formulated in terms of the maximal $L_2$-gains from the attack to the target vertices and from the attack to monitor vertices. More specifically, the objective function in [121] is given by

$$G_r(v_a, v_m) = \sup_{a \neq 0} \frac{\|y_r\|_{L_2}^2}{\|a\|_{L_2}} - \lambda \sup_{a \neq 0} \frac{\|y_m\|_{L_2}^2}{\|a\|_{L_2}}, \quad (\lambda \geq 0).$$

The above objective in [121] also considers two different outputs $y_r(t)$ and $y_m(t)$, but note that the output energies are maximized separately, thus leading to two different optimal input signals $a(t)$ in the general case. By contrast, our objective function (I.8) investigates the worst-case attack impact that is simultaneously characterized by the two outputs $y_r(t)$ and $y_m(t)$ w.r.t. a single input signal $a(t)$.

Next, we tackle the problem of the optimal selection of a monitor vertex through a game-theoretic approach.

2.3 Game-theoretic Approach to Monitor Vertex Selection

To defend against adversaries, we consider that the detector tackles the following problem.

Problem 1. (Optimal monitor selection) Given a target vertex and an arbitrary attack vertex, select a monitor vertex that minimizes the worst-case impact of the stealthy data injection attack at the attack vertex.

As the attack vertex is arbitrary, we formulate Problem 1 as a game between the detector and adversary, where the players choose $v_a$ and $v_m$ to respectively maximize and minimize the function $J_r(v_a, v_m)$ described in (I.8). Hence, Problem 1 is formalized as a zero-sum game with $J_r(v_a, v_m)$ as the game-payoff, namely

$$\min_{v_m \neq v_r \in V} \max_{v_a \neq v_r \in V} J_r(v_a, v_m).$$

(I.9)

While Problem 1 investigates an optimal selection of the monitor vertex, there is no a priori guarantee that a suitable monitor vertex exists for which (I.9) is bounded from above. The following problem raises a question of finding feasible monitor vertices such that the worst-case impact of the stealthy data injection attack is bounded.

Problem 2. (Feasible monitor vertices) Given a target vertex and an arbitrary attack vertex, find a set of feasible monitor vertices such that the worst-case impact of the stealthy data injection attack is bounded.
Formally, a set of feasible monitor vertices w.r.t. the target vertex $v_\tau$ is defined as $\mathcal{M}_\tau \triangleq \{v_m \neq v_\tau \in \mathcal{V} \mid \max_{v_a \neq v_\tau \in \mathcal{V}} J_\tau(v_a, v_m) < \infty\}$.

By definition, if $\mathcal{M}_\tau \neq \emptyset$, the detector may select a vertex $v_m \in \mathcal{M}_\tau$ to ensure that (I.8) is feasible for any attack vertex, which in turn guarantees that the zero-sum game (I.9) admits a bounded value. Furthermore, characterizing the set $\mathcal{M}_\tau$ allows us to restrict the possible choices of the detector to $\mathcal{M}_\tau$. Hence, by addressing Problem 2 and characterizing $\mathcal{M}_\tau$, we can tackle Problem 1 by reformulating the zero-sum game (I.9) as

$$
\min_{v_m \neq v_\tau \in \mathcal{V}} \max_{v_a \neq v_\tau \in \mathcal{V}} J_\tau(v_a, v_m) \tag{I.10}
$$

s.t. $v_m \in \mathcal{M}_\tau$.

The next section characterizes the set of feasible monitor vertices $\mathcal{M}_\tau$ by investigating the feasibility of (I.8) with respect to system-theoretic properties of the dynamical system (I.4)-(I.6).

3 Characterization of Feasible Monitor Vertices

Let us denote the continuous-time systems $\Sigma_\tau \triangleq (-L, e_\tau, 0)$ and $\Sigma_m \triangleq (-L, e_a, e_m, 0)$. Inspired by [123, Th. 2], the feasibility of the optimization problem (I.8) is related to the invariant zeros of $\Sigma_\tau$ and $\Sigma_m$, which are defined as follows.

**Definition 1.** (Invariant zeros) Consider the strictly proper system $\Sigma \triangleq (A, B, C, 0)$ with $A, B,$ and $C$ are real matrices with appropriate dimensions. A tuple $(\lambda, \bar{x}, g) \in \mathbb{C} \times \mathbb{R}^N \times \mathbb{R}$ is a zero dynamics of $\Sigma$ if it satisfies

$$
\begin{bmatrix}
\lambda I - A & -B \\
C & 0 \\
\end{bmatrix}
\begin{bmatrix}
\bar{x} \\
g \\
\end{bmatrix} =
\begin{bmatrix}
0 \\
0 \\
\end{bmatrix}, \quad \bar{x} \neq 0.
\tag{I.11}
$$

In this case, a finite $\lambda$ is called a finite invariant zero of $\Sigma$. Further, the strictly proper system $\Sigma$ always has at least one invariant zero at infinity [128, Ch. 3].

More specifically, the optimization (I.8) is feasible if and only if the unstable invariant zeros of $\Sigma_m$ are also invariant zeros of $\Sigma_\tau$ [123, Th. 2]. To derive a necessary and sufficient condition characterizing the set of feasible monitor vertices, we will investigate both finite and infinite invariant zeros of the two systems $\Sigma_m$ and $\Sigma_\tau$. The following Lemma considers the former.

**Lemma 1.** Consider a networked control system associated with a connected undirected graph $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, \mathcal{A})$, whose vertex dynamics and control law are described in (I.1) and (I.2), respectively. Suppose that the networked control
system is driven by the stealthy data injection attack (I.3) at a single attack
vertex $v_a$, and observed by a single monitor vertex $v_m$, resulting in the state-
space model $\Sigma_m \triangleq (-L, e_a, e_m^\top, 0)$. Then, the networked control system $\Sigma_m$
has no invariant zero on the closed positive real line.

**Proof:** The proof follows directly from the results in [132, Th. 3.7 & 3.9].

**Remark 2.** By inheriting the results in [133], the other invariant zeros on
the closed right half-plane possibly exist if the input and output vertices have
short weak paths and long strong paths between them. On the other hand, the
graph representing the system (I.1) under control law (I.2) is unweighted,
i.e., all the edges have the same weight values, conflicting with the above
sufficient condition in [133]. We leave the necessary condition under which
the system $\Sigma_m$ has no invariant zeros on the closed right half-plane for future
research.

Based on the above remarks, assuming that the system $\Sigma_m$ has no finite
unstable zero, we then investigate the infinite zeros of the systems $\Sigma_m$ and
$\Sigma_\tau$. In the investigation, we make use of known results connecting infinite
invariant zeros mentioned in Definition 1 and the relative degree of a linear
system, which is defined below.

**Definition 2.** (Relative degree) [35, Ch. 13] Consider the strictly proper
system $\Sigma \triangleq (A, B, C, 0)$ with $A \in \mathbb{R}^{n \times n}$, $B$, and $C$ are real matrices with
appropriate dimensions. The system $\Sigma$ is said to have relative degree $r$ ($1 \leq
r \leq n$) if the following conditions satisfy

$$CA^kB = 0, \quad 0 \leq k < r - 1,$$

$$CA^{r-1}B \neq 0.$$  \hspace{1cm} (I.12)

**Remark 3.** Let $H(s) = C(sI - A)^{-1}B$ be the transfer function of the above
system $\Sigma$. The relative degree $r$ of the system $\Sigma$ defined in Definition 2 is
also the difference between the degrees of the denominator and the numerator
of $H(s)$ [35], which in turn corresponds to the degree of the infinite zero [128,
Ch. 3].

Based on Definition 2, let us denote $r_\tau a$ and $r_{ma}$ as the relative degrees
of $\Sigma_\tau$ and $\Sigma_m$, respectively. In the scope of this study, we have assumed
that the cyber-attack (I.3) has no direct impact on the outputs (I.5) and
(I.6), resulting in strictly proper systems $\Sigma_\tau$ and $\Sigma_m$. This implies that
the relative degrees $r_\tau a$ and $r_{ma}$ of $\Sigma_\tau$ and $\Sigma_m$ are positive, yielding their
infinite zeros. Those infinite zeros will be considered to present the following
Theorem that gives us a necessary and sufficient condition for finding feasible
monitor vertices $M_r$.

**Theorem 1.** Consider the strictly proper systems $\Sigma_\tau \triangleq (-L, e_a, e^T_\tau, 0)$ and $\Sigma_m \triangleq (-L, e_a, e^T_m, 0)$, in which the two systems have the same stealthy data
injection attack input at a single attack vertex $v_a$ but different output ver-
tices, i.e., $v_\tau$ for $\Sigma_\tau$ and $v_m$ for $\Sigma_m$. Suppose the systems $\Sigma_\tau$ and $\Sigma_m$ have
relative degrees $r_\tau a$ and $r_{ma}$, respectively. Then, the worst-case impact of
the stealthy data injection attack (I.8) is bounded if and only if the following
condition holds

$$r_{ma} \leq r_\tau a. \quad \text{(I.13)}$$

**Proof:** Followed by [123, Th. 2], the optimization problem (I.8) is feasible
if and only if $\Sigma_m$ has unstable invariant zeros that are also invariant zeros of
$\Sigma_\tau$. Based on Lemma 1 and Remark 2, $\Sigma_m$ has no finite unstable invariant
zero, which leaves us to analyze infinite zeros of those systems. Recall the
equivalence between the relative degree of a SISO system and the degree of
its infinite zero. Hence, a necessary condition to guarantee the feasibility of
the optimization (I.8) is that the number of infinite invariant zeros of $\Sigma_m$
is not greater than that of $\Sigma_\tau$. This implies $r_{ma} \leq r_\tau a$. For sufficiency, it
remains to show that if $r_{ma} \leq r_\tau a$, any infinite zeros of $\Sigma_m$ are also infinite
zeros of $\Sigma_\tau$. We will investigate each infinite zero of $\Sigma_m$ by starting from
their transfer functions with zero initial states

$$G_{\tau a}(s) = e^T_\tau (sI + L)^{-1}e_a = \frac{P_{\tau a}(s)}{Q(s)},$$

$$G_{ma}(s) = e^T_m (sI + L)^{-1}e_a = \frac{P_{ma}(s)}{Q(s)}, \quad \text{(I.14)}$$

where $s \in \mathbb{C}$. Based on Remark 3 and the minimal realisations $\Sigma_\tau$ and $\Sigma_m$,
$P_{\tau a}(s)$, $P_{ma}(s)$, and $Q(s)$ are the polynomials of degrees $N - r_\tau a$, $N - r_{ma}$,
and $N$, respectively. Let us denote $z_k = \sigma_k + j\omega_k \in \mathbb{C}$, $k \in \{1, 2, \ldots, r_{ma}\}$
with infinite module as infinite zeros of $\Sigma_m$. Indeed, [134] $z_k$ ($1 \leq k \leq r_{ma}$)
is an infinite zero of maximal degree $r_{ma}$ of $\Sigma_m$ if it satisfies

$$\lim_{\|z_k\|_2 \to \infty} z_k^q G_{ma}(z_k) = 0, \quad (0 \leq q \leq r_{ma} - 1),$$

$$\lim_{\|z_k\|_2 \to \infty} z_k^{r_{ma}} G_{ma}(z_k) \neq 0. \quad \text{(I.15)}$$
Further, with $0 \leq q \leq r_{ma} - 1$, we also basically have

$$\lim_{\|z_k\|_2 \to \infty} z_k^q G_{\tau a}(z_k) = \lim_{\|z_k\|_2 \to \infty} \frac{z_k^q P_{\tau a}(z_k)}{Q(z_k)} = 0. \quad (I.16)$$

The above limit (I.16) holds because the denominator $z^q P_{\tau a}(s)$ is the polynomial of degree $N - r_{\tau a} + q \leq N - 1 < N$, the degree of the polynomial $Q(z_k)$. This implies that any infinite zeros $z_k$ of maximal degree $r_{ma}$ of $\Sigma_m$ are also infinite zeros of degree $r_{ma}$ of $\Sigma_\tau$.

The following Lemma introduces a sufficient condition under which feasible monitor vertices guarantee the feasibility of the optimization (I.8) for an arbitrary attack vertex.

**Lemma 2.** Consider a networked system associated with a connected undirected graph $G \triangleq (V, E, A)$, whose vertex dynamics and control law are described in (I.1) and (I.2), respectively. The networked system is driven by the stealthy data injection attack at an arbitrary attack vertex $v_a$ with its impact measured at a given target vertex $v_\tau$. Suppose that there exists a feasible monitor vertex $v_m$ that directly connects to all the neighbors of the target vertex $v_\tau$. Then, the optimisation (I.8) is feasible. Furthermore, defining $A_m \triangleq I + A$, this vertex $v_m$ satisfies

$$e_\tau^\top A_m e_m = e_\tau^\top A^2 e_\tau. \quad (I.17)$$

**Proof:** Recalling that the relative degrees of $\Sigma_\tau$ and $\Sigma_m$ are related to the length of the shortest paths (i.e., distance) from $v_a$ to $v_\tau$ and $v_m$, respectively [132, Th. 3.2], the first part of the proof follows directly from the fact that a vertex $v_m$ is connected to all the neighbors of $v_\tau$. This implies that the distance from any arbitrary attack vertex $v_a \neq v_\tau$ to $v_m$ will be less or equal to the distance from $v_a$ to $v_\tau$. Thus, the vertex $v_m$ satisfies (I.13). The remainder of the proof expresses the relation between $v_m$ and $v_\tau$ in terms of the adjacency matrix and is omitted due to space limitations.

**Remark 4.** To seek a set of feasible monitor vertices, the algebraic condition (I.17) is simply tested with all the vertices $v_m \neq v_\tau \in V$.

## 4 Numerical Examples

To validate the obtained results, let us take an example of a 10-vertex networked control system depicted in Fig. I.2. We simply verify that no pair of attack and monitor vertices exhibits finite unstable zeros. Suppose that $v_5$
Table I.1: Game payoff (I.8) w.r.t. target vertex $v_5$ for the detector and the adversary corresponding to their chosen pair of monitor and attack vertices.

<table>
<thead>
<tr>
<th>$v_m$</th>
<th>$v_1$</th>
<th>$v_2$</th>
<th>$v_3$</th>
<th>$v_4$</th>
<th>$v_5$</th>
<th>$v_6$</th>
<th>$v_7$</th>
<th>$v_8$</th>
<th>$v_9$</th>
<th>$p^*(v_m)$ (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$v_1$</td>
<td>1</td>
<td>1.0062</td>
<td>1.2405</td>
<td>$\infty$</td>
<td>1.4384</td>
<td>$\infty$</td>
<td>$\infty$</td>
<td>1.2417</td>
<td>1.0074</td>
<td>0</td>
</tr>
<tr>
<td>$v_2$</td>
<td>1.2124</td>
<td>1</td>
<td>1.7337</td>
<td>$\infty$</td>
<td>1.4669</td>
<td>$\infty$</td>
<td>$\infty$</td>
<td>1.1984</td>
<td>0</td>
<td>$\approx 100$</td>
</tr>
<tr>
<td>$v_3$</td>
<td>1.6565</td>
<td>1.2329</td>
<td>1</td>
<td>1.0943</td>
<td>1.1905</td>
<td>1.008</td>
<td>$\infty$</td>
<td>1.2569</td>
<td>1.2681</td>
<td>$\approx 0$</td>
</tr>
<tr>
<td>$v_4$</td>
<td>$\infty$</td>
<td>$\infty$</td>
<td>1.1742</td>
<td>1</td>
<td>1.4407</td>
<td>1</td>
<td>$\infty$</td>
<td>1.0126</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$v_6$</td>
<td>1.1886</td>
<td>1.0029</td>
<td>1.1729</td>
<td>1.2122</td>
<td>1</td>
<td>1.0045</td>
<td>1.212</td>
<td>$\infty$</td>
<td>1.0038</td>
<td>0</td>
</tr>
<tr>
<td>$v_7$</td>
<td>$\infty$</td>
<td>2.2853</td>
<td>1</td>
<td>1</td>
<td>1.2928</td>
<td>1</td>
<td>$\infty$</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$v_9$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$\infty$</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$v_{10}$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$\infty$</td>
<td>1</td>
<td>2.3027</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

is the target vertex. There are two feasible monitor vertices $v_3$ and $v_6$, which satisfy the algebraic condition (I.17). Indeed, we simulate two scenarios, in which the detector monitors the outputs of the vertices $v_3$ (feasible) and $v_2$ (infeasible). Meanwhile, the adversary selects the vertex $v_4$ to conduct malicious attack signals at frequency 1.67 Hz depicted in Fig. I.3a. The outputs of the monitor vertices $v_2$, $v_3$ and the target vertex $v_5$ are shown in Fig. I.3b. Fig. I.3b shows that the output of the feasible monitor vertex $v_3$ (red dash-dotted line) approximately tracks the figure for the target vertex $v_5$ (blue dashed line). The energy produced by the output of the vertices $v_5$ and $v_3$ witnesses no noticeable difference, namely around 1.04. By contrast, the output energy of the infeasible monitor vertex $v_2$ (yellow dotted line) is only 0.27, almost four times as low as the output energy of the target vertex $v_5$. More specifically, the output energies of those vertices over time horizon are illustrated in Fig. I.4. Next, we will investigate how the ratio of the output energy of the above vertices progresses when increasing the frequency of the attack signals (see Fig. I.5). As seen in Fig. I.5, the gap between the two lines dramatically increases following the rise of the attack signal frequency. While the blue dotted-line ($v_m = v_3$) almost remains unchanged at 1.0, the red dashed-line ($v_m = v_2$) significantly becomes unbounded as the attack signal frequency increases. This implies that with massively high frequencies of the attack signals, the adversary is capable of manipulating the adversarial effect on the output of the target vertex at wish while remaining undetected at the infeasible monitor vertex $v_2$.

Next, the above results will be verified once again by computing the game payoff $J_5(v_a, v_m)$ with pairs of attack and monitor vertices ($v_a, v_m \neq v_5 \in \mathcal{V}$) (see Tab. I.1). Looking at the third column ($v_m = v_3$) and the fifth column ($v_m = v_6$) of Tab. I.1, no cell gives infinite value. On the other hand, the other columns show at least one infinite game payoff. This assessment once
Figure I.2: 10-vertex networked control system with target vertex $v_5$, attack vertex $v_4$, and feasible monitor vertices $v_3$ and $v_6$.

Again confirms that $v_m = v_3$ and $v_m = v_6$ are the feasible monitor vertices solving Problem 2.

By observing the game payoffs with the target vertex $v_5$ in Tab. I.1, there is no pure Nash equilibrium. However, this game always admits a mixed-strategy Nash equilibrium [112]. Next, we investigate the mixed-strategy Nash equilibrium for this example. Let us denote $p(v_a)$ and $p(v_m)$ as the probabilities of attack $v_a$ and monitor vertices $v_m$, respectively. $P(v_a) = [p(v_a=1), \ldots, p(v_a=10)]^\top$, $P(v_m) = [p(v_m=1), \ldots, p(v_m=10)]^\top$. The expected game payoff w.r.t. the target vertex $v_5$ for attack vertex $v_a$ and monitor vertex $v_m$ is given by

\begin{equation}
Q_5(v_a, v_m) = P(v_a)^\top J_5 P(v_m),
\end{equation}

where $J_5 = [J_5(v_i, v_j)_{ij}]$ is a 9×9-game matrix computed in Tab. I.1. There
4. Numerical Examples

Figure I.3: (a) Attack signals directly injected into the input of $v_4$ at frequency 1.67 Hz; (b) Outputs of target $v_5$, feasible $v_3$, infeasible vertices $v_2$.

Figure I.4: The output energies of vertices $v_2$, $v_3$, and $v_5$ over time horizon.

exits a saddle point $(v^*_a, v^*_m)$ satisfies

$$-\infty < Q_5(v^*_a, v^*_m) \leq Q_5(v^*_a, v^*_m) \leq Q_5(v^*_a, v^*_m) < \infty, \quad (I.19)$$

$$\forall v_a, v_m \neq v_r \in \mathcal{V}.$$  

The saddle point $(v^*_a, v^*_m)$ in the condition above indicates that a deviation of selecting $v_a(v_m)$ does not increase(decrease) the optimal expected game payoff $Q_5(v^*_a, v^*_m)$. From the numerical results in Tab. I.1, while the probability of selecting $v_m = 6$ is approximately 100%, the figures for $v_a = 2$ is
approximately 100%. The optimal probabilities $P^*(v_a)$ and $P^*(v_m)$ give us the optimal expected game payoff $Q_5(v^*_a, v^*_m) = 1.4669$.

5 Conclusion

In this paper, we investigated a continuous-time networked control system in the presence of a cyber-attack conducted by an adversary. An optimal sensor placement problem was raised such that a detector places a sensor at a vertex to monitor such a cyber-attack. We invoked a single-adversary-single-detector zero-sum game to describe the optimal sensor placement problem. This game was then formulated by employing a min-max optimization problem. In order to guarantee the feasibility of the min-max optimization problem, this paper presented a necessary and sufficient condition and an algebraic sufficient condition to find feasible monitor vertices. By placing a sensor at one of the feasible monitor vertices, the detector possibly monitors the cyber-attack. Further, the mixed-strategy Nash equilibrium of the zero-sum game was also analyzed to determine the optimal sensor placement. In future works, by inheriting the concept of an untouchable target vertex in this study, our game will be expanded to consider multiple adversaries and multiple detectors.
Title
A Zero-Sum Game Framework for Optimal Sensor Placement in Uncertain Networked Control Systems under Cyber-Attacks

Authors
Anh Tung Nguyen, Sribalaji C. Anand, and André Teixeira

Edited version of
A Zero-Sum Game Framework for Optimal Sensor Placement in Uncertain Networked Control Systems under Cyber-Attacks

Abstract
This paper proposes a game-theoretic approach to address the problem of optimal sensor placement against an adversary in uncertain networked control systems. The problem is formulated as a zero-sum game with two players, namely a malicious adversary and a detector. Given a protected performance vertex, we consider a detector, with uncertain system knowledge, that selects another vertex on which to place a sensor and monitors its output with the aim of detecting the presence of the adversary. On the other hand, the adversary, also with uncertain system knowledge, chooses a single vertex and conducts a cyber-attack on its input. The purpose of the adversary is to drive the attack vertex as to maximally disrupt the protected performance vertex while remaining undetected by the detector. As our first contribution, the game payoff of the above-defined zero-sum game is formulated in terms of the Value-at-Risk of the adversary’s impact. However, this game payoff corresponds to an intractable optimization problem. To tackle the problem, we adopt the scenario approach to approximately compute the game payoff. Then, the optimal monitor selection is determined by analyzing the equilibrium of the zero-sum game. The proposed approach is illustrated via a numerical example of a 10-vertex networked control system.
1 Introduction

Networked control systems have been playing a crucial role in modeling, analysis, and operation of real-world large-scale interconnected systems such as power systems, transportation networks, and water distribution networks. Those systems consist of multiple interconnected subsystems which generally communicate with each other via insecure communication channels to share their information. This insecure protocol may leave the networked control systems vulnerable to cyber-attacks such as denial-of-service and false-data injection attacks [15], inflicting serious financial loss and civil damages. Reports on actual damages such as Stuxnet [56] and Industroyer [135] have described the catastrophic consequences of such cyber-attacks for an Iranian nuclear program and a Ukrainian power grid, respectively. Motivated by the above observation, cyber-physical security has increasingly received much attention from control society in recent years.

One of the most popular security metrics is the game-theoretic approach that has been successfully applied to deal with the problem of robustness, security, and resilience of networked control systems [112]. This approach affords us to address the robustness and security of networked control systems within the common well-defined framework of $H_\infty$ robust control design. Further, many other concepts of games considering networked systems subjected to cyber-attacks such as dynamic [130], stochastic [131], network monitoring [121,136], and zero-sum games [137] have been recently studied. Although the above games were successful in studying control systems subjected to cyber-attacks such as denial-of-service and stealthy data injection attacks, the full system model knowledge was assumed to be available to both the malicious adversary and the detector. This assumption might be restrictive when it comes to large-scale interconnected systems which can consist of a huge number of subsystems. This can be explained by a variety of facts such as (i) limited availability of computational resources for modeling, (ii) limited availability of modeling data, and (iii) modeling errors. Thus, the adversary and the detector might have limited system knowledge instead of accurate system parameters, which will be addressed throughout this paper.

In this paper, we deal with the problem of optimal sensor placement against an adversary in an uncertain networked control system which is represented by interconnected vertices. Given a protected performance vertex, the detector monitors the system by selecting a single monitor vertex and placing a sensor to measure its output with the purpose of detecting cyber-attacks. Meanwhile, the adversary chooses a single vertex to attack and directly injects attack signals into its input via the wireless network. The aim of the adversary is to steer the attack vertex as to maximally disrupt the
1. Introduction

Figure II.1: Visualization of a zero-sum game between a detector and an adversary in a networked control system.

protected performance vertex while remaining undetected by the detector. The contributions of this paper are the following

1. The problem of optimal sensor placement against the adversary is formulated as a zero-sum game between two strategic players, i.e., the adversary and the detector, with the same uncertain system knowledge.

2. Due to the uncertainty, the game payoff of the zero-sum game, which is a min-max optimization problem, is computationally intractable [138]. To deal with the problem, we adopt the scenario approach [139] to approximately compute the above game payoff.

3. We show that the existence of a finite solution to the problem is related to the system-theoretic properties of the dynamical system, namely its invariant zeros and relative degrees.

4. The solutions to the problem of the optimal sensor placement are provided by investigating the pure and the mixed-strategy equilibrium of the zero-sum game in a numerical example.

We conclude this section by providing the notations which are used throughout this paper. The problem description is given in Section 2. Thereafter, Section 3 formulates the problem of optimal sensor placement as a
zero-sum game with the game payoff based on a risk metric. The evaluation of the game payoff is carried out in Section 4. Section 5 presents a numerical example of the zero-sum game between an adversary and a detector and computes the optimal monitor selection based on the mixed-strategy Nash equilibrium. Concluding remarks are provided in Section 6.

**Notation:** the set of real positive numbers is denoted as $\mathbb{R}_+^+$; $\mathbb{R}^n$ and $\mathbb{R}^{n \times m}$ stand for sets of real $n$-dimensional vectors and $n$-row $m$-column matrices, respectively. Let us define $e_i \in \mathbb{R}^n$ with all zero elements except the $i$-th element that is set as 1. A continuous-time system with the state-space model $\dot{x}(t) = Ax(t) + Bu(t)$, $y(t) = Cx(t) + Du(t)$ is denoted as $\Sigma \triangleq (A, B, C, D)$. Consider the norm $\|x\|_{L_2[0,T]} \triangleq \int_0^T \|x(t)\|_2^2 \, dt$. The space of square-integrable functions is defined as $L_2[0,\infty)$ and the extended space is defined as $L_2[0,T]$ for $T > 0$. We denote $\mathbb{I}_A(x)$ as an indicator function such that $\mathbb{I}_A(x) = 1$ if $x \in A$, otherwise $\mathbb{I}_A(x) = 0$. The probability of $X$ is denoted as $\mathbb{P}(X)$. For $x \in \mathbb{R}$, $\lfloor x \rfloor$ represents a value rounded to the nearest integer greater than or equal to $x$. Let $G \triangleq (\mathcal{V}, \mathcal{E}, A, \Theta)$ be an undirected weighted digraph with the set of $N$ vertices $\mathcal{V} = \{v_1, v_2, \ldots, v_N\}$, the set of edges $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$, the weighted adjacency matrix $A \triangleq [a_{ij}]$, and the weighted self-loop matrix $\Theta$. For any $(v_i, v_j) \in \mathcal{E}$, $i \neq j$, the element of the weighted matrix $a_{ij}$ is positive, and with $(v_i, v_j) \notin \mathcal{E}$ or $i = j$, $a_{ij} = 0$. The degree of vertex $v_i$ is denoted as $d_i = \sum_{j=1}^n a_{ij}$ and the degree matrix of the graph $G$ is defined as $D = \text{diag}(d_1, d_2, \ldots, d_N)$, where $\text{diag}$ stands for a diagonal matrix. For each vertex $v_i$, it has a positive weighted self-loop gain $\theta_i > 0$. The weighted self-loop matrix of the graph $G$ is defined as $\Theta = \text{diag}(\theta_1, \theta_2, \ldots, \theta_N)$. The Laplacian matrix, representing the graph $G$, is defined as $L = [\ell_{ij}] = D - A + \Theta$. Further, $G$ is called an undirected graph if $A$ is symmetric. An edge of an undirected graph $G$ is denoted by a pair $(v_i, v_j) \in \mathcal{E}$. An undirected graph is connected if for any pair of vertices there exists at least one path between two vertices. The set of all neighbours of vertex $v_i$ is denoted as $\mathcal{N}_i = \{v_j \in \mathcal{V} \mid (v_i, v_j) \in \mathcal{E}\}$.

## 2 Problem Description

This section firstly presents the description of a networked control system. Then, we introduce a malicious adversary who with limited system knowledge conducts a cyber-attack to maliciously affect the system performance.
2. Problem Description

2.1 Networked Control System Description

Consider a networked control system associated with a connected undirected graph $G = (\mathcal{V}, \mathcal{E}, A, \Theta)$ with $N$ vertices, the state-space model of each one-dimensional vertex $v_i$, $i \in \{1, 2, \ldots, N\}$, is described as

$$\dot{x}_i^\Delta(t) = \sum_{v_j \in \mathcal{N}_i} \ell_{ij}^\Delta (x_i^\Delta(t) - x_j^\Delta(t)) + \tilde{u}_i(t), \quad (\text{II.1})$$

$$y_{i}^\Delta(t) = x_i^\Delta(t), \quad (\text{II.2})$$

where $x_i^\Delta(t), \tilde{u}_i(t) \in \mathbb{R}$ are the state of vertex $v_i$ and its control input received from its controller over the wireless network (see Fig. II.1), respectively. The performance of the networked control system (II.1) is measured via the state of a given vertex $v_{\tau} \in \mathcal{V}$ in (II.1). The weight parameters $\ell_{ij}^\Delta, \forall(v_i, v_j) \in \mathcal{E}$, are uncertain and assumed to be structured as $\ell_{ij}^\Delta = \bar{\ell}_{ij} + \delta_{ij}$, where $\bar{\ell}_{ij}$ and $\delta_{ij}$ are the nominal value and the bounded probabilistic uncertainty of $\ell_{ij}^\Delta$, respectively.

First, we consider the wireless network healthy, i.e., the absence of cyber-attacks. Thus, the received control input $\tilde{u}_i(t)$ of vertex $v_i$, $i \in \{1, 2, \ldots, N\}$, is the same as the control input sent by its controller:

$$\tilde{u}_i(t) = u_i(t) = -\theta_i x_i^\Delta(t), \quad (\text{II.3})$$

where $u_i(t)$ is the control input designed and sent by the controller of vertex $v_i$. $\theta_i \in \mathbb{R}^+$ is an adjustable self-loop control gain of vertex $v_i$.

For convenience, let us denote $x^\Delta(t) \triangleq [x_1^\Delta(t), x_2^\Delta(t), \ldots, x_N^\Delta(t)]^\top$ as the state of the networked control system. The dynamics of the networked control system (II.1) under the control law (II.3) can be rewritten as

$$\dot{x}^\Delta(t) = -L^\Delta x^\Delta(t), \quad (\text{II.4})$$

where the uncertain matrix $L^\Delta$ is defined as: $L^\Delta \triangleq \bar{L} + \Delta$, $\Delta \in \Omega$, where $\Omega$ is a closed and bounded set, $\bar{L} \triangleq [\bar{\ell}_{ij}]$ and $\Delta \triangleq [\delta_{ij}]$ are nominal value and bounded uncertainty of $L^\Delta$, respectively. Next, let us make use of the following assumptions.

**Assumption 1.** We assume that the healthy networked control system (II.4) is at its equilibrium before being attacked.

**Assumption 2.** The input of the given performance vertex $v_{\tau}$ is protected from any attacks. Further, its state is unmeasurable.
2.2 Adversary Description

This part introduces resources and an attack strategy of the adversary with limited system knowledge, so-called bounded-rational adversary [138, Def. 2.2].

System knowledge

The adversary knows the location of the protected target vertex $v_\tau$, the appearance of a detector, the set of $N$ vertices $\mathcal{V}$, and the set of edges $\mathcal{E}$. However, the adversary does not know the exact location of the detector and has limited knowledge about $L^\Delta$ in (II.4). The adversary only knows $\bar{L}$ and $\Omega$ instead of $L^\Delta$.

Disruption resource

Except for the protected target vertex $v_\tau$, the adversary is able to conduct a cyber-attack on the input of another vertex. The adversary firstly assumes the location of a monitor vertex $v_m$ selected by the detector. Then, the adversary selects a vertex $v_a \in \mathcal{V} \setminus \{v_\tau\}$ and injects a malicious attack signal $a(t) \in \mathbb{R}$ on its input with the aim of manipulating the output of the protected target vertex $v_\tau$. The control input (II.3) of vertex $v_i$, $i \in \{1, 2, \ldots, N\}$, received from its controller over the attacked wireless network can be described as follows

$$\tilde{u}_i(t) = u_i(t) + \begin{cases} 0, & v_i \neq v_a, \\ a(t), & v_i = v_a. \end{cases} \quad \text{(II.5)}$$

Thus, the adversary perceives the system model (II.4) under the control law (II.5) with two outputs at the two vertices $v_\tau$ and $v_m$ as an uncertain dynamical system described by

$$\dot{x}^\Delta(t) = -L^\Delta x^\Delta(t) + e_a a(t), \quad \text{(II.6)}$$

$$y^\Delta_\tau(t) = e_\tau^\top x^\Delta(t), \quad \text{(II.7)}$$

$$y^\Delta_m(t) = e_m^\top x^\Delta(t). \quad \text{(II.8)}$$

Adversary strategy

The goal of the adversary is to maliciously manipulate the output of the protected target vertex $v_\tau$ while remaining stealthy with the detector. To this end, the adversary conducts the stealthy data injection attack, which is defined as follows. Consider the above structure of the uncertain continuous-time system (II.6)-(II.8) which is denoted as $\Sigma^\Delta_{r,m} \triangleq (-L^\Delta, e_a, [e_\tau, e_m]^\top, 0)$,
with target output \( y^\Delta_t(t) = e^\top_x x^\Delta(t) \) and monitor output \( y^\Delta_m(t) = e^\top_m x^\Delta(t) \). The input signal \( a(t) \) of the system \( \Sigma^{\Delta}_{\tau,m} \) is called the stealthy data injection attack if the monitor output satisfies \( \| y^\Delta_m \|_{L_2[0,T]}^2 < \sigma \), in which \( \sigma > 0 \) is called an alarm threshold. Further, the impact of the stealthy data injection attack is measured via the energy of the target output over the horizon \([0, T]\), i.e., \( \| y^\Delta_t \|_{L_2[0,T]}^2 \).

Due to limited system knowledge, the uncertain system dynamics (II.6)-(II.8) are not explicitly available to the adversary. Such an issue causes difficulty for the adversary in designing the attack strategy. To deal with the issue, the next section adopts a risk metric to evaluate the attack impact over the probabilistic uncertainty set, which can be evaluated by the adversary to select an attack vertex.

## 3 Problem Formulation

We consider that both the adversary and the detector have the same bounded uncertainty about the system knowledge. Based on this assumption, for a given uncertain parameter and attack and monitor vertices, the attack impact is characterized via an optimal control problem. Then, we aggregate the attack impact over the probabilistic uncertainty set by means of a risk metric. Finally, the problem of optimal selection of attack and monitor vertices is formulated as a zero-sum game between two strategic players, the adversary and the detector, where the game payoff corresponds to the risk of the attack impact evaluated over the probabilistic uncertainty.

### 3.1 Stealthy Data Injection Attack Policy

Due to the presence of uncertainty in the system model (II.6)-(II.8), the attack impact \( J_\tau(v_a, v_m; \Delta, a) \) on the target vertex \( v_\tau \) by the attack vector \( a \in L_{2e} \) becomes a function of the random variable \( \Delta \in \Omega \)

\[
J_\tau(v_a, v_m; \Delta, a) \triangleq \| y^\Delta_t \|_{L_2}^2 1_A(a), \quad (II.9)
\]

\[
A \triangleq \{ a | \| y^\Delta_m \|_{L_2}^2 \leq \sigma, (II.6), (II.8), \ x(0) = 0 \}, \quad (II.10)
\]

where \( y^\Delta_t(t) \) and \( y^\Delta_m(t) \) are the output of the target vertex \( v_\tau \) and the output of the monitor vertex \( v_m \), respectively. From (II.9), the worst-case attack impact on the target vertex \( v_\tau \) with the random variable \( \Delta \in \Omega \) can be formulated as follows

\[
\sup_{a \in L_{2e}} J_\tau(v_a, v_m; \Delta, a). \quad (II.11)
\]
It is worth noting that (II.11) is introduced to evaluate the worst-case attack impact for each pair of $v_a$ and $v_m$, thus allowing one to compare the impact for different pairs of attack and monitor vertices. Further, the worst-case attack impact (II.11) is proportional to the alarm threshold $\sigma$ for all possible pairs of $v_a$ and $v_m$. Therefore, without loss of generality, let us set the alarm threshold $\sigma = 1$ in the remainder of this paper.

**Remark 1.** Due to the random variable $\Delta \in \Omega$, the worst-case impact (II.11) becomes a random variable. Thus, in order to compare the worst-case impacts made by pairs of $v_a$ and $v_m$ over the uncertainty set $\Omega$, we need to employ a risk metric which will be introduced in the rest of this subsection.

After investigating the worst-case attack impact (II.11) on the target vertex $v_\tau$ with all the possible pairs of attack $v_a$ and monitor vertices $v_m$, the adversary firstly chooses the attack vertex $v_a$ such that the corresponding risk (defined in Definition 1) is maximized [138]. Then, the adversary directly injects the stealthy data injection attack on the input of the selected attack vertex $v_a$. To this end, the adversary deals with the following optimization problem:

$$\max_{v_a \neq v_\tau \in \mathcal{V}} J_{\tau}(v_a, v_m), \quad (II.12)$$

$$J_{\tau}(v_a, v_m) = R_{\Delta \in \Omega} \left[ \sup_{a \in \mathcal{L}_2} J_{\tau}(v_a, v_m; \Delta, a) \right], \quad (II.13)$$

where $R_{\Delta \in \Omega}$ is a risk metric evaluated over the probabilistic uncertainty set. In this paper, we use the well-known Value-at-Risk [140] as our risk metric, which is defined below.

**Definition 1.** (Value-at-Risk (VaR)): Given a random variable $X$ and $\beta \in (0, 1)$, the VaR is defined as

$$\text{VaR}_{\beta}(X) \triangleq \inf \left\{ x | \mathbb{P}[X \leq x] \geq 1 - \beta \right\}. \quad (II.14)$$

With a specified level $\beta \in (0, 1)$, $\text{VaR}_{\beta}$ is the lowest amount of $x$ such that with probability $1 - \beta$, the random variable $X$ does not exceed $x$. \hfill \triangleright

In order to counter the adversary, the detector adopts the game-theoretic approach to design its detection strategy, which will be introduced in the next part.

### 3.2 Game-theoretic Approach to Sensor Placement

The detector chooses a vertex $v_m \in \mathcal{V} \setminus \{v_\tau\}$ and monitors its output with the purpose of minimizing the risk (II.13). Hence, the detector addresses the following problem.
Problem 1. (Optimal monitor selection) Given a target vertex $v_\tau$ and an arbitrary attack vertex $v_a$, select a monitor vertex that minimizes the risk corresponding to the worst-case attack impact $J_\tau(v_a, v_m)$ defined in (II.13).

The above detector objective is converted into the following optimization problem:

$$\min_{v_m \neq v_\tau \in \mathcal{V}} J_\tau(v_a, v_m). \quad (\text{II.15})$$

From the scenario of a single-adversary-single-detector we are considering, the adversary objective (II.12), and the detector objective (II.15), we formulate Problem 1 as a zero-sum game with the game payoff (II.13) between two players, i.e., the adversary and the detector, as follows:

$$\min_{v_m \neq v_\tau \in \mathcal{V}} \max_{v_a \neq v_\tau \in \mathcal{V}} J_\tau(v_a, v_m). \quad (\text{II.16})$$

The min-max optimization problem (II.16) admits a saddle-point equilibrium $(v^*_a, v^*_m)$ [112] if and only if it satisfies

$$-\infty < J_\tau(v_a, v_m^*) \leq J_\tau(v^*_a, v^*_m) \leq J_\tau(v^*_a, v_m) < \infty,$$

$$\forall v_a, v_m \in \mathcal{V} \setminus \{v_\tau\}. \quad (\text{II.17})$$

The game payoff of the saddle-point equilibrium $J_\tau(v^*_a, v^*_m)$ implies that a deviation of the attack vertex $\forall v_a \in \mathcal{V} \setminus \{v_\tau, v_a^*\}$ does not gain the game payoff and a deviation of the monitor vertex $\forall v_m \in \mathcal{V} \setminus \{v_\tau, v_m^*\}$ does not decrease the game payoff.

Remark 2. Since the zero-sum game (II.16) determined by discrete decisions of the adversary and the detector might be solved via linear programming [141, Ch. 5], we need to evaluate the game payoff defined in (II.13) for all the possible pairs of $v_a$ and $v_m$. However, computing (II.13) requires us not only to address the non-convexity of the worst-case impact (II.11) but also to devise a computationally efficient approximation of (II.13) over a continuous uncertainty set.

The next section will give us an efficient method to approximately compute the game payoff (II.13) for each selected pair of $v_a$ and $v_m$.

4 Evaluating the Game Payoff

There are two difficulties in solving the zero-sum game (II.16). The first difficulty is that: for any given pair of $v_a, v_m$, and uncertainty $\Delta \in \Omega$,
the function $\sup_{a \in \mathcal{L}_2} J_{\tau}(v_a, v_m; \Delta, a)$ is a non-convex optimization problem. Secondly, since the set $\Omega$ is continuous, the problem of assessing the game payoff (II.13) is computationally intractable. Thus, in this section, we aim to address both difficulties by invoking the scenario approach [139] that discretizes the uncertainty set $\Omega$.

4.1 Worst-case Attack Impact for a Sampled Uncertainty Point

We begin by considering the case of a sampled uncertainty realization $\Delta_i \in \Omega$. Let us denote the value of the corresponding uncertain Laplacian matrix in (II.6) as $L^{\Delta_i}$ and the uncertain system (II.6)-(II.8) as $\Sigma_{\tau, m}^{\Delta_i} \triangleq \left(-L^{\Delta_i}, e_a, [e_{\tau}, e_m]^T, 0\right)$ with the attack input at vertex $v_a$, the target output at vertex $v_{\tau}$, and the monitor output at vertex $v_m$. For such an isolated uncertainty, the worst-case attack impact can be written as

$$\sup_{a \in \mathcal{L}_2} J_{\tau}(v_a, v_m; \Delta_i, a). \quad (II.19)$$

Following the details in [124, Prop. 1], the optimal control problem (II.19) can be equivalently rewritten as the following convex SDP

$$\gamma_i^* \triangleq \min_{\gamma_i \in \mathbb{R}^+, P_i = P_i^T \succeq 0} \gamma_i$$

subject to

$$R(\Sigma_{\tau, m}^{\Delta_i}, P_i, \gamma_i) \leq 0,$$

where

$$R(\Sigma_{\tau, m}^{\Delta_i}, P_i, \gamma_i) \triangleq \begin{bmatrix} -L^{\Delta_i} P_i & P_i L^{\Delta_i} P_i e_a & \gamma_i e_m e_m^T + e_{\tau} e_{\tau}^T & 0 \\ e_a^T P_i & 0 & 0 & 0 \end{bmatrix}.$$

(II.21)

Next, we tackle the game payoff evaluation over a continuous set of uncertainties $\Omega$ by first approximating the continuous uncertainty set $\Omega$ with a discrete set $\Omega_{M_1}$ of sampled uncertainty realizations, with cardinality $M_1$, and then using the point-wise evaluation of the worst-case attack impact described in (II.20).

4.2 Approximate Game Payoff Function

The game payoff (II.13) is difficult to determine since the risk metric operates over a continuous set $\Omega$. To this end, we adopt the scenario approach [139] to approximate the continuous uncertainty set $\Omega$, and consequently determine the approximate game payoff (II.13). Before this, we
**4. Evaluating the Game Payoff**

rewrite (II.13) for a given $\beta \in (0, 1)$ as (II.22).

$$J_\tau(v_a, v_m) = \inf \gamma \quad \text{s.t. } \mathbb{P}_\Omega[X \leq \gamma] \geq 1 - \beta,$$

where $X = \sup_{a \in \mathcal{L}_2} J_\tau(v_a, v_m; \Delta, a)$, $\Delta \in \Omega$, and the subscript to the probability operator denotes that it operates over the set $\Omega$. Next, we apply the scenario approach to determine the approximate value of the optimization problem (II.22) in the following theorem.

**Theorem 1.** Let $\epsilon_1 \in (0, 1)$ represent the accuracy with which the probability operator $\mathbb{P}_\Omega$ in (II.22) is approximated. Let $\beta_1 \in (0, 1)$ represent the confidence with which the accuracy $\epsilon_1$ is guaranteed, i.e.,

$$\mathbb{P}\{|\mathbb{P}_\Omega(X \leq \gamma) - \hat{P}_{M_1}| \geq \epsilon_1\} \leq \beta_1.$$  

(II.23)

Here $\hat{P}_{M_1}$ represents the approximation of the probability operator $\mathbb{P}_\Omega$ in (II.22) defined as

$$\hat{P}_{M_1} \triangleq \frac{1}{M_1} \sum_{i=1}^{M_1} I(X \leq \gamma), \text{ where } M_1 \geq \frac{1}{2\epsilon_1^2} \log \frac{2}{\beta_1}. \quad (II.24)$$

Then, the VaR$_\beta$ defined in (II.13) can be obtained with an accuracy $\epsilon_1$ and confidence $\beta_1$ by solving

$$\hat{\gamma} = \min \left\{ \gamma \in \Omega \left| \frac{1}{M_1} \sum_{i=1}^{M_1} \mathbb{I}(\gamma_i^* \leq \gamma) \geq 1 - \beta_1 \right. \right\}, \quad (II.25)$$

where $\hat{\gamma}$ represents the VaR$_\beta$ with an accuracy $\epsilon_1$. The value of $\gamma_i^*, i \in \{1, 2, \ldots, M_1\}$, is obtained by solving (II.20).

**Proof:** The proof follows directly from our previous results in [138, Th. 4.4].

**Remark 3.** Solving (II.25) with the risk metric defined in Definition 1 gives us a measure of risk for a corresponding pair of $v_a$ and $v_m$ that has been evaluated over the explicit probabilistic uncertainty set $\Omega$. This risk measure is different from the worst-case impact (II.11), which is a function of a random variable $\Delta \in \Omega$.

Theorem 1 provides a method to compute the approximate value of game payoff (II.13) which was difficult to compute previously. In order to evaluate the result of Theorem 1, the next subsection will address the feasibility of the optimization problem (II.25).
4.3 Feasibility Analysis

For $M_1$ sampled uncertainty $\Delta_i \in \Omega_{M_1}$, the following lemma gives us the necessary and sufficient condition to ensure that the problem (II.25) is feasible and therefore admits a finite upper bound.

Lemma 1 (Boundedness). Consider $M_1$ i.i.d. realizations of uncertainty $\Delta_i \in \Omega_{M_1}$. The optimal solution of (II.25) with these $M_1$ realizations of uncertainty is bounded if and only if the optimal value of (II.20) is bounded for at least $[M_1(1 - \beta_1)]$ system realizations.

Proof: The proof follows directly from our previous results in [138, Lem. 4.5].

Then, we investigate the feasibility of the optimization problem (II.20) for a system realization corresponding to a given sampled uncertainty $\Delta_i \in \Omega_{M_1}$. Let us denote the following systems $\Sigma_{r_i}^{\Delta_i} \triangleq (-L^{\Delta_i}, e_a, e_r^\top, 0)$ and $\Sigma_{m_i}^{\Delta_i} \triangleq (-L^{\Delta_i}, e_a, e_m^\top, 0)$. Inspired by [123, Th. 2], the feasibility of the optimization problem (II.20) is related to the invariant zeros of $\Sigma_{r_i}^{\Delta_i}$ and $\Sigma_{m_i}^{\Delta_i}$, which are defined as follows.

Definition 2. (Invariant zeros) Consider the strictly proper system $\Sigma \triangleq (A, B, C, 0)$ with $A$, $B$, and $C$ are real matrices with appropriate dimensions. A tuple $(\lambda, \bar{x}, g) \in \mathbb{C} \times \mathbb{C}^N \times \mathbb{C}$ is a zero dynamics of $\Sigma$ if it satisfies

$$
\begin{bmatrix}
\lambda I - A & -B \\
C & 0
\end{bmatrix}
\begin{bmatrix}
\bar{x} \\
g
\end{bmatrix} =
\begin{bmatrix}
0 \\
0
\end{bmatrix}, \quad \bar{x} \neq 0.
$$

(II.26)

In this case, a finite $\lambda$ is called a finite invariant zero of $\Sigma$. Further, the strictly proper system $\Sigma$ always has at least one invariant zero at infinity [128, Ch. 3].

More specifically, let us state the following lemma.

Lemma 2. [123, Th. 2] Consider the two following continuous time systems $\Sigma_{r_i}^{\Delta_i} \triangleq (-L^{\Delta_i}, e_a, e_r^\top, 0)$ and $\Sigma_{m_i}^{\Delta_i} \triangleq (-L^{\Delta_i}, e_a, e_m^\top, 0)$. The optimization problem (II.20) is feasible if and only if the unstable invariant zeros of $\Sigma_{r_i}^{\Delta_i}$ are also invariant zeros of $\Sigma_{m_i}^{\Delta_i}$.

Inspired by Lemma 2, we will investigate both finite and infinite invariant zeros of the two systems $\Sigma_{r_i}^{\Delta_i}$ and $\Sigma_{m_i}^{\Delta_i}$.

Finite invariant zeros

Let us state the following lemma that considers the finite invariant zeros of $\Sigma_{m_i}^{\Delta_i}$.
Lemma 3. Consider a networked control system associated with a connected undirected graph $G \triangleq (V, E, A, \Theta)$, whose closed-loop dynamics is described in (II.6)-(II.8) for a given sampled uncertainty $\Delta_i \in \Omega_{M_1}$. Suppose that the networked control system is driven by the stealthy data injection attack at a single attack vertex $v_a$, and observed by a single monitor vertex $v_m$, resulting in the state-space model $\Sigma_{m}^{\Delta_i} \triangleq (-L^\Delta_i, c_a, e_m^\top, 0)$. Then, there exist self-loop control gains $\theta_i, i \in \{1, 2, \ldots, N\}$, in (I.2) such that the networked control system $\Sigma_{m}^{\Delta_i}$ has no finite unstable invariant zero.

Proof: We postpone the proof to Appendix A. ■

The constructive proof of Lemma 3 (see Appendix A) gives us a design procedure to ensure that the system $\Sigma_{m}^{\Delta_i}$ has no finite unstable zero.

Infinite invariant zeros

We now investigate the infinite invariant zeros of the systems $\Sigma_{m}^{\Delta_i}$ and $\Sigma_{\tau}^{\Delta_i}$. In the investigation, we make use of known results connecting infinite invariant zeros mentioned in Definition 2 and the relative degree of a linear system, which is defined below.

Definition 3. (Relative degree) [35, Ch. 13] Consider the strictly proper system $\Sigma \triangleq (A, B, C, 0)$ with $A \in \mathbb{R}^{n \times n}, B,$ and $C$ are real matrices with appropriate dimensions. The system $\Sigma$ is said to have relative degree $r$ (1 ≤ $r$ ≤ $n$) if the following conditions satisfy

$$
CA^kB = 0, \quad 0 \leq k < r - 1,
$$

$$
CA^{-1}B \neq 0.
$$

(II.27)

Based on Definition 3, let us denote $r_{\tau_a}$ and $r_{ma}$ as the relative degrees of $\Sigma_{\tau}^{\Delta_i}$ and $\Sigma_{m}^{\Delta_i}$, respectively. In the scope of this study, we have assumed that the cyber-attack (II.5) has no direct impact on the outputs (II.7) and (II.8), resulting in strictly proper systems $\Sigma_{\tau}^{\Delta_i}$ and $\Sigma_{m}^{\Delta_i}, \forall \Delta_i \in \Omega_{M_1}$. This implies that the relative degrees $r_{\tau_a}$ and $r_{ma}$ of $\Sigma_{\tau}^{\Delta_i}$ and $\Sigma_{m}^{\Delta_i}$ are positive, yielding their infinite zeros. By following our existing result related to those infinite zeros [137, Th. 7] the infinite zeros of $\Sigma_{m}^{\Delta_i}$ are also the infinite zeros of $\Sigma_{\tau}^{\Delta_i}$ if and only if the following condition holds

$$
r_{ma} \leq r_{\tau_a}.
$$

(II.28)
Boundedness of solutions

After analyzing both finite and infinite zeros of the two systems \( \Sigma^\Delta_i \) and \( \Sigma^\Delta_m \), the following theorem gives us a sufficient condition to ensure the feasibility of the optimization problem (II.20), and thus of the existence of a finite upper bound on the corresponding optimal value.

**Theorem 2.** Consider the strictly proper systems \( \Sigma^\Delta_i \triangleq (-L^\Delta_i, e, e^\top, 0) \) and \( \Sigma^\Delta_m \triangleq (-L^\Delta_m, e, e^\top, 0) \), in which the two systems have the same stealthy data injection attack input at a single attack vertex \( v_a \) but different output vertices, i.e., \( v_T \) for \( \Sigma^\Delta_i \) and \( v_m \) for \( \Sigma^\Delta_m \). Suppose the systems \( \Sigma^\Delta_i \) and \( \Sigma^\Delta_m \) have relative degrees \( r_{\tau a} \) and \( r_{ma} \), respectively. Then, the problem (II.20) admits a finite solution if

1. the self-loop control gains \( \theta_i, \ i \in \{1,2,\ldots,N\} \), in (I.2) are chosen such that the system \( \Sigma^\Delta_m \) has no finite unstable zeros; and
2. the condition (II.28) holds.

**Proof:** The proof is postponed to Appendix B.

The sufficient condition (II.28) will be verified by computing the approximate game payoffs (II.25) in Theorem 1 and the equilibrium of the zero-sum game (II.16) will be analyzed via a numerical example in the next section.

5 Numerical Examples

To validate the obtained results, through a numerical example, this section i) applies (II.25) with two different values of \( \beta \) to the example with the aim of verifying (II.28); ii) examines the saddle-point equilibrium of the zero-sum game (II.16) with the two different values of \( \beta \); iii) computes the mixed-strategy Nash equilibrium of the zero-sum game in case there is no saddle-point equilibrium. Let us take an example of a 10-vertex networked control system depicted in Fig. II.2. The simulation parameters are chosen as follows:

\[
L^\Delta \triangleq [L^\Delta_{ij}] = [\bar{\ell}_{ij}] + [\delta_{ij}] + \Theta, \tag{II.29}
\]
\[
\bar{\ell}_{ij} = -10, \ \delta_{ij} \in [-0.5, 0.5], \ \forall (v_i, v_j) \in \mathcal{E}, i \neq j, \tag{II.30}
\]
\[
\bar{\ell}_{ij} = \delta_{ij} = 0, \ \forall (v_i, v_j) \notin \mathcal{E}, \tag{II.31}
\]
\[
\ell^\Delta_{ij} = - \sum_{v_j \in N_i} (\bar{\ell}_{ij} + \delta_{ij}), \ \theta_0 = 0.5. \tag{II.32}
\]
5. Numerical Examples

5.1 Computing the Approximate Game Payoff

To compute (II.25), let us choose $\epsilon_1 = 0.06, \beta_1 = 0.08$, and $M_1 = 450$, which satisfy (II.24). For any sampled uncertainty $\Delta_i \in \Omega_{M_1}$, the chosen uniform offset self-loop control gain $\theta_0$ (see Appendix A) ensures that $\Sigma \Delta_i$ has no finite unstable zero, which validates Lemma 3. We will present two cases by selecting two values of the specified level $\beta$ in (II.22), i.e., $\beta_a = 0.08$ and $\beta_b = 0.15$. Suppose that $v_5$ is the protected target vertex (see Assumption 2 and Fig. II.2). There are two possible monitor vertices $v_2$ and $v_6$, which satisfy the necessary and sufficient condition (II.28) for any $v_a \in V \setminus \{v_5\}$ (see Fig. II.2). For more clarity, we compute the approximate game payoff (II.25) w.r.t. the target vertex $v_5$ for each pair of $v_a \in V \setminus \{v_5\}$ and $v_m \in \{v_2, v_6\}$ in the cases $\beta = \beta_a$ and $\beta = \beta_b$, which gives us

\begin{align*}
\mathcal{J}_5(v_a, v_m=2; \beta_a) & \leq 1.5848, \quad \mathcal{J}_5(v_a, v_m=6; \beta_a) \leq 1.5055, \quad (II.33) \\
\mathcal{J}_5(v_a, v_m=2; \beta_b) & \leq 1.5550, \quad \mathcal{J}_5(v_a, v_m=6; \beta_b) \leq 1.4803. \quad (II.34)
\end{align*}

Otherwise, there exits at least an attack vertex $v_a \in V \setminus \{v_5\}$ pairing with an arbitrary monitor $v_m \in V \setminus \{v_2, v_5, v_6\}$ to yield infinite game payoffs, e.g., $\mathcal{J}_5(v_a=3, v_m=1; \beta_a) = \infty, \mathcal{J}_5(v_a=3, v_m=1; \beta_b) = \infty, \mathcal{J}_5(v_a=10, v_m=3; \beta_a) = \infty, \mathcal{J}_5(v_a=10, v_m=3; \beta_b) = \infty$. In order to explain those infinite values, we verify the condition (II.28) by checking the relative degrees among those vertices via Fig. II.2, i.e., $r_{a=3, m=5} = 2 < r_{a=3, m=1} = 3$ and $r_{a=10, m=5} = 2 < r_{a=10, m=3} = 3$, which violate the necessary and sufficient condition (II.28).

5.2 Examining the Saddle-point Equilibrium

Next, we will investigate the equilibrium of the zero-sum game in the cases $\beta = \beta_a$ and $\beta = \beta_b$. Fig. II.3 illustrates the game payoffs for $v_a \in \{v_1, v_{10}\}$ and $v_m \in \{v_2, v_6\}$ corresponding to $\Delta_i \in \Omega_{M_1}$. In both cases $\beta = \beta_a$ and $\beta = \beta_b$, since those game payoffs dominate the values of the other choices of $v_a \in V \setminus \{v_1, v_5, v_{10}\}$ and $v_m \in \{v_2, v_6\}$, we only show four marked-lines in Fig. II.3.

In the first case $\beta = \beta_a = 0.08$

the crossing points of the green dotted-line and marked-lines are the approximate game payoffs with $\beta = \beta_a$ for the corresponding pairs of attack and monitor vertices (see Box A in Fig. II.3). By observing those approximate game payoffs in Fig. II.3, one has

\begin{align*}
\mathcal{J}_5(\forall v_a \in V \setminus \{v_5, v_{10}\}, v_m=6; \beta_a) & \quad (II.35) \\
< \mathcal{J}_5(v_a=10, v_m=6; \beta_a) & < \mathcal{J}_5(v_a=10, v_m=2; \beta_a). \quad (II.36)
\end{align*}
According to the definition of the saddle-point equilibrium in (II.18), the inequalities (II.36) imply that the example admits a saddle-point equilibrium \((v^*_a = v_{10}, v^*_m = v_6)\) with \(\beta = \beta_a\).

**In the second case** \(\beta = \beta_b = 0.15\)

the approximate game payoffs are the crossing points of the marked-lines and the blue dashed-line (see Box B in Fig. II.3). Those crossing points give us

\[
\mathcal{J}_5(v_{a=1}, v_{m=2}; \beta_b) = 1.4603, \quad (\text{II.37})
\]

\[
\mathcal{J}_5(v_{a=10}, v_{m=6}; \beta_b) = 1.4803, \quad (\text{II.38})
\]

\[
\mathcal{J}_5(v_{a=1}, v_{m=6}; \beta_b) = 1.4856, \quad (\text{II.39})
\]

\[
\mathcal{J}_5(v_{a=10}, v_{m=2}; \beta_b) = 1.5550. \quad (\text{II.40})
\]

From (II.40), we will examine whether a saddle-point equilibrium exists. If the detector monitors \(v_{m=2}\), the adversary simply attacks \(v_{a=10}\) to maximize the risk. But, in the case of \(v_{a=10}\), the detector can move to \(v_{m=6}\) to reduce the risk since \(\mathcal{J}_5(v_{a=10}, v_{m=6}; \beta_b) < \mathcal{J}_5(v_{a=10}, v_{m=2}; \beta_b)\). Then, the adversary can obtain a higher risk by attacking \(v_{a=1}\) instead of \(v_{a=10}\), i.e., \(\mathcal{J}_5(v_{a=1}, v_{m=6}; \beta_b) > \mathcal{J}_5(v_{a=10}, v_{m=6}; \beta_b)\). Monitoring \(v_{m=2}\) yields a lower risk for the detector, i.e., \(\mathcal{J}_5(v_{a=1}, v_{m=2}; \beta_b) < \mathcal{J}_5(v_{a=1}, v_{m=6}; \beta_b)\). The story comes back to the beginning since the adversary simply attacks \(v_{a=10}\) to
maximize the risk. The above observation implies that the example with \( \beta = \beta_b \) does not admit a saddle-point equilibrium defined in (II.18). However, the game always admits a mixed-strategy Nash equilibrium [112], which will be computed in the next subsection.

### 5.3 Computing Mixed-strategy Nash Equilibrium

We compute the mixed-strategy Nash equilibrium for the example with the cases \( \beta = \beta_a \) and \( \beta = \beta_b \). Let us denote \( \mathbb{P}(v_a; \beta) \) and \( \mathbb{P}(v_m; \beta) \), \( \beta \in \{ \beta_a = 0.08, \beta_b = 0.15 \} \) as the probabilities for attack \( v_a \) and monitor vertices \( v_m \), respectively. For convenience, we denote

\[
\mathbb{P}(v_a; \beta) = [\mathbb{P}(v_{a=1}; \beta), \ldots, \mathbb{P}(v_{a=10}; \beta)]^T, (v_a \neq v_5)
\]

and

\[
\mathbb{P}(v_m; \beta) = [\mathbb{P}(v_{m=1}; \beta), \ldots, \mathbb{P}(v_{m=10}; \beta)]^T, (v_m \neq v_5)
\]

The expected game payoff of the example w.r.t. the target vertex \( v_5 \) for attack vertex \( v_a \) and

Figure II.3: Approximate game payoff (II.25) with \( \beta = \beta_a = 0.08 \) and \( \beta = \beta_b = 0.15 \) in case the detector selects \( v_{m=2} \) or \( v_{m=6} \) and the adversary attacks \( v_{a=1} \) or \( v_{a=10} \). The other game payoffs yielded by the other choices of \( v_a \) and \( v_m \) are removed due to the ineffectiveness.
monitor vertex $v_m$ is
\[
Q_5(v_a, v_m; \beta) = \bar{P}(v_a; \beta) \top \mathcal{J_5}(v_m; \beta),
\]
where $\mathcal{J_5} = [\mathcal{J_5}(v_i, v_j; \beta)_{ij}]$ is a $9 \times 9$-game matrix, whose $ij$-entry is filled by $\mathcal{J_5}(v_a=i, v_m=j; \beta)$. Similarly to (II.18), there exits a saddle point $(v_a^*, v_m^*)$ if it satisfies
\[
Q_5(v_a, v_m^*; \beta) \leq Q_5(v_a^*, v_m^*; \beta) \leq Q_5(v_a^*, v_m; \beta),
\]
\[
\forall v_a, v_m \in \mathcal{V} \setminus \{v_r\}. \tag{II.42}
\]
The saddle point $(v_a^*, v_m^*)$ in (II.43) indicates that a deviation of selecting $v_a(v_m)$ does not increase(decrease) the optimal expected game payoff $Q_5(v_a^*, v_m^*; \beta)$. Further, since the possible choices of the detector are restricted to $\{v_2, v_6\}$, we simply obtain $\mathbb{P}(\forall v_m \in \mathcal{V} \setminus \{v_2, v_5, v_6\}; \beta) = 0$. More specifically, by using linear programming [141, Ch. 5] to compute (II.43), we receive the following optimal solution

**In the first case** $\beta = \beta_a = 0.08$

\[
\mathbb{P}^*(v_m=6; \beta_a) = 100\%, \ \mathbb{P}^*(v_m=2; \beta_a) = 0\%, \tag{II.44}
\]
\[
\mathbb{P}^*(v_a=10; \beta_a) = 100\%, \ \mathbb{P}^*(\forall v_a \in \mathcal{V} \setminus \{5, 10\}; \beta_a) = 0\%. \tag{II.45}
\]
The above optimal solution once again confirms that a pair $(v_a^* = v_{10}, v_m^* = v_6)$ is the pure saddle-point equilibrium (II.18) of the example with $\beta = \beta_a$, which was also verified in (II.36).

**In the second case** $\beta = \beta_b = 0.15$

we obtain the following optimal solution

\[
\mathbb{P}^*(v_m=6; \beta_b) \approx 94.72\%, \ \mathbb{P}^*(v_m=2; \beta_b) \approx 5.28\%, \tag{II.46}
\]
\[
\mathbb{P}^*(v_a=10; \beta_b) \approx 25.29\%, \ \mathbb{P}^*(v_a=1; \beta_b) \approx 74.71\%, \tag{II.47}
\]
\[
\mathbb{P}^*(\forall v_a \in \mathcal{V} \setminus \{1, 5, 10\}; \beta_b) = 0\%. \tag{II.48}
\]
The above optimal solution clearly shows that the example does not admit a pure saddle-point equilibrium (II.18) with $\beta = \beta_b$, which was discussed at the end of the previous subsection.

6 Conclusion

In this paper, we studied a continuous-time networked control system attacked by an adversary with uncertain system knowledge. The purpose of
the adversary was to manipulate the output of a protected target vertex by directly conducting the stealthy data injection attack on another vertex. Meanwhile, an optimal sensor placement problem was formulated such that a detector with the same uncertain system knowledge places a sensor at a vertex in order to unmask the adversary. We developed a risk-based game-theoretic framework to describe the interactions between the two players, the adversary and the detector, in the presence on probabilistic parameter uncertainty. In particular, we formulate the optimal decisions as a zero-sum game, where the game payoff is taken as a risk metric evaluated over the probabilistic uncertainty set. Due to the continuous nature of the uncertainty set, the zero-sum game could not be solved directly. Thus, we employed the scenario approach to approximately compute the game payoff over a number of samples of uncertain parameters. After approximately evaluating the game payoff for each pair of monitor and attack vertices, the mixed-strategy Nash equilibrium of the zero-sum game was also computed by linear programming. In future works, our game will be expanded to consider multiple attacks and monitor vertices. Characterizing an analytical solution to the equilibrium of the game between the adversary and the detector would also be a promising topic.

Appendix A: Proof of Lemma 1

Let us denote a tuple \((\lambda^\Delta_m, \bar{x}_m^\Delta, g_m^\Delta)\) as a zero dynamics of \(\Sigma^\Delta_m\), where a finite \(\lambda^\Delta_m\) is called a finite invariant zero of \(\Sigma^\Delta_m\). From Definition 1, one has that the tuple \((\lambda^\Delta_m, \bar{x}_m^\Delta, g_m^\Delta)\) satisfies

\[
\begin{bmatrix}
\lambda_m^\Delta I + L^\Delta & -e_a \\
e_m^\top & 0
\end{bmatrix}
\begin{bmatrix}
\bar{x}_m^\Delta \\
g_m^\Delta
\end{bmatrix}
= \begin{bmatrix}
0 \\
0
\end{bmatrix}.
\]

The above equation is rewritten as

\[
\begin{bmatrix}
(\lambda_m^\Delta - \theta_0)I + L^\Delta & -e_a \\
e_m^\top & 0
\end{bmatrix}
\begin{bmatrix}
\bar{x}_m^\Delta \\
g_m^\Delta
\end{bmatrix}
= \begin{bmatrix}
0 \\
0
\end{bmatrix},
\]

(II.50)

where \(\theta_0 \in \mathbb{R}_+\) is a uniform offset self-loop control gain. From (II.51), the finite value \((\lambda_m^\Delta - \theta_0) \in \mathbb{C}\) is an invariant zero of a new state-space model \(\Sigma_{0m}^\Delta \triangleq (-L^\Delta - \theta_0 I, e_a, e_m^\top, 0)\). For all \(\lambda_m^\Delta \in \mathbb{C}\) satisfies (II.51), the control gain \(\theta_0\) can be adjusted such that \(\theta_0 > \text{Re}(\lambda_m^\Delta)\), resulting in that \(\Sigma_{0m}^\Delta\) has no finite unstable zero. Then, the self-loop control gains \(\theta_i, i \in \{1, 2, \ldots, N\}\), in (I.2) are tuned with \(\theta_0\) such that the system \(\Sigma_{m}^\Delta\) is identical with \(\Sigma_{0m}^\Delta\). By this tuning procedure, the system \(\Sigma_{m}^\Delta\) also has no finite unstable invariant zero.
Appendix B: Proof of Theorem 2

Based on Lemma 2, the optimization problem (II.20) is feasible if and only if $\Sigma^\Delta_m$ has unstable invariant zeros that are also invariant zeros of $\Sigma^\Delta_r$. By applying the control design procedure in the proof of Lemma 1 (see Appendix A), we ensure that $\Sigma^\Delta_m$ has no finite unstable invariant zeros, which leaves us to analyze infinite zeros of those systems. Recall the equivalence between the relative degree of a SISO system and the degree of its infinite zero. Hence, a necessary condition to guarantee the feasibility of the optimization (II.20) is that the number of infinite invariant zeros of $\Sigma^\Delta_m$ is not greater than that of $\Sigma^\Delta_r$. This implies $r_{ma} \leq r_{ra}$. For sufficiency, it remains to show that if $r_{ma} \leq r_{ra}$, any infinite zeros of $\Sigma^\Delta_m$ are also infinite zeros of $\Sigma^\Delta_r$. The proof directly follows our previous results [137, Th. 7].
Title
Optimal Detector Placement in Networked Control Systems under Cyber-attacks with Applications to Power Networks

Authors
Anh Tung Nguyen, Sribalaji C. Anand, André M. H. Teixeira, and Alexander Medvedev

Edited version of
Optimal Detector Placement in Networked Control Systems under Cyber-attacks with Applications to Power Networks

Abstract
This paper proposes a game-theoretic method to address the problem of optimal detector placement in a networked control system under cyber-attacks. The networked control system is composed of interconnected agents where each agent is regulated by its local controller over unprotected communication, which leaves the system vulnerable to malicious cyber-attacks. To guarantee a given local performance, the defender optimally selects a single agent on which to place a detector at its local controller with the purpose of detecting cyber-attacks. On the other hand, an adversary optimally chooses a single agent on which to conduct a cyber-attack on its input with the aim of maximally worsening the local performance while remaining stealthy to the defender. First, we present a necessary and sufficient condition to ensure that the maximal attack impact on the local performance is bounded, which restricts the possible actions of the defender to a subset of available agents. Then, by considering the maximal attack impact on the local performance as a game payoff, we cast the problem of finding optimal actions of the defender and the adversary as a zero-sum game. Finally, with the possible action sets of the defender and the adversary, an algorithm is devoted to determining the Nash equilibria of the zero-sum game that yield the optimal detector placement. The proposed method is illustrated on an IEEE benchmark for power systems.
1 Introduction

Society’s rising demands require the development of complex and networked systems such as power grids, transportation networks, and water distribution networks. To enhance the performance and the efficiency of such systems, they might be divided into interconnected subsystems which are managed remotely through insecure communication channels. This insecure protocol possibly leaves the networked control systems vulnerable to cyber-attacks such as false data injection, covert, and replay attacks [15], inflicting serious civil damages and financial loss. In the last decade, an Iranian industrial control system and a Ukrainian power grid have witnessed the catastrophic consequences of malware such as Stuxnet [56] and Industroyer [135], respectively. Motivated by the above observation, defense strategies are needed to deal with such cyber-attacks with the purpose of protecting the networked control systems.

In this paper, we deal with the problem of optimal detector placement against a cyber-adversary in a networked control system which is represented by interconnected linear second-order agents. Every agent is regulated by its local controller through unprotected communication, which leaves the system vulnerable to malicious cyber-attacks. To guarantee a given local performance, the defender selects an agent on which to place a detector at its controller with the purpose of detecting malicious cyber-attacks. Meanwhile, the malicious adversary chooses an agent on which to inject attack signals with the purpose of maximally worsening the local performance while remaining stealthy to the defender. The contributions of this paper are the following:

1. The boundedness of the worst-case attack impact is guaranteed by a necessary and sufficient condition based on the suitable choices of control parameters and the system-theoretic property of the underlying dynamical system, namely relative degree. This condition restricts the possible choices of the defender to a subset of available agents.

2. The bounded worst-case attack impact is employed as a game payoff that enables us to translate the purposes of the defender and the adversary into a zero-sum game.

3. Based on the notions of the Nash equilibria [112], an algorithm is devoted to determining Nash equilibria of the zero-sum game that yield the best strategies of the defender and the adversary.

To illustrate the obtained results, we apply our proposed method to the IEEE 14-bus system which represents a portion of the American Power Network. We conclude this section by providing the notation used in this paper.
Notation: the sets of real positive (negative) numbers are denoted as \( \mathbb{R}_+ \) (\( \mathbb{R}_- \)); \( \mathbb{R}^n \) (\( \mathbb{C}^n \)) stands for sets of real (complex) \( n \)-dimensional vectors; every vector \( v \) and matrix \( A \) can be denoted \( v = [v_i] \) where \( v_i \) is \( i \)-th element and \( A = [a_{ij}] \) where \( a_{ij} \) is \((i, j)\) entry, respectively; \( I \) stands for an identity matrix with an appropriate dimension. Let us define \( e_i \in \mathbb{R}^n \) with all zero elements except the \( i \)-th element that is set as 1. Consider the norm \( \|x\|_2^2 = \frac{1}{T} \int_0^T \|x(t)\|_2^2 \, dt \), where we simplify the notation to \( \|x\|_2^2 \) if the time horizon \([0, T]\) is clear from the context. The space of square-integrable functions is defined as \( L_2^{[0, 1]} \), \( f: \mathbb{R}_+ \to \mathbb{R} \mid \|f\|_2^2 < 1 \) and the extended space be defined as \( L_2^{e, [0, T]} \), \( f: \mathbb{R}_+ \to \mathbb{R} \mid \|f\|_2^2 < 1 \), \( 0 < T < \infty \). Let \( G = (V, E, A) \) be a graph with the set of \( N \) vertices \( V = \{1, 2, \ldots, N\} \), the set of edges \( E \subseteq V \times V \), and the adjacency matrix \( A = [a_{ij}] \). For every \((i, j) \neq i \in E \), \( a_{ij} > 0 \) and with \((i, j) \notin E \) or \( i = j \), \( a_{ij} = 0 \). The degree of vertex \( i \) is denoted as \( \Delta_i = \sum_{j=1}^n a_{ij} \) and the degree matrix of graph \( G \) is defined as \( \Delta = \text{diag}([\Delta_i]) \), where \( \text{diag} \) stands for a diagonal matrix. The Laplacian matrix is defined as \( L = [\ell_{ij}] = \Delta - A \). Further, \( G \) is called an undirected connected graph if and only if matrix \( A \) is symmetric and the algebraic multiplicity of zero as an eigenvalue of \( L \) is one. The set of all neighbours of vertex \( i \) is denoted as \( \mathcal{N}_i = \{j \in V | (i, j) \in E\} \). We denote a set \( V_i = V \setminus \{i\} \).

2 Problem Formulation

This section first describes a networked control system under cyber-attacks. Then, we introduce the resources and the strategies of the defender and the adversary. Finally, the worst-case attack impact on the local performance is analyzed.

2.1 Networked Control System under Cyber-attacks

Consider an undirected connected graph \( G = (V, E, A) \) consisting of \( N \) agents where each agent \( i \) has a second-order state-space model:

\[
\dot{p}_i(t) = v_i(t), \tag{III.1}
\]

\[
m_i \dot{v}_i(t) = \sum_{j \in \mathcal{N}_i} \ell_{ij}(p_i(t) - p_j(t)) - h_i v_i(t) + \hat{u}_i(t), \tag{III.2}
\]

\[
y_i(t) = p_i(t), \tag{III.3}
\]

where \( p_i(t), v_i(t) \in \mathbb{R} \) are the states, \( \hat{u}_i(t) \in \mathbb{R} \) is the healthy/attacked input, and \( y_i(t) \in \mathbb{R} \) is the output of agent \( i \). The local performance of the entire network is evaluated via the output energy over a given, possibly
infinite, time horizon of a given agent $\rho \in \mathcal{V}$ denoted as $\|y_\rho\|_{L_2}^2$. Parameters $m_i, h_i \in \mathbb{R}_+$ and $\forall (i,j) \in \mathcal{E}$, $\ell_{ij} \in \mathbb{R}$ are given. We utilize the following healthy local control law, which is adapted from [22, Ch. 4], for each agent $i \in \mathcal{V}$

$$u_i(t) = -\theta_i y_i(t) + \phi_i \xi_i(t), \quad (III.4)$$

$$\dot{\xi}_i(t) = -\frac{1}{\tau} \xi_i(t) - \frac{\kappa_D}{\tau} y_i(t),$$

where $\xi_i(t)$ is a virtual control input of agent $i$ and $\theta_i, \phi_i, \kappa_D$, and $\tau \in \mathbb{R}_+$ are control parameters. If the communication channel to agent $i$ from its local controller is attacked by an adversary, $\tilde{u}_i(t) \neq u_i(t)$ which will be described in the following subsection; otherwise $\tilde{u}_i(t) = u_i(t)$. Let us employ the following assumption.

**Assumption 1.** The communication between the controller and the system of the given performance agent $\rho \in \mathcal{V}$ is protected from any cyber-attacks. Further, its controller is unavailable for the defender to place a detector. \(\triangleleft\)

For convenience, let us use the following notation in the remainder of the paper: $p(t) \triangleq [p_i(t)], v(t) \triangleq [v_i(t)], \xi(t) \triangleq [\xi_i(t)], x(t) \triangleq [x_1(t)^T, x_2(t)^T, \ldots, x_N(t)^T]^T$ where $x_i(t) \triangleq [p_i(t), v_i(t), \xi_i(t)]^T.$ $M \triangleq \text{diag}([m_i]),$ $H \triangleq \text{diag}([h_i]), \Theta \triangleq \text{diag}([\theta_i]),$ and $\Phi \triangleq \text{diag}([\phi_i]).$

**Remark 1.** The control law (III.4) will drive the system dynamics (III.1)-(III.2) to a closed-loop system that is different from the one in [22, Ch. 4], due to no interaction of states $v_i$ among agents. Thus, we will need to show how this control law stabilizes the system (III.1)-(III.2) in Section 2.3. Further, this control law plays an important role in the strategy of the defender which will be introduced in Section 3. \(\triangleleft\)

**Remark 2.** In this study, we determine the local performance of the entire network through the energy of the output measurement of the agent $\rho$ over a possibly infinite time horizon. On the other hand, other local performances can be utilized based on different applications. We leave the comparison among local performances for future work. \(\triangleleft\)

### 2.2 Resources of the Adversary and the Defender

**System knowledge:**

The malicious adversary and the defender know the location of the given protected performance agent $\rho$, the appearance of their competitors, the agent set $\mathcal{V}$, and the edge set $\mathcal{E}$. They also know all the system parameters $M$, $H$, $\Theta$, $\Phi$, $\kappa_D$, and $\tau$ as well as the detection mechanism which the defender will utilize.
Players’ possible actions:

According to \textit{Assumption 1}, each player is able to choose a single agent in $\mathcal{V}_{-\rho}$ to implement their strategies. The adversary selects the attack agent $a \in \mathcal{V}_{-\rho}$ on which to conduct a malicious attack signal $\zeta(t) \in \mathbb{R}$ on its input with the aim of maximally disrupting the output of the performance agent $\rho$ as follows:

$$\tilde{u}_i(t) = u_i(t) + \begin{cases} 0, & i \in \mathcal{V}_{-a}, \\ \zeta(t), & i \equiv a. \end{cases}$$ (III.5)

Meanwhile, the defender chooses the detection agent $d \in \mathcal{V}_{-\rho}$ on which to place a detector that generates a residual signal with the purpose of detecting the cyber-attack. These strategies of the two players are illustrated in Fig. III.1 and described in detail below.

\textbf{Remark 3.} In the scope of this study, we assume that the location of the performance agent $\rho$ is revealed to both the defender and the malicious adversary to simplify the security problem. The problem of an unknown performance agent is left for future work.

\subsection*{2.3 Strategies of the Adversary and the Defender}

Before going into those strategies, let us rewrite the closed-loop networked control system with its dynamics (III.1)-(III.3) under the control law (III.4)-(III.5) as follows

$$\dot{x}(t) = Ax(t) + E_a \zeta(t),$$ (III.6)
$$y_i(t) = C_i x(t), \quad \forall i \in \mathcal{V},$$ (III.7)
$$y_\rho(t) = C_\rho x(t),$$ (III.8)

where

$$A = \begin{bmatrix} 0 & I & 0 \\ -M^{-1}(L + \Theta) & -M^{-1} H & M^{-1} \Phi \\ 0 & -\frac{\kappa D}{\tau} I & -\frac{1}{\tau} I \end{bmatrix},$$

$$E_a = \left[ 0^T, e_a^T, 0^T \right]^T,$$

$$C_i = \left[ e_i^T, 0^T, 0^T \right].$$

\textbf{Lemma 1.} Consider the healthy system (III.6) where $\zeta(t) = 0$ and assume that $\mathcal{G}$ is an undirected connected graph. Then, the matrix $A$ in (III.6) is Hurwitz.
Figure III.1: Illustration of a networked control system with the (green) protected performance agent under cyber-attack. While the defender selects the (blue) detection agent on which to place a detector, the adversary chooses the (red) attack agent on which to conduct a cyber-attack.

**Proof:** Consider the candidate Lyapunov function

\[ V(x(t)) = x(t)^\top \bar{P} x(t), \]  

(III.9)

where

\[
\bar{P} = \begin{bmatrix}
M^{-1}(L + \Theta + \sigma H) & \sigma I & 0 \\
\sigma I & I & 0 \\
0 & 0 & \kappa_D^{-1} \tau M^{-1} \Phi
\end{bmatrix},
\]

(III.10)

The constraint (III.10) ensures that the Lyapunov function (III.9) is positive definite. Next, let us take the time-derivative of the Lyapunov function (III.9) along the trajectories of dynamics (III.6) with \( \zeta(t) = 0 \):

\[
\dot{V}(x(t)) = x(t)^\top (A^\top \bar{P} + \bar{P} A) x(t) = -x(t)^\top \bar{Q} x(t),
\]

(III.11)
where
\[
\bar{Q} = \begin{bmatrix}
2\sigma M^{-1}(L + \Theta) & 0 & -\sigma M^{-1}\Phi \\
0 & 2(M^{-1}H - \sigma I) & 0 \\
-\sigma M^{-1}\Phi & 0 & 2\kappa_D^{-1}M^{-1}\Phi 
\end{bmatrix}.
\]

The constraint (III.10) also ensures that matrix \( \bar{Q} \) is positive definite. This implies that \( \dot{V}(x(t)) \) in (III.11) is negative definite and the matrix \( A \) in (III.6) is Hurwitz.

Lemma 1 enables us to have the following assumption.

**Assumption 2.** The networked control system (III.6) is at its equilibrium \( x_e = 0 \) before being attacked.

**Defender strategy:**

At the chosen detection agent \( d \in \mathcal{V}_{-\rho} \), the defender employs a detector as follow:

\[
\begin{align*}
\dot{x}_d(t) &= A\hat{x}_d(t) + K_d\eta_d(t), \quad \hat{x}_d(0) = 0, \quad \text{(III.12)} \\
\eta_d(t) &= y_d(t) - C_d\hat{x}_d(t), \quad \text{(III.13)}
\end{align*}
\]

where \( \hat{x}_d(t) \in \mathbb{R}^N \) is the estimated state of the networked system observed at agent \( d \) and \( \eta_d(t) \in \mathbb{R} \) is the residual signal which will be used to detect cyber-attacks. Since the result in Lemma 1 implies that \((A, C_d)\) is detectable, matrix \( K_d \) can be suitably designed such that the matrix \((A - K_dC_d)\) is Hurwitz. Let us denote \( \bar{x}_d(t) \triangleq x(t) - \hat{x}_d(t) \) and \( z_d(t) \triangleq [x(t)^\top, \bar{x}_d(t)^\top]^\top \). From (III.6)-(III.8) and (III.12)-(III.13), the augmented model can be rewritten as follows:

\[
\begin{align*}
\dot{z}_d(t) &= A_dz_d(t) + \bar{E}_a\zeta(t), \quad \text{(III.14)} \\
y_{\rho}(t) &= \bar{C}_\rho z_d(t), \quad \text{(III.15)} \\
\eta_d(t) &= \bar{C}_d z_d(t), \quad \text{(III.16)}
\end{align*}
\]

where \( y_{\rho}(t) \) and \( \eta_d(t) \) are the outputs of the protected performance agent \( \rho \) and the residual signal generated by the detector placed at agent \( d \in \mathcal{V}_{-\rho} \), respectively; and

\[
A_d = \begin{bmatrix} A & 0 \\ 0 & A - K_dC_d \end{bmatrix}, \quad \bar{E}_a = \begin{bmatrix} E_a \\ E_a \end{bmatrix}, \quad \bar{C}_\rho = \begin{bmatrix} C_\rho \\ 0^\top \end{bmatrix}, \quad \bar{C}_d = \begin{bmatrix} 0^\top \\ C_d \end{bmatrix}.
\]

(III.17)

We suppose that the defender detects cyber-attacks if the energy of the residual signal over a given time horizon \([0, T]\) exceeds a given threshold \( \delta \), i.e., \( \|\eta_d\|^2_{\mathcal{L}_2[0, T]} > \delta^2 \).
Adversary strategy:

The goal of the adversary is to maximally disrupt the output of the protected performance agent $\rho$ while remaining stealthy to the detector placed at agent $d$. To this end, the adversary conducts the stealthy data injection attack, which is defined as follows. Consider the continuous-time system (III.14), (III.16), the attack input signal $\zeta(t)$ is called the stealthy data injection attack if the residual signal satisfies $\|\eta_d\|_{L^2}^2 \leq \delta^2$ where $\delta > 0$ is given and called an alarm threshold.

2.4 Worst-case Attack Impact on the Local Performance

Consider the continuous-time system (III.14)-(III.16) denoted as $\Sigma_{pd} \triangleq (A_d, \bar{E}_a, [\bar{C}_\rho^T, \bar{C}_d^T]^T, 0)$. The malicious adversary attacks the input of the attack agent $a$ with the purpose of maliciously maximizing impact on the output of the given performance agent $\rho$ while remaining undetected by the defender. This adversary purpose is translated into the following non-convex optimal control problem [124, Sec. 4]:

$$
\gamma^*_{\rho}(a, d) \triangleq \sup_{\zeta \in L_{2e}, z_d(0) = 0} \|y_{\rho}\|_{L^2}^2 \\
\text{s.t.} \quad \|\eta_d\|_{L^2}^2 \leq \delta^2,
$$

which has the dual problem as follows:

$$
\inf_{\gamma_{\rho} \in \mathbb{R}^+} \left[ \sup_{\zeta \in L_{2e}, z_d(0) = 0} \left( \|y_{\rho}\|_{L^2}^2 - \gamma_{\rho} \delta^{-2} \|\eta_d\|_{L^2}^2 \right) + \gamma_{\rho} \right].
$$

The dual problem (III.19) is feasible if $\|y_{\rho}\|_{L^2}^2 - \gamma_{\rho} \delta^{-2} \|\eta_d\|_{L^2}^2 \leq 0, \forall \zeta \in L_{2e}$ and $z_d(0) = 0$, which results in the following optimization problem:

$$
\gamma^*_{\rho}(a, d) \triangleq \min_{\gamma_{\rho} \in \mathbb{R}^+} \gamma_{\rho} \\
\text{s.t.} \quad \|y_{\rho}\|_{L^2}^2 \leq \gamma_{\rho} \delta^{-2} \|\eta_d\|_{L^2}^2, \forall \zeta \in L_{2e},
$$

$$
z_d(0) = 0.
$$

The strong duality can be proven by utilizing S-Procedure [126, Ch. 4]. Recalling the key results in dissipative system theory for linear systems with quadratic supply rates [127], the constraint of (III.20) can be translated into a linear matrix inequality [124, Prop. 1] as follows:

$$
\gamma^*_{\rho}(a, d) \triangleq \min_{\gamma_{\rho} \in \mathbb{R}^+, \mathbf{F} = \mathbf{F}^\top \geq 0} \gamma_{\rho} \\
\text{s.t.} \quad R(\Sigma_{pd}, \mathbf{F}, \gamma_{\rho}) \leq 0,
$$
3. Optimal Detector Placement

where

\[
R(\Sigma_{\rho d}, F, \gamma_\rho) \triangleq \begin{bmatrix}
A_d^T F - FA_d & F\bar{E}_a \\
\bar{E}_d^T F & 0
\end{bmatrix}
- \begin{bmatrix}
\gamma_\rho \delta^{-2} \bar{C}_d \bar{C}_d^T & -\bar{C}_\rho \bar{C}_\rho^T \\
0 & 0
\end{bmatrix}.
\]

The convex optimization problem (III.21) can be solved numerically efficiently to obtain the worst-case attack impact on the local performance measured at the performance agent \(\rho\). With this worst-case attack impact, we are ready to state the following problem that will be addressed in the remainder of the paper.

**Problem 1.** Given a protected performance agent \(\rho\) and an arbitrary attack agent \(a \in \mathcal{V}_-\rho\), select a detection agent \(d \in \mathcal{V}_-\rho\) on which to place a detector that minimizes the worst-case attack impact on the performance agent \(\rho\).

**Remark 4.** The two strategic players, which are the adversary and the defender, have symmetric information as described in Section 2.1. They know the action space of their competitors instead of actual actions. Therefore, we assume that the two players perform their actions based on such available information at the same time, resulting in a non-cooperative game [102] which will be presented in the following section.

3 Optimal Detector Placement

We first present a necessary and sufficient condition for the defender to ensure that the worst-case attack impact on the local performance is bounded. This condition restricts the possible choices of the defender to a subset of available agents. Then, we translate Problem 1 into a zero-sum game between two strategic players, namely the malicious adversary and the defender. Finally, within the framework of zero-sum games, an algorithm is proposed to find Nash equilibria that yield the best strategies for the two players.

3.1 Boundedness of the Worst-case Attack Impact on the Local Performance

Let us evaluate the attack impact of the adversary through the optimization problem (III.18). The feasibility of the optimization problem (III.18) is related to invariant zeros of \(\Sigma_\rho = (A_d, \bar{E}_a, \bar{C}_\rho, 0)\) and \(\Sigma_d = (A_d, \bar{E}_a, \bar{C}_d, 0)\), which are defined as follows.
Definition 1. (Invariant zeros) Consider the strictly proper system \( \bar{\Sigma} \triangleq (\bar{A}, \bar{B}, \bar{C}, 0) \) with \( \bar{A}, \bar{B}, \) and \( \bar{C} \) are real matrices with appropriate dimensions. A tuple \((\bar{\lambda}, \bar{x}, \bar{g}) \in \mathbb{C} \times \mathbb{C}^N \times \mathbb{C}\) is a zero dynamics of \( \bar{\Sigma} \) if it satisfies

\[
\begin{bmatrix}
\lambda I - \bar{A} & -\bar{B} \\
\bar{C} & 0
\end{bmatrix}
\begin{bmatrix}
\bar{x} \\
\bar{g}
\end{bmatrix}
= \begin{bmatrix}
0 \\
0
\end{bmatrix}, \quad \bar{x} \neq 0.
\] (III.22)

In this case, a finite \( \bar{\lambda} \) is called a finite invariant zero of \( \bar{\Sigma} \). Further, the strictly proper system \( \bar{\Sigma} \) always has at least one invariant zero at infinity [128].

More specifically, let us state the following lemma.

Lemma 2. [123, Th. 2] Consider the two following continuous time systems \( \Sigma_\rho = (A_d, E_a, \bar{C}_d, 0) \) and \( \Sigma_d = (A_d, E_a, \bar{C}_d, 0) \). The optimization problem (III.18) is feasible if and only if the unstable invariant zeros of \( \Sigma_d \) are also invariant zeros of \( \Sigma_\rho \).

Inspired by the result in Lemma 2 and the definition of invariant zeros in Definition 1, we will investigate both finite and infinite invariant zeros of the two systems \( \Sigma_d \) and \( \Sigma_\rho \).

Finite invariant zeros:

Let us state the following lemma that considers the finite invariant zeros.

Lemma 3. Consider the system \( \Sigma_m = (A, E_a, C_d, 0) \) defined in (III.6), (III.7) and, for \( \lambda_d \in \mathbb{C} \), define

\[
\mathcal{Q}(\lambda_d) = L + \Theta + \lambda_d^2 M + \lambda_d H + \frac{\lambda_d \kappa_D}{\tau \lambda_d + 1} \Phi.
\] (III.23)

The system \( \Sigma_m \) has a finite zero at \( \lambda_d \in \mathbb{C} \) if, and only if, \( \mathcal{Q}(\lambda_d) \) is nonsingular and \( e_d^T \mathcal{Q}(\lambda_d)^{-1} e_a = 0 \)

Proof: The proof is postponed to Appendix A.

The above result establishes the equivalence between the existence of an invariant zero of \( \Sigma_m \) at \( \lambda_d \in \mathbb{C} \) and the matrix \( \mathcal{Q}(\lambda_d)^{-1} \) having a zero at the entry \( [\mathcal{Q}(\lambda_d)^{-1}]_{da} \). Next, we leverage this result to show that the detector \( \Sigma_d = (A_d, \bar{E}_a, \bar{C}_d, 0) \) has no unstable zero on the real line.

Lemma 4. Consider system dynamics (III.14),(III.16) represented by \( \Sigma_d = (A_d, \bar{E}_a, \bar{C}_d, 0) \) and assume that \( \mathcal{G} \) is an undirected connected graph. Then, for any choice of attack agent \( a \in \mathcal{V}_-\rho \) and detection agent \( d \in \mathcal{V}_-\rho \), the corresponding system \( \Sigma_d \) has no finite invariant zero on the positive real line.
3. Optimal Detector Placement

Proof: The proof is postponed to Appendix B.

Unfortunately, the result in Lemma 4 cannot be directly extended to consider complex invariant zeros on the right half-plane. The extension on how to deal with complex invariant zeros is left for future work. In the remainder of the paper, we assume that the system $\Sigma_d$ has no finite, complex unstable zeros.

**Infinite invariant zeros:**

We now investigate the infinite invariant zeros of the systems $\Sigma_\rho$ and $\Sigma_d$. In the investigation, we make use of known results connecting infinite invariant zeros and the relative degree (see [35, Ch. 13]) of a linear system. Let us denote $r(\rho,a)$ and $r(d,a)$ as the relative degrees of $\Sigma_\rho$ and $\Sigma_d$, respectively. By following our existing result related to those infinite zeros [137, Th. 7], the infinite zeros of $\Sigma_d$ are also the infinite zeros of $\Sigma_\rho$ if and only if the following condition holds

$$r(d,a) \leq r(\rho,a).$$

(III.24)

The following theorem presents the necessary and sufficient condition which ensures that the optimization problem (III.18) admits a finite solution.

**Theorem 1.** Consider a networked control system associated with an undirected connected graph $\mathcal{G} = (V, E, A)$ and two continuous-time systems $\Sigma_\rho = (A_d, \bar{E}_a, \bar{C}_\rho, 0)$ and $\Sigma_d = (A_d, \bar{E}_a, \bar{C}_d, 0)$. Suppose $\Sigma_\rho$ and $\Sigma_d$ have relative degrees $r(\rho,a)$ and $r(d,a)$, respectively. The optimization problem (III.18) admits a finite solution if, and only if, the condition (III.24) holds and the parameters $\theta_i, \phi_i, \kappa_D, \tau \in \mathbb{R}_+$ are such that, for every $\lambda_d \in \mathbb{C}$ on the right half plane, the matrix $Q(\lambda_d)^{-1}$ has no zero entries.

Proof: Following from Lemma 3, a suitable choice of parameters $\theta_i, \phi_i, \kappa_D, \tau \in \mathbb{R}_+$ ensures that the system $\Sigma_d$ has no finite unstable zero for any choice of $a$ and $d$ if, and only if, the matrix $Q(\lambda_d)^{-1}$ has no zero entries for every $\lambda_d \in \mathbb{C}$ on the right half plane. This result and the condition (III.24) fulfill the necessary and sufficient condition in Lemma 2 which guarantees that the optimization problem (III.18) admits a finite solution.

For every arbitrary attack agent $a \in V_\rho$, let us define the detection set $\mathcal{D} \subseteq V_\rho$ containing agents which satisfy the necessary and sufficient condition in Theorem 1. The possible action set of the defender will be restricted to the detection set $\mathcal{D}$.

**Assumption 3.** The detection set $\mathcal{D}$ is not empty, i.e., $\mathcal{D} = \{d_1, d_2, \ldots, d_{|\mathcal{D}|}\}$ where $|\mathcal{D}| \geq 1$.  

\[\triangle\]
Assumption 3 enables the defender to optimally select an agent on which to place the observer (III.12)-(III.13) with the purpose of detecting the cyber-attack conducted by the adversary. How the defender selects the optimal detector placement will be addressed by a game-theoretic approach, which has been widely used in [121,142], in the next subsection.

Remark 5. To compute a detection set $\mathcal{D}$ for a given undirected connected graph $\mathcal{G}$, we can utilize an undirected unweighted graph $\mathcal{G}'$ such that $\mathcal{G}$ and $\mathcal{G}'$ have the same topology. Through the graph $\mathcal{G}'$, we adopt the result in [137, Lem. 8] to characterize candidate detection agents that fulfill the condition (III.24) for every attack agent $a \in \mathcal{V}_{-\rho}$. Such found agents also satisfy the condition (III.24) for every attack agent $a \in \mathcal{V}_{-\rho}$ in case we consider $\mathcal{G}'$. <

3.2 Game-theoretic Approach to Optimal Detector Placement

According to Theorem 1, since the optimization problem (III.18) is feasible for all the possible choices of the attack agent $a \in \mathcal{V}_{-\rho}$ and the detection agent $d \in \mathcal{D}$, we employ the worst-case attack impact (III.18) as a game payoff that enables us to translate Problem 1 into a zero-sum game between the malicious adversary and the defender. While the adversary wants to maximize the game payoff, the defender desires to minimize the same game payoff, i.e., Problem 1 is represented as follows

$$\max_{a \in \mathcal{V}_{-\rho}} \min_{d \in \mathcal{D}} \gamma^*_\rho(a, d) < \infty. \tag{III.25}$$

For every pair of an attack agent $a \in \mathcal{V}_{-\rho}$ and a detection agent $d \in \mathcal{D}$, we find the corresponding game payoff $\gamma^*_\rho(a, d)$ by solving the convex optimization problem (III.21). Then, the existence of a pure Nash equilibrium $(a^*, d^*)$ is equivalent to concluding that the following equality holds

$$\min_{d_i \in \mathcal{D}} [\alpha_i] = \max_{a_i \in \mathcal{V}_{-\rho}} [\beta_i], \tag{III.26}$$

where $\alpha_i = \max_{a_j \in \mathcal{V}_{-\rho}} \gamma^*_\rho(a_j, d_i)$; $\beta_i = \min_{d_j \in \mathcal{D}} \gamma^*_\rho(a_i, d_j)$. The pure optimal detector placement at the detection agent $d_i^*$ has the same index $i$ with $\alpha_i^*$ where

$$\alpha_i^* = \arg\min_{d_i \in \mathcal{D}} [\alpha_i]. \tag{III.27}$$

The failure of the condition (III.26) implies that no pure Nash equilibrium exists [112]. However, the game always admits a mixed-strategy Nash equilibrium which will be computed in the remainder of this section.
Algorithm 1 Optimal detector placement

**Input:** possible detection set $\mathcal{D}$ and attack set $\mathcal{V}_{-\rho}$.

**Output:** optimal detector placement

1. For every pair of $a \in \mathcal{V}_{-\rho}$ and $d \in \mathcal{D}$, solve (III.21) to obtain the corresponding game payoff $\gamma^*_p(a,d)$.
2. **if** condition (III.26) is fulfilled **then**
   - return a pure detector placement at $d^*_i$ where its index $i$ is determined by (III.27).
3. **else** solve (III.28) to obtain $P^*$ and $Q^*$
   - return a mixed-strategy optimal detector placement represented by $Q^*$.
4. **end if**

Let us denote the probability of an agent $a \in \mathcal{V}_{-\rho}$ that is attacked by the adversary as $p_a \in [0;1]$; the probability of an agent $d \in \mathcal{D}$ that is employed to implement the detector (III.12)-(III.13) by the defender as $q_d \in [0;1]$; vectors $P = [p_i]$ and $Q = [q_i]$. According to [112], the optimal mixed-strategy $(P^*,Q^*)$ of the adversary and the defender can be found as follows:

$$
J^*_p(P^*,Q^*) = \min_P \max_Q \sum_{a \in \mathcal{V}_{-\rho}} \sum_{d \in \mathcal{D}} p_a \gamma^*_p(a,d) q_d,
$$

s.t. \( \sum_{a \in \mathcal{V}_{-\rho}} p_a = 1, \sum_{d \in \mathcal{D}} q_d = 1, \)

Inspired by [141, Ch. 5], the min-max optimization problem (III.28) can be efficiently solved by linear programming. Let us summarize the procedure how to determine the optimal detector placement in Algorithm 1. In the following section, we will demonstrate our proposed Algorithm 1 in a case study of power systems.

4 A Case Study

In this section, we demonstrate our obtained results via the IEEE 14-bus system (Fig. III.2). The system includes 14 buses and 20 transmission lines. The behavior of a bus $i \in \{1,2,\ldots,14\}$ can be described by the so-called swing equation [22]:

$$
m_i \ddot{p}_i + h_i \dot{p}_i - \ddot{u}_i(t) = - \sum_{j \in N_i} P_{ij},
$$

where $m_i$ and $h_i$ are the inertia and damping coefficients, respectively, $\ddot{u}_i(t)$ is the healthy/attacked mechanical input power and $P_{ij}$ is the active power
flow from bus $j$ to bus $i$. Considering that there are no power losses and $V_i = |V_i|e^{jp_i}$ ($j^2 = -1$) and $p_i$ be the complex voltage and the phase angle of the bus $i$, respectively. The active power flow $P_{oij}$ from bus $j$ to bus $i$ is given by

$$P_{oij} = -\ell_{ij} \sin(p_i - p_j), \quad (III.30)$$

where $-\ell_{ij} \in \mathbb{R}_+$ is the susceptance of the power transmission line connecting bus $i$ with bus $j$. Those parameters consisting of line susceptance $\ell_{ij}$, inertia $m_i$, and damping $h_i$ can be found at [143]. Since the phase angles usually are close, we can linearize (III.30) and rewrite the dynamics (III.29) of bus $i$ as follows

$$m_i \ddot{p}_i + h_i \dot{p}_i = \sum_{j \in \mathcal{N}_i} \ell_{ij} (p_i(t) - p_j(t)) + \tilde{u}_i(t), \quad (III.31)$$

which is equivalent to the ones in (III.1)-(III.3) we investigated in the previous sections. Suppose that the mechanic power input $\tilde{u}_i(t)$ coincides with the one in (III.4)-(III.5).

Next, we present numerical results by using Algorithm 1. Suppose that bus 12 (coded green) is the protected performance bus. The certain alarm threshold is selected as $\delta^2 = 2.6$. Recalling Remark 5, we characterize the possible detection set $\mathcal{D} = \{6, 13\}$ containing buses that fulfill the condition (III.24). The control parameters are selected as follows: $\theta_i = 1.5$, $\phi_i = 2.2$, $\kappa_d = 2$, and $\tau = 0.4 \ \forall i \in \mathcal{V}$. Those control parameters fulfill the necessary and sufficient condition in Theorem 1 to ensure that the game payoff is bounded. At the step 1 of Algorithm 1, for every pair of $a \in \mathcal{V}_{-p}$ and $d \in \mathcal{D}$, we solve (III.21) by using CVX [144] to obtain the following result: $\alpha = [4.7449, 4.3917]$ and $\beta = [2.4494, 2.5561, 2.6185, 2.5585, 2.4198, 2.3087, 2.5199, 2.5257, 2.4695, 2.4673, 2.3705, 2.0717, 2.2119]$. At the step 2 of Algorithm 1, since 4.3917 = min[$\alpha_i$] $\neq$ max[$\beta_i$] = 2.6185, the condition (III.26) fails, implying that the zero-sum game does not admit a pure Nash equilibrium. Then, we move to the step 3 to find a mixed-strategy $J_p^* = 3.3757$ at $p_6^* = 0.562$, $p_{13}^* = 0.438$, $p_{i \in \mathcal{V} \setminus \{6, 12, 13\}}^* = 0$, $q_6^* = 0.4878$, and $q_{13}^* = 0.5122$.

Let us assume that the defender places a detector at the local controller of bus 13 and the adversary conducts the stealthy data injection attack on the input of bus 6. By observing the output energy of the detection bus 13 in Fig. III.3a which is under the certain threshold $\delta^2$, the attack signal in Fig. III.3b is stealthy to the detector placed at bus 13. However, the adversary only causes a bounded malicious attack impact on the output energy of the local performance bus 12 (see Fig. III.3a). The adversary cannot increase the amplitude of the attack signal to gain its attack impact.
on the output energy of the performance bus 12 since the energy output of the detection bus 13 crosses the certain threshold $\delta^2 = 2.6$, which enables the defender to detect the cyber-attack.

5 Conclusion

In this paper, we addressed the problem of optimal detector placement in a networked control system under cyber-attacks. First, we presented the necessary and sufficient condition, which is related to the suitable choice of control parameters and the relative degree of dynamic systems, to ensure that the worst-case attack impact on the local performance is bounded. This condition restricts possible detection agents to a subset of available agents. Then, the problem of optimal detector placement was formulated as
Figure III.3: (a) Output energy of the performance bus 12 and the detection bus 13; (b) Attack signal $\zeta(t)$ conducted on the input of bus 6.

A zero-sum game between the defender and the adversary where the game payoff was represented by the bounded worst-case attack impact on the local performance. Finally, an algorithm was devoted to finding the optimal detector placement. The obtained results were illustrated by an actual case study of power systems, namely the IEEE 14-bus system.
Appendix A: Proof of Lemma 3

Let us denote a tuple \((\lambda_d, \bar{x}_d, g_d) \in \mathbb{C} \times \mathbb{C}^{3N} \times \mathbb{C}\) as a zero dynamics of \(\Sigma_m\) where \(\lambda_d\) is a finite invariant zero of \(\Sigma_m\) and \(\bar{x}_d = [\nu_1^T, \nu_2^T, \nu_3^T]^T\) where \(\nu_1, \nu_2, \nu_3 \in \mathbb{C}^N\). From the condition (III.22) in Definition 1, \((\lambda_d, \bar{x}_d, g_d)\) of \(\Sigma_m\) satisfies

\[
\begin{bmatrix}
\lambda_d I & -I & 0 & 0 \\
M^{-1}(L + \Theta) & \lambda I + M^{-1}H & -M^{-1}\Phi & e_a \\
0 & \frac{\kappa_D}{\tau} I & (\lambda + \frac{1}{\tau}) I & 0 \\
e_d^T & 0 & 0 & \bar{g}
\end{bmatrix}
\begin{bmatrix}
\nu_1 \\
\nu_2 \\
\nu_3 \\
\bar{g}
\end{bmatrix} = 0.
\]

Solving the above system of equations partially for \(\nu_3\) and \(\nu_2\), as functions of \(\nu_1\), and then for \(\nu_1\) as a function of \(\bar{g}\) gives us the remaining equation

\[
e_d^T M Q(\lambda_d)^{-1} \frac{\lambda_d \kappa_D}{\tau \lambda_d + 1} e_a \bar{g} = 0,
\]

(III.32)

\[
Q(\lambda_d) = L + \Theta + \lambda_d^2 M + \lambda_d H + \frac{\lambda_d \kappa_D}{\tau \lambda_d + 1} \Phi.
\]

From (III.32), given the positivity of the parameters \(\theta_i, \phi_i, \kappa_D, \) and \(\tau \in \mathbb{R}^+\), it follows that \((\lambda_d, \bar{x}_d, g_d) \in \mathbb{C} \times \mathbb{C}^{3N} \times \mathbb{C}\) is a zero dynamics of \(\Sigma_m\) with \(\bar{g} \neq 0\) if, and only if, \(e_d^T M Q(\lambda_d)^{-1} e_a = [Q(\lambda_d)^{-1}]_{da} = 0\) where matrix \(M\) is a diagonal positive definite matrix.

Appendix B: Proof of Lemma 4

Let us consider the continuous-time systems \(\Sigma_{mo} = (A - K_d C_d, E_a, C_d, 0)\), \(\Sigma_m = (A, E_a, C_d, 0)\), and \(\Sigma_o = (A - K_d C_d, K_d, -C_d, 1)\). From the condition (III.22) and the structure of matrices (III.17), the set of invariant zeros of the system \(\Sigma_d\) is the union of the set of eigenvalues of matrix \(A\) and the set of invariant zeros of the system \(\Sigma_{mo}\). Thanks to Lemma 1, all the eigenvalues of matrix \(A\) is stable. It remains to investigate invariant zeros of the system \(\Sigma_{mo}\). On the other hand, we have the set of invariant zeros of the \(\Sigma_{mo}\) is contained by the union of the set of invariant zeros of \(\Sigma_o\) and the set of invariant zeros of \(\Sigma_m\). By following Definition 1, the condition (III.22) gives us that the invariant zeros of the system \(\Sigma_o\) coincides with eigenvalues of matrix \(A\) in (III.6), which are stable, no matter how the matrix \(K_d\) in the observer (III.12) is designed. In the end, we only need to investigate invariant zeros of \(\Sigma_m\). The proof follows from a contradiction argument. Let us denote a tuple \((\lambda_d, \bar{x}_d, g_d) \in \mathbb{C} \times \mathbb{C}^{3N} \times \mathbb{C}\) as a zero dynamics of \(\Sigma_m\) where \(\lambda_d\) is assumed to be real and positive.
For every real positive value $\lambda_d$, the matrix $Q(\lambda_d)$ in (III.23) is positive definite, yielding that $Q(\lambda_d)$ is non-singular and $-Q(\lambda_d)$ is Hurwitz. Further, since matrix $Q(\lambda_d)$ represents a strongly connected graph $\mathcal{G}$ with added self-loops, it is irreducible [145, Ch. 6]. Obviously, $-Q(\lambda_d)$ is also a Metzler matrix. According to [146, Th. 10.3], $Q(\lambda_d)^{-1}$ is a positive matrix whose all entries are real positive, that is, $[Q(\lambda_d)^{-1}]_{da} > 0$ for all vertices $d$ and $a$. Following the result of Lemma 3, we conclude that a real positive value $\lambda_d$ cannot be a zero of the system $\Sigma_m$, thus concluding the proof.
Title
Security Allocation in Networked Control Systems under Stealthy Attacks

Authors
Anh Tung Nguyen, André M. H. Teixeira, and Alexander Medvedev

Edited version of
Security Allocation in Networked Control Systems under Stealthy Attacks

Abstract

This paper considers the problem of security allocation in a networked control system under stealthy attacks in which the system is comprised of interconnected subsystems represented by vertices. A malicious adversary selects a single vertex on which to conduct a stealthy data injection attack to maximally disrupt the local performance while remaining undetected. On the other hand, a defender selects several vertices on which to allocate defense resources against the adversary. First, the objectives of the adversary and the defender with uncertain targets are formulated in probabilistic ways, resulting in an expected worst-case impact of stealthy attacks. Next, we provide a graph-theoretic necessary and sufficient condition under which the cost for the defender and the expected worst-case impact of stealthy attacks are bounded. This condition enables the defender to restrict the admissible actions to a subset of available vertex sets. Then, we cast the problem of security allocation in a Stackelberg game-theoretic framework. Finally, the contribution of this paper is highlighted by utilizing the proposed admissible actions of the defender in the context of large-scale networks. A numerical example of a 50-vertex networked control system is presented to validate the obtained results.

1 Introduction

Networked control systems are ubiquitous in modern societies, with examples including transportation networks, power systems, and water distribution networks. These systems, utilizing non-proprietary information and communication technologies such as public Internet and wireless communi-
cation, are exposed to the threat of cyber attacks [15, 56, 135], which can cause severe financial and societal consequences. For instance, an Iranian industrial control system and a Ukrainian power grid have witnessed the catastrophic consequences of malware such as Stuxnet in 2010 [56] and Industroyer in 2016 [135], respectively. Thus, in light of these alarming realities, the issue of security has acquired unprecedented significance in the realm of control systems.

In terms of cyber attacks on control systems, deception attacks that undermine the integrity of control systems have emerged as an area of increasing scholarly interest. For example, Pang and Liu have proposed an encryption-based predictive control mechanism to counteract and mitigate such attacks [100]. Another form of deception attacks, replay attacks, has been unmasked by physical watermarking [57, 80] and multiplicative watermarking [53]. Meanwhile, the development of stealthy attacks on control systems has been made to evade the most advanced detection schemes [8, 48, 62, 65].

Upon review of the above existing studies [8, 48, 53, 57, 62, 65, 80, 100], it is noticed that they have concentrated on secure estimation and secure control from either the defender’s or the adversary’s perspective. Nonetheless, it is crucial to note that both parties are confronted with similar challenges, as the defender has limited resources to counteract malicious activities, while the adversary also faces energy and detectability constraints when executing attacks. As a result, addressing the security problem within a unified framework that encompasses both the defender and the adversary is of utmost importance.

Game theory offers a unified framework to consider the objectives and actions of both strategic players, namely the defender and the adversary [112]. It also allows us to deal with the robustness and security of cyber-physical systems within the common well-defined framework of $H_{\infty}$ robust control design [137]. Further, many other concepts of games describing networked systems subjected to cyber attacks such as matrix games [129, 137, 147], dynamic games [130], stochastic games [131], and network monitoring games [136] have been recently studied. Recent studies [119, 137, 147, 148] have utilized the common concept of zero-sum games to address the problem of input attacks on cyber-physical systems. The investigation of control systems exposed to cyber attacks has been extensively studied through game theoretic approaches [130, 131, 136]. However, these approaches have not accounted for the deployment of detectors in an effort to increase the detection of cyber attacks. This creates a significant gap in knowledge which must be addressed in order to enhance security measures.

One such effort to close the aforementioned gap has been presented in a game-theoretic formulation outlined by Pirani et al. [121]. The game payoff
in [121] has been formulated by combining the maximum $L_2$ gains of multiple outputs with respect to a single input representing the attack signal. On the one hand, these multiple $L_2$ gains are evaluated separately and thus may be attained for different optimal input signals. Further, the utilization of a maximum gain for characterizing the detectability corresponds to an optimistic perspective, where the adversary attempts to maximize the energy of the detection output, instead of the opposite. Therefore, in order to address the critical issue of cyber security and develop a security metric against cyber attacks, it is imperative to thoroughly investigate the optimal placement of sensors in a networked system to minimize the impact of cyber attacks while maintaining maximum detectability.

Additionally, the above existing studies [121, 129, 130, 136, 137, 147, 148] investigated the security problem by letting the defender and the adversary select their actions simultaneously. However, this formulation may not always be applicable in practical situations where an adversary probably moves after observing the action of the defender. To deal with this limitation, a game-theoretic Stackelberg framework [102] offers a more practical solution. In the framework, after analyzing possible attack scenarios, the defender, so-called the leader, has the power to select and announce their

Figure IV.1: An illustration of a networked control system with the (green) performance vertex under a stealthy attack. While the defender selects the (blue) monitor vertices on which to place a sensor at each monitor vertex, the adversary selects the (red) attack vertex on which to conduct a stealthy attack.
action first, knowing that the malicious adversary bases their actions on the leader’s decision. Then, the malicious adversary, so-called the follower, finds the best response to the defender’s action.

This paper considers a continuous-time networked control system, associated with an undirected connected graph, under stealthy attacks involving two strategic agents: a malicious adversary and a defender. The system is comprised of multiple interconnected one-dimensional subsystems, referred to as vertices, in which a single performance vertex is selected to represent the local performance of the entire network. The purpose of the adversary is to maliciously degrade the local performance without being detected. To pursue this purpose, the adversary selects one vertex on which to launch a stealthy data injection attack on its input. Meanwhile, the defender allocates defense resources by selecting a set of monitor vertices to measure their outputs with the aim of alleviating the attack impact. Given the strategic nature of both agents, we investigate the optimal selection of the monitor vertices using the Stackelberg game-theoretic approach described above. By leveraging the concept of the Stackelberg game in [102], we can elucidate the complex interplay between the two agents and identify their best actions. Figure IV.1 visualizes the above-defined game in a networked control system. The contributions of this paper are the following:

1. A novel objective function, the expected output-to-output gain, is proposed to capture the expected worst-case impact of stealthy attacks with uncertain performance vertex.

2. We cast the security allocation problem in a Stackelberg game-theoretic framework with the defender as the leader and the malicious adversary as the follower.

3. We propose a control design for which we provide a graph-theoretic necessary and sufficient condition under which the defender guarantees the boundedness of the cost and the expected worst-case impact of stealthy attacks.

4. Leveraging the uncertainty of the attack and performance vertices, we show that the necessary and sufficient condition in 3) restricts the admissible choice of monitor sets to be dominating sets of the graph.

5. We highlight the advantage of the proposed security allocation scheme in the context of large-scale networks.

The remainder of this paper is organized as follows. Section 2 provides the description of a networked control system under stealthy attacks, the worst-case impact of stealthy attacks caused by the malicious adversary,
2. Problem Formulation

In this section, we first describe a networked control system under stealthy attacks in the presence of a defender and a malicious adversary. The malicious adversary conducts a stealthy data injection attack on the input of a vertex with the purpose of degrading the local performance of the system.

Notation: the set of real positive numbers is denoted as $\mathbb{R}_+$; $\mathbb{R}^n$ and $\mathbb{R}^{n \times m}$ stand for sets of real $n$-dimensional vectors and $n$-row $m$-column matrices, respectively. Let us define $e_i \in \mathbb{R}^n$ with all zero elements except the $i$-th element is set as 1. A continuous linear time-invariant (LTI) system with the state-space model $\dot{x}(t) = \bar{A}x(t) + \bar{B}u(t)$, $y(t) = \bar{C}x(t) + \bar{D}u(t)$ is denoted as $\bar{\Sigma} \triangleq (\bar{A}, \bar{B}, \bar{C}, \bar{D})$. Consider the norm $\|x\|_{L_2[0,T]}^2 \triangleq \frac{1}{T} \int_0^T \|x(t)\|_2^2 \text{dt}$, we simplify the notation $\|x\|_{L_2}^2$ if the time horizon $[0,T]$ is clear from the context. The space of square-integrable functions is defined as $L_2 \triangleq \{ f: \mathbb{R}_+ \rightarrow \mathbb{R} \mid \|f\|_{L_2[0,\infty]}^2 < \infty \}$ and the extended space be defined as $L_2e \triangleq \{ f: \mathbb{R}_+ \rightarrow \mathbb{R} \mid \|f\|_{L_2[0,T]}^2 < \infty, \forall \ 0 < T < \infty \}$. For a vector $x \in \mathbb{R}^n$, $\|x\|_0$ denotes the number of non-zero elements in the vector $x$. Let $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, A)$ be a graph with the set of $N$ vertices $\mathcal{V} = \{1, 2, \ldots, N\}$, the set of edges $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$, and the adjacency matrix $A = [a_{ij}]$. For any $(i,j) \in \mathcal{E}$, $i \neq j$, the element of the adjacency matrix $a_{ij}$ is positive, and with $(i,j) \notin \mathcal{E}$ or $i = j$, $a_{ij} = 0$. The degree of vertex $i$ is denoted as $\Delta_i = \sum_{j=1}^{n} a_{ij}$ and the degree matrix of graph $\mathcal{G}$ is defined as $\Delta = \text{diag}(\Delta_1, \Delta_2, \ldots, \Delta_N)$, where $\text{diag}$ stands for a diagonal matrix. The Laplacian matrix is defined as $L = [\ell_{ij}] = \Delta - A$. Further, $\mathcal{G}$ is called an undirected connected graph if and only if matrix $A$ is symmetric and the algebraic multiplicity of zero as an eigenvalue of $L$ is one. The set of all neighbours of vertex $i$ is denoted as $\mathcal{N}_i = \{ j \in \mathcal{V} \mid (i,j) \in \mathcal{E} \}$. We denote a subset set $\mathcal{V}_{-i} \triangleq \mathcal{V} \setminus \{i\}$. 

2 Problem Formulation

In this section, we first describe a networked control system under stealthy attacks in the presence of a defender and a malicious adversary. The malicious adversary conducts a stealthy data injection attack on the input of a vertex with the purpose of degrading the local performance of the system.
Meanwhile, the defender desires to alleviate the attack impact on the system through placing sensors at several vertices. In the remainder of this section, we analyze the worst-case impact of stealthy attacks on the system based on the output-to-out gain security metric, which will be utilized to formulate the objectives of the adversary and the defender.

2.1 Networked Control System under Stealthy Attacks

Consider an undirected connected graph $G = (V, E, A)$ with $N$ vertices, the state-space model of a one-dimensional vertex $i$ is described:

$$\dot{x}_i(t) = u_i(t), \quad i \in \{1, 2, \ldots, N\},$$

(IV.1)

where $x_i(t) \in \mathbb{R}$ is the state of vertex $i$. The local performance of the entire network is evaluated via the output energy of a vertex $\rho \in V$ over a given, possibly infinite, time horizon denoted as $\|x_\rho\|^2_{L_2}$.

Each vertex $i \in V$ is controlled by the following control law:

$$u_i(t) = -\theta_i x_i(t) + \sum_{j \in N_i} (x_j(t) - x_i(t)),$$

(IV.2)

where $\theta_i \in \mathbb{R}_+$ is an adjustable self-loop control gain at vertex $i$. This self-loop control gain will be used to improve the security of the entire network later in this paper. For convenience, let us denote $x(t)$ as the state of the entire network, $x(t) = [x_1(t), x_2(t), \ldots, x_N(t)]^\top$.

To get prepared for facing malicious activities, the defender selects a subset of the vertex set $V$ as a set of monitor vertices (say $M = \{m_1, m_2, \ldots, m_{|M|}\}$) on which to place a sensor at each selected monitor vertex. Due to practical reasons, the number of utilized sensors should be constrained. Let us denote $n_s$ as the sensor budget that is the maximum number of utilized sensors, i.e., $|M| \leq n_s$.

On the other hand, the malicious adversary selects a vertex $a \in V$ on which to conduct an additive time-dependent attack signal $\zeta(t) \in \mathbb{R}$, where $\zeta \in L_{2e}$, at its input as follows:

$$u_a(t) = -\theta_a x_a(t) + \sum_{j \in N_a} (x_j(t) - x_a(t)) + \zeta(t).$$

(IV.3)

The purpose of the malicious adversary is to maximally disrupt the local performance of the entire network that is represented as the energy of the unknown performance vertex $\rho$ while remaining stealthy to the defender. In practice, the location of the performance vertex $\rho$ should not be revealed publicly, leading to the following reasonable assumption.
2. Problem Formulation

Assumption 1. The performance vertex $\rho$ and attack vertex $a$ are distinct, i.e., $a \in \mathcal{V}_{-\rho}$ and $\rho \in \mathcal{V}_{-a}$.

The system model (IV.1) under the control law (IV.2)-(IV.3) can be rewritten in the presence of the attack signal at the vertex $a \in \mathcal{V}_{-\rho}$ with outputs of the performance vertex $\rho$ and outputs observed at the monitor vertices $m_k \in \mathcal{M}$

\[
\dot{x}(t) = -\bar{L}x(t) + e_a \zeta(t), \quad (IV.4)
\]
\[
y_{\rho}(t) = e_{\rho}^T x(t), \quad (IV.5)
\]
\[
y_{\mathcal{M}}(t) = C_{\mathcal{M}}^T x(t), \quad (IV.6)
\]
where $C_{\mathcal{M}} = [e_{m_1}, e_{m_2}, \ldots, e_{m_{|\mathcal{M}|}}]$, $\bar{L} = L + \Theta$, and $\Theta = \text{diag}(\theta_1, \theta_2, \ldots, \theta_N)$. The Laplacian matrix $L$ is associated with the undirected connected graph $\mathcal{G}$ and $\theta_i \in \mathbb{R}_+$, $\forall i \in \mathcal{V}$, resulting in that all the eigenvalues of the matrix $\bar{L}$ are positive real. This property of $\bar{L}$ ensures that the state of the network $x(t)$ asymptotically converges to the origin in case of attack-free, affording us to employ the following assumption.

Assumption 2. The system (IV.4) is at its equilibrium $x_e = 0$ before being affected by the attack signal $\zeta(t)$.

In the scope of this study, we mainly focus on the stealthy data injection attack that will be defined in the following. Consider the above structure of the continuous LTI system (IV.4)-(IV.6), which we denote as $\Sigma_{\rho\mathcal{M}} \triangleq (-\bar{L}, e_a, [e_{\rho}, C_{\mathcal{M}}]^T, 0)$, with the performance output $y_{\rho}(t) = e_{\rho}^T x(t)$ and the monitor outputs $y_{m_k}(t) = e_{m_k}^T x(t)$, $\forall m_k \in \mathcal{M}$. The input signal $\zeta(t)$ of the system $\Sigma_{\rho\mathcal{M}}$ is called the stealthy data injection attack if the monitor outputs satisfy $\|y_{m_k}\|_{L_2}^2 < \delta_{m_k}$, for all $m_k \in \mathcal{M}$, in which $\delta_{m_k} > 0$ is given for each corresponding monitor vertex $m_k$ and called an alarm threshold. This means that the adversary is said to be detected if there exists at least one monitor vertex $m_k \in \mathcal{M}$ whose output energy crosses its corresponding alarm threshold $\delta_{m_k}$. Further, the impact of the stealthy data injection attack is measured via the energy of the performance vertex $\rho$ over the horizon $[0, T]$, i.e., $\|y_{\rho}\|_{L_2[0,T]}^2$.

The worst-case impact of the stealthy data injection attack conducted by the malicious adversary on the local performance will be further investigated. Then, this worst-case attack impact will be utilized to formulate the objectives of the adversary and the defender in the following subsection.

2.2 Worst-case Impact of Stealthy Attacks

Since the performance vertex $\rho$ is unknown to the adversary, we will investigate the attack impact for all the possible locations of the performance...
vertex in this subsection. We start by considering a fixed performance vertex.

**For a fixed performance vertex \( \rho \)**

According to *Assumption 1*, given a fixed performance vertex \( \rho \), the adversary selects an attack vertex \( a \in V_{-\rho} \) while the defender selects a set of monitor vertices \( \mathcal{M} (|\mathcal{M}| \leq n_s) \). The worst-case impact of stealthy attacks on the fixed performance vertex \( \rho \) is formulated as follows:

\[
J_\rho(a, \mathcal{M}) \triangleq \sup_{x(0)=0, \; \zeta \in \mathcal{L}_{2e}} \|y_\rho\|_{\mathcal{L}_2}^2 \\
\text{s.t.} \quad \|y_{m_k}\|_{\mathcal{L}_2}^2 \leq \delta_{m_k}, \; \forall m_k \in \mathcal{M}.
\]

(IV.7)

The dual problem of (IV.7) is given as follows:

\[
\inf_{\gamma_{m_k} > 0} \left[ \sup_{x(0)=0, \; \zeta \in \mathcal{L}_{2e}} \left( \|y_\rho\|_{\mathcal{L}_2}^2 - \sum_{m_k \in \mathcal{M}} \gamma_{m_k} \|y_{m_k}\|_{\mathcal{L}_2}^2 \right) \right. \\
\left. + \sum_{m_k \in \mathcal{M}} \gamma_{m_k} \delta_{m_k} \right].
\]

(IV.8)

The dual problem (IV.8) is bounded only if \( \|y_\rho\|_{\mathcal{L}_2}^2 - \sum_{m_k \in \mathcal{M}} \gamma_{m_k} \|y_{m_k}\|_{\mathcal{L}_2}^2 \leq 0, \; \forall \zeta \in \mathcal{L}_{2e} \) and \( x(0) = 0 \), which results in the following minimization problem:

\[
J_\rho(a, \mathcal{M}) = \min_{\gamma_{m_k} > 0} \sum_{m_k \in \mathcal{M}} \gamma_{m_k} \delta_{m_k},
\]

(IV.9)

\[
\text{s.t.} \quad \|y_\rho\|_{\mathcal{L}_2}^2 - \sum_{m_k \in \mathcal{M}} \gamma_{m_k} \|y_{m_k}\|_{\mathcal{L}_2}^2 \leq 0, \\
x(0) = 0, \; \forall \zeta \in \mathcal{L}_{2e}.
\]

The strong duality can be proven by utilizing S-Procedure [126, Ch. 4]. Recalling the key results in dissipative system theory for linear systems with quadratic supply rates [127], the constraint in (IV.9) can be translated into a linear matrix inequality [124, Prop. 1] as follows:

\[
J_\rho(a, \mathcal{M}) = \min_{\gamma_{m_k} > 0, \; P = P^\top \geq 0} \sum_{m_k \in \mathcal{M}} \gamma_{m_k} \delta_{m_k},
\]

(IV.10)

\[
\text{s.t.} \quad \begin{bmatrix} -\bar{L}P - P\bar{L} & Pe_a \\ e_a^\top P & 0 \end{bmatrix} + \begin{bmatrix} e_\rho \\ 0 \end{bmatrix} \begin{bmatrix} e_\rho^\top & 0 \end{bmatrix} \leq 0,
\]

\[
- \sum_{m_k \in \mathcal{M}} \gamma_{m_k} \begin{bmatrix} e_{m_k} \\ 0 \end{bmatrix} \begin{bmatrix} e_{m_k}^\top & 0 \end{bmatrix} \leq 0.
\]
To guarantee the existence of a solution to the optimization problem (IV.10), we need to show the feasibility of the optimization problem (IV.7). This feasibility will be studied in Section 3 after we formulate the expected worst-case impact of stealthy attacks in the case of a probabilistic performance vertex in the following subsection.

**For a probabilistic performance vertex**

Due to the importance of the performance vertex \( \rho \), its location should not be revealed publicly. Thus, to investigate the worst-case impact of stealthy attacks (IV.7), the malicious adversary considers the location of the performance vertex \( \rho \) in a probabilistic way, described by conditional probabilities, i.e., given an attack vertex \( a \in \mathcal{V} \), the conditional probability \( \pi^a(\rho|a) \) \( (0 < \pi^a(\rho|a) < 1, \ \forall \rho \neq a) \) stands for the belief of the malicious adversary in the location of the performance vertex \( \rho \). To neutralize the malicious adversary, the defender selects a probability distribution to the target vertex of the malicious adversary, analogously denoted by \( \pi^d(\rho|a) \) \( (0 < \pi^d(\rho|a) < 1, \ \forall \rho \neq a) \). According to Assumption 1, one has \( \sum_{\rho \in \mathcal{V}_{-a}} \pi^d(\rho|a) = 1 \) and \( \sum_{\rho \in \mathcal{V}_{-a}} \pi^d(\rho|a) = 1 \).

Considering the uncertain objectives of the two agents in probabilistic ways leads to their objective functions in the following. When the defender selects the set of monitor vertices \( \mathcal{M} \) and the adversary selects attack vertex \( a \), the defender desires to minimize the following cost:

\[
R(a, \mathcal{M}) = c(|\mathcal{M}|) + \sum_{\rho \in \mathcal{V}_{-a}} \pi^d(\rho|a)J_\rho(a, \mathcal{M}), \tag{IV.11}
\]

where \( c(|\mathcal{M}|) \) is a cost for the number of utilized sensors. This sensor-to-cost function \( c(|\mathcal{M}|) \) has the following properties: 1) it significantly increases as the number of utilized sensors increases, and 2) it is bounded for any monitor set \( \mathcal{M} \subseteq \mathcal{V} \). Meanwhile, the malicious adversary desires to maximize the following expected worst-case impact of stealthy attacks:

\[
Q(a, \mathcal{M}) = \sum_{\rho \in \mathcal{V}_{-a}} \pi^a(\rho|a)J_\rho(a, \mathcal{M}). \tag{IV.12}
\]

From (IV.7), \( J_\rho(a, \mathcal{M}) \) is non-negative for every pair of attack vertex \( a \) and monitor set \( \mathcal{M} \). Thus, the cost \( R(a, \mathcal{M}) \) and the expected worst-case impact of stealthy attacks \( Q(a, \mathcal{M}) \) are bounded when the worst-case impact of stealthy attacks (IV.7) on every performance vertex \( \rho \in \mathcal{V}_{-a} \) is bounded. In the next section, we will present how the defender finds a set of admissible monitor vertices \( \mathcal{M} \) that guarantees the boundedness of the worst-case impact of stealthy attacks (IV.7) for every attack vertex.
Remark 1. In a similar scenario, another objective function based on $L^2$-gain for both the adversary and the defender has been proposed in [121, Sec. 3]. The objective function in [121, Sec. 3] was formulated in terms of the maximal $L^2$-gains from the attack vertex $a$ to the performance vertex $\rho$ and from the attack vertex $a$ to the monitor vertex $m_k$. More specifically, the objective function in [121, Sec. 3] is given by

$$W_\rho(a, m_k) = \sup_{\|\zeta\|_{L^2} \neq 0} \frac{\|y_\rho\|^2_{L^2}}{\|\zeta\|^2_{L^2}} - \lambda \sup_{\|\zeta\|_{L^2} \neq 0} \frac{\|y_{m_k}\|^2_{L^2}}{\|\zeta\|^2_{L^2}}, \quad (\lambda \geq 0).$$

The above objective $W_\rho(a, m_k)$ also considers two different outputs $y_\rho(t)$ and $y_{m_k}(t)$, but note that the output energies are maximized separately, thus leading to two different optimal input signals $\zeta(t)$ in general cases. By contrast, our objective function (IV.7) considers the worst-case impact of stealthy attacks that is simultaneously characterized by the multiple outputs $y_\rho(t)$ and $y_{m_k}(t)$ with respect to a single input signal $\zeta(t)$.

3 Characterizing the Set of Monitor Vertices

In this section, we first provide an upper bound of the worst-case impact of stealthy attacks (IV.7). The feasibility of this upper bound is guaranteed by a necessary and sufficient condition. From the investigation of this upper bound, we provide a graph-theoretic necessary and sufficient condition under which the cost (IV.11) and the expected worst-case impact (IV.12) are bounded. This condition, then, allows us to limit the admissible actions of the defender. In the remainder of this section, we show how the defender characterizes their admissible actions.

3.1 Evaluating the Worst-case Impact of Stealthy Attacks

The following lemma states a key property of the worst-case impact of stealthy attacks (IV.7).

Lemma 1. Consider the continuous LTI system $\Sigma_M = (\bar{L}, e_a, C_M^T, 0)$ with a given performance vertex $\rho$, an attack vertex $a \in V_{-\rho}$, and a non-empty monitor vertex set $\mathcal{M}$, the worst-case impact (IV.7) has an upper bound:

$$J_\rho(a, \mathcal{M}) \leq \underline{J}_\rho(a, \mathcal{M}), \quad (IV.13)$$

where

$$\underline{J}_\rho(a, \mathcal{M}) = \min_{m_k \in \mathcal{M}} \left\{ \sup_{x(0)=0, \zeta \in L_{2e}} \frac{\|y_\rho\|^2_{L^2}}{\|\zeta\|^2_{L^2}} \left| \begin{array}{c} \text{s.t.} \quad \|y_{m_k}\|^2_{L^2} \leq \delta_{m_k} \end{array} \right. \right\}. \quad (IV.14)$$
3. Characterizing the Set of Monitor Vertices

Proof: The proof is postponed to Appendix A. ■

Lemma 1 enables us to guarantee the boundedness of the worst-case impact of stealthy attacks (IV.7) through considering the isolated worst-case impact of stealthy attacks (IV.14) at a single monitor vertex $m_k \in \mathcal{M}$. Next, at the first stage in the investigation of the boundedness of the worst-case impact of stealthy attacks (IV.14), we adopt a result in [123]. Inspired by [123, Th. 2], the feasibility of the optimization problem (IV.14) is related to the invariant zeros of $\Sigma_{\rho} \triangleq (-\bar{L}, e_a, e_{p}^\top, 0)$ and $\Sigma_{m_k} \triangleq (-\bar{L}, e_a, e_{m_k}^\top, 0)$, which are defined as follows.

Definition 1 (Invariant zeros). Consider the strictly proper LTI system $\Sigma \triangleq (\bar{A}, \bar{B}, \bar{C}, 0)$ where $\bar{A}, \bar{B},$ and $\bar{C}$ are real matrices with appropriate dimensions. A tuple $(\bar{\lambda}, \bar{x}, \bar{g}) \in \mathbb{C} \times \mathbb{C}^N \times \mathbb{C}$ is a zero dynamics of $\Sigma$ if it satisfies

\[
\begin{bmatrix}
\bar{\lambda}I - \bar{A} & -\bar{B} \\
\bar{C} & 0
\end{bmatrix}
\begin{bmatrix}
\bar{x} \\
\bar{g}
\end{bmatrix} =
\begin{bmatrix}
0 \\
0
\end{bmatrix}, \quad \bar{x} \neq 0.
\] (IV.15)

In this case, a finite $\bar{\lambda}$ is called a finite invariant zero of the system $\Sigma$. Further, the strictly proper system $\Sigma$ always has at least one invariant zero at infinity [128, Ch. 3].

More specifically, to guarantee the boundedness of the worst-case impact of stealthy attacks (IV.14), let us state the following lemma.

Lemma 2 ([123, Th. 2]). Consider the following continuous LTI systems $\Sigma_{\rho} \triangleq (-\bar{L}, e_a, e_{p}^\top, 0)$ and $\Sigma_{m_k} \triangleq (-\bar{L}, e_a, e_{m_k}^\top, 0)$, $\forall m_k \in \mathcal{M}$. The optimization problem (IV.14) is feasible if, and only if, there exists at least one system $\Sigma_{m_k}$ such that its unstable invariant zeros are also invariant zeros of $\Sigma_{\rho}$.

Proof: The proof follows directly the result in [123, Th. 2]. ■

The result in Lemma 2 enables us to investigate invariant zeros of $\Sigma_{m_k}$. Let us adopt the following lemma from our previous work [148] that considers finite invariant zeros of $\Sigma_{m_k}$.

Lemma 3 ([148, Lem. 4.4]). Consider a networked control system associated with an undirected connected graph $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, A)$, whose closed-loop dynamics is described in (IV.4). Suppose that the networked control system is driven by the stealthy data injection attack at a single attack vertex $a$, and observed by a single monitor vertex $m_k$, resulting in the state-space model $\Sigma_{m_k} \triangleq (-\bar{L}, e_a, e_{m_k}^\top, 0)$. Then, there exist self-loop control gains $\theta_i$, $\forall i \in \{1, 2, \ldots, N\}$, in (IV.2) such that $\Sigma_{m_k}$ has no finite unstable invariant zero.
Proof: The proof is postponed to Appendix B.

Lemma 3 enables us to carefully design the control law (IV.2) such that for every pair of an input vertex \( a \) and an output vertex \( m_k \), the corresponding LTI system \( \Sigma_{m_k} = (-\bar{L}, e_a, e_{m_k}^\top, 0) \) has no unstable invariant zero. Hence, it leaves us to investigate infinite invariant zeros of systems \( \Sigma_{m_k}, \forall m_k \in \mathcal{M} \) in the following subsection.

3.2 Infinite Invariant Zeros

We investigate the infinite invariant zeros of the systems \( \Sigma_\rho \) and \( \Sigma_{m_k}, \forall m_k \in \mathcal{M} \). In the investigation, we make use of known results connecting infinite invariant zeros mentioned in Definition 1 and the relative degree of a linear system, which is defined below.

Definition 2 (Relative degree [35, Ch. 13]). Consider the strictly proper LTI system \( \bar{\Sigma} \triangleq (\bar{A}, \bar{B}, \bar{C}, 0) \) with \( \bar{A} \in \mathbb{R}^{n \times n} \), \( \bar{B} \), and \( \bar{C} \) are real matrices with appropriate dimensions. The system \( \bar{\Sigma} \) is said to have relative degree \( r \) (\( 1 \leq r \leq n \)) if the following conditions satisfy

\[
\bar{C} \bar{A}^k \bar{B} = 0, \quad 0 \leq k < r - 1,
\]

\[
\bar{C} \bar{A}^{r-1} \bar{B} \neq 0.
\]

Remark 2. Let \( \bar{H}(s) = \bar{C}(sI - \bar{A})^{-1} \bar{B} \) be the transfer function of the above system \( \bar{\Sigma} \). The relative degree \( r \) of the system \( \bar{\Sigma} \) defined in Definition 2 is also the difference between the degrees of the denominator and the numerator of \( \bar{H}(s) \) [35], which in turn corresponds to the degree of the infinite zero if \( \bar{\Sigma} \) is minimal realization [128, Ch. 3].

Based on Definition 2, let us denote \( r_{(\rho,a)} \) and \( r_{(m_k,a)} \) as the relative degrees of \( \Sigma_\rho \) and \( \Sigma_{m_k} \), respectively. In the scope of this study, we have assumed that the attack signal \( \zeta(t) \) in (IV.3) has no direct impact on the outputs (IV.5) and (IV.6), resulting in strictly proper systems \( \Sigma_\rho \) and \( \Sigma_{m_k} \). This implies that the relative degrees \( r_{(\rho,a)} \) and \( r_{(m_k,a)} \) of the systems \( \Sigma_\rho \) and \( \Sigma_{m_k} \) are positive, yielding their infinite invariant zeros. Let us state the following theorem that considers infinite invariant zeros of the systems \( \Sigma_\rho \) and \( \Sigma_{m_k} \) to provide a necessary and sufficient condition under which the boundedness of the worst-case impact of stealthy attacks (IV.14) is guaranteed.

Theorem 1. Consider the strictly proper LTI systems \( \Sigma_\rho \triangleq (-\bar{L}, e_a, e_{\rho}^\top, 0) \) and \( \Sigma_{m_k} \triangleq (-\bar{L}, e_a, e_{m_k}^\top, 0), \forall m_k \in \mathcal{M} \), in which the systems have the same stealthy data injection attack input (IV.3) at a single attack vertex
3. Characterizing the Set of Monitor Vertices

$a \in \mathcal{V}_{-\rho}$ but different output vertices (IV.5)-(IV.6), i.e., $\rho$ for $\Sigma_\rho$ and $m_k$ for $\Sigma_{m_k}$. Suppose the systems $\Sigma_\rho$ and $\Sigma_{m_k}$ have relative degrees $r_{(\rho,a)}$ and $r_{(m_k,a)}$, respectively. Then, the worst-case impact of stealthy attacks (IV.14) is bounded if, and only if, there exists at least one system $\Sigma_{m_k}$ such that the following condition holds

$$r_{(m_k,a)} \leq r_{(\rho,a)}. \quad \text{(IV.17)}$$

**Proof:** The proof is postponed to Appendix C.

Given a probabilistic performance vertex $\rho$ and an arbitrary attack vertex $a \in \mathcal{V}_{-\rho}$, Theorem 1 hints a solution to detecting malicious activities. The defender might choose a non-empty monitor set $\mathcal{M} \subseteq \mathcal{V}$ such that there always exists at least one monitor vertex $m_k \in \mathcal{M}$ that fulfills the condition (IV.17). The following subsection presents how to find such a monitor set $\mathcal{M}$.

**Remark 3.** Let us consider the following continuous LTI system $\Sigma_{\mathcal{M}} = (-\bar{L}, e_a, C_{\mathcal{M}}^T, 0)$ where its input is at the vertex $a$ and its outputs are at monitor vertices $m_k \in \mathcal{M}$. By employing the definition of the relative degree of single-input-multiple-output systems, adapted from [149], the relative degree of the system $\Sigma_{\mathcal{M}}$ is the least relative degree from its input to its single monitor vertex. Thus, we need to find at least one monitor vertex $m_k$ such that it fulfills the condition (IV.17), resulting in the boundedness of (IV.14). This result eventually allows us to guarantee that the worst-case impact of stealthy attacks in (IV.7) is bounded according to the property in (IV.13).

### 3.3 Dominating Sets

Consider a subset $\mathcal{M} \subseteq \mathcal{V}$ where its cardinality is not greater than the sensor budget $n_s$, the maximum number of available sensors, i.e., $\mathcal{M} = \{m_1, m_2, \ldots, m_{|\mathcal{M}|}\}$ and $|\mathcal{M}| \leq n_s$. A monitor set $\mathcal{M}$ is admissible if it contains at least one monitor vertex $m_k \in \mathcal{M}$ such that this vertex $m_k$ fulfills the necessary and sufficient condition (IV.17) in Theorem 1. This set $\mathcal{M}$ is called a dominating set which is defined below.

**Definition 3 (Dominating set).** Given an undirected graph $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, \mathcal{A})$, a subset of the vertex set $\mathcal{D} \subseteq \mathcal{V}$ is called a dominating set if, for every vertex $u \in \mathcal{V} \setminus \mathcal{D}$, there is a vertex $v \in \mathcal{D}$ such that $(u, v) \in \mathcal{E}$. 

The following lemma presents a necessary and sufficient condition under which a subset of the vertex set is a dominating set.
Lemma 4. Consider an undirected graph $G = (V, E, A)$, a subset $M \subseteq V$ is a dominating set of $V$ if, and only if, the following condition holds

$$\|C(M)\|_0 = N,$$  \hfill (IV.18)

where $C(M) = \sum_{m_k \in M} (A + I)e_{m_k}$ and $N$ is the cardinality of the vertex set $V$.

Proof: The proof is postponed to Appendix D.

By investigating all the subsets of $V$, we can find all the dominating sets which fulfill the condition (IV.18). Let us make use of the following assumption.

Assumption 3. The vertex set $V$ has at least one dominating set such that it contains at most $n_s$ elements.

Based on Assumptions 1-3 and the above results in Lemma 1 and Theorem 1, we are now ready to state the following theorem that provides a graph-theoretic necessary and sufficient condition under which the cost (IV.11) and the expected worst-case impact of stealthy attacks (IV.12), caused by the stealthy data injection attack at an arbitrary attack vertex $a$, are bounded.

Theorem 2. Suppose that Assumptions 1-3 hold. Consider the networked control system (IV.4) associated with an undirected connected graph $G$ where the system has the stealthy data injection attack (IV.3) at the input of an arbitrary attack vertex $a$ and outputs (IV.6) at monitor vertices $m_k \in M$. The cost $R(a, M)$ in (IV.11) and the expected worst-case impact of stealthy attacks $Q(a, M)$ in (IV.12) are bounded if, and only if, the monitor set $M$ is a dominating set of $G$.

Proof: Let us consider the following continuous LTI systems $\Sigma_{\rho} \triangleq (-\bar{L}, e_a, e_{\rho}^T, 0)$ and $\Sigma_{m_k} \triangleq (-\bar{L}, e_a, e_{m_k}^T, 0), \forall m_k \in M$. The systems have the same stealthy data injection attack at the input of an arbitrary attack vertex $a$ but $\Sigma_{\rho}$ has an output at an arbitrary performance vertex $\rho$ and $\Sigma_{m_k}$ has an output at monitor vertex $m_k$. Based on Definition 2, Assumption 1 guarantees that the relative degree of $\Sigma_{\rho}$ is not lower than one, i.e., $r_{(\rho,a)} \geq 1$.

We begin by providing sufficiency. Assumption 3 ensures that there exists at least one dominating set that has at most $n_s$ elements. Therefore, the defender selects the monitor set $M$ as one of such dominating sets. According to Definitions 2-3, there exists at least one system $\Sigma_{m_k}$, where its input is at an arbitrary attack vertex $a$ and its output is at the monitor.
vertex \( m_k \) \((m_k \in \mathcal{M})\), such that its relative degree is not greater than one, i.e., \( r_{(m_k,a)} \leq 1 \).

Based on the above observation, one has

\[
r_{(m_k,a)} \leq 1 \leq r_{(\rho,a)},
\]

fulfilling the condition \((IV.17)\). From the results in \textit{Theorem 1 and Lemma 1}, the satisfaction of \((IV.17)\) allows us to guarantee the boundedness of the worst-case impact of stealthy attacks \((IV.7)\). Therefore, the cost \( R(a,\mathcal{M}) \) and the expected worst-case impact of stealthy attacks \( Q(a,\mathcal{M}) \) are bounded based on their definitions in \((IV.11)-(IV.12)\).

For necessity, let us present a contradiction argument by assuming that the cost \( R(a,\mathcal{M}) \) and the expected worst-case impact of stealthy attacks \( Q(a,\mathcal{M}) \) are bounded while the monitor set \( \mathcal{M} \) is not a dominating set of \( G \). Based on the definitions of \( Q(a,\mathcal{M}) \) and \( R(a,\mathcal{M}) \) in \((IV.11)-(IV.12)\), they are bounded if, and only if, \( J_{\rho}(a,\mathcal{M}) \) is bounded for all pairs of \( \rho \) and \( a \). Since the attack vertex \( a \) can be chosen arbitrarily and the monitor set \( \mathcal{M} \) is not a dominating set, the attack vertex \( a \) can be chosen such that it does not belong to \( \mathcal{M} \) and none of its neighbors belongs to \( \mathcal{M} \), resulting in \( r_{(m_k,a)} > 1 \ \forall m_k \in \mathcal{M} \). On the other hand, the adversary considers all the possibilities of the performance vertex \( \rho \) including \((\rho,a) \in \mathcal{E}\), resulting in \( r_{(\rho,a)} = 1 \). The above observation gives us

\[
r_{(\rho,a)} = 1 < r_{(m_k,a)}, \ \forall m_k \in \mathcal{M}; \tag{IV.19}
\]

violating the necessary and sufficient condition \((IV.17)\). Hence, for this particular pair of \( \rho \) and \( a \), the worst-case impact of stealthy attacks \( J_{\rho}(a,\mathcal{M}) \) is unbounded, contradicting the assumption.

\textit{Lemma 4} enables us to determine whether a subset of \( \mathcal{V} \) is a dominating set. On the other hand, \textit{Theorem 2} affords us to restrict the admissible actions of the defender to dominating sets of \( \mathcal{V} \). This step is beneficial to the defender in selecting monitor vertices such that the cost \((IV.11)\) and the worst-case impact of stealthy attacks \((IV.12)\) are always bounded. More detail on how the defender and the malicious adversary select their actions will be given in the following section.

\textbf{Remark 4.} \textit{Regarding the concept of dominating sets, Lemma 4 is an alternative presentation of Definition 3. We can easily see their equivalence through the proof of Lemma 4 in Appendix 7. Given the graph configuration consisting of vertices and edges, Definition 3 affords us to characterize dominating sets. Meanwhile, Lemma 4 provides an algebraic condition that allows us to find dominating sets when the adjacency matrix and canonical basis vectors, representing single vertices, are given.}
4 Stackelberg Security Game

In this section, to assist the defender and the malicious adversary in selecting their best actions, we employ the Stackelberg game-theoretic framework where the defender acts as the leader and the malicious adversary acts as the follower of the game. Subsequently, we provide an algorithm to illustrate the procedure of how the two agents seek their best actions.

4.1 Game Setup

To investigate the best actions of the defender and the adversary, we assume that they are two strategic players in a game. The defender can select at most $n_s$ monitor vertices on which to place one sensor at each selected vertex with the purpose of detecting malicious activities. Given Assumption 3, let us denote the set of dominating sets as $D$, where each dominating set has at most $n_s$ elements, i.e., $D = \{ M | M \subseteq V, |M| \leq n_s, M \text{satisfies (IV.18)} \}$. This set $D$ is chosen as the action space of the defender. Meanwhile, the malicious adversary is able to select any vertex to conduct the stealthy data injection attack, i.e., the action space of the malicious adversary is $A = V$, the vertex set.

Based on the catastrophic consequences caused by famous malware such as Stuxnet and Industroyer [56, 135], the defender should decide their defense strategy regardless of the presence of malicious adversaries since the defender does not know when adversaries appear. Thus, it is reasonable to let the defender select and announce their action publicly before the presence of the adversary [114, 116]. The defender is called the leader of the Stackelberg game [102]. The purpose of the defender is to minimize the cost function $R(a, M)$ in (IV.11). Subsequently, after observing the leader’s action, the adversary, with the full system knowledge, selects their action with the purpose of maximizing the expected worst-case impact of stealthy attacks (IV.12). The adversary is called the follower. Let us summarize the resources and the purposes of the defender and the malicious adversary as follows:

Model knowledge

The defender and the malicious adversary have the following information, i.e., they know the vertex set $V$, the edge set $E$, the self-loop gains $\theta_i$ ($\forall i \in V$), the alarm threshold $\delta_i$ ($\forall i \in V$), the sensor budget $n_s$, the cost for the number of utilized sensors $c(|M|)$. On the other hand, given an attack vertex $a$, the defender and the adversary have their own probability distributions to the performance vertex $\rho$, i.e., the defender considers the malicious target through the conditional probability $\pi^d(\rho|a)$ while the adversary assumes
Table IV.2: Components of the Stackelberg security game between a defender and a malicious adversary.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Players</td>
<td>Defender and Adversary</td>
</tr>
</tbody>
</table>
| Action Space    | Defender: $D = \{ \mathcal{M} \mid \mathcal{M} \subseteq \mathcal{V}, |\mathcal{M}| \leq n_s, (IV.18) \}$
|                 | Adversary: $A = \{ a \mid a \in \mathcal{V} \}$                           |
| Game Payoff & Goal | Defender minimizes $R(a, \mathcal{M})$ defined in (IV.11)  |
|                 | Adversary maximizes $Q(a, \mathcal{M})$ defined in (IV.12)                |
| Information     | Defender takes action first                                                 |
| Structure       | Adversary responds to Defender’s action                                    |

the location of the performance vertex through the conditional probability $\pi^a(\rho|a)$.

**Action space**

The malicious adversary can select any attack vertex $a \in \mathcal{V}$ and assume that this attack vertex is distinct from the performance vertex $\rho$, i.e., $a \neq \rho$. Meanwhile, due to the sensor budget $n_s$ and the boundedness of the cost (IV.11) and the expected worst-case impact of stealthy attacks (IV.12) given from Theorem 2, the defender is only allowed to select an element in $D$ that contains dominating sets.

**Objective**

The defender wants to minimize the cost function $R(a, \mathcal{M})$ in (IV.11) by selecting an optimal dominating set $\mathcal{M}^* \in D$ with knowing that the malicious adversary bases their action on the defender’s decision. Given the action of the defender, the malicious adversary desires to maximize the expected worst-case impact of stealthy attacks $Q(a, \mathcal{M})$ in (IV.12) by selecting an optimal attack vertex $a^*(\mathcal{M}^*) \in A = \mathcal{V}$. Thus, the leader considers the following problem.

**Problem 2.** The defender is required to select an optimal dominating set $\mathcal{M}^* \in D$ that minimizes the cost (IV.11).

The components of the Stackelberg game between the defender and the malicious adversary are summarized in Table IV.2. We cast the Problem 2 in the Stackelberg game-theoretic framework with the defender as the leader, who selects and announces their action first, and the malicious adversary as the follower. This Stackelberg game always admits an optimal action [102], which is defined below.
Definition 4 (Stackelberg optimal action [150]). If there exists a mapping \( T : \mathcal{D} \rightarrow \mathcal{A} \) such that, for any fixed \( M \in \mathcal{D} \), one has \( Q(TM, M) \geq Q(a, M) \) for all \( a \in \mathcal{A} \), and if there exists \( M^* \in \mathcal{D} \) such that \( R(TM^*, M^*) \leq R(TM, M) \) for all \( M \in \mathcal{D} \), then the pair \((a^*(M^*), M^*)\) is called a Stackelberg optimal action with the defender as the leader and the adversary as the follower of the game.

Based on Definition 4, we first analyze the Stackelberg optimal action and then provide an algorithm that finds it in the following subsection.

4.2 Stackelberg Optimal Action

Recall Problem 2 and Definition 4, the defender finds their optimal action by solving the following optimization problem:

\[
\mathcal{M}^* = \arg \min_{\mathcal{M} \in \mathcal{D}} R(a^*(\mathcal{M}), \mathcal{M}), \tag{IV.20}
\]

where

\[
a^*(\mathcal{M}) = \arg \max_{a \in \mathcal{A}} R(a, \mathcal{M}). \tag{IV.21}
\]

After observing the defender’s optimal action, the adversary finds their optimal action by solving the following optimization problem:

\[
a^*(\mathcal{M}^*) = \arg \max_{a \in \mathcal{A}} Q(a, \mathcal{M}^*). \tag{IV.22}
\]

One can verify that the optimal solution \((a^*(\mathcal{M}^*), \mathcal{M}^*)\) found through the optimization problems (IV.20)-(IV.22) is equivalent to the one in Definition 4. Finally, the procedure of finding the Stackelberg optimal action for the adversary and the defender \((a^*(\mathcal{M}^*), \mathcal{M}^*)\) is summarized in Algorithm 2.

5 Computational Complexity

In this section, we highlight the benefits of characterizing admissible monitor sets as dominating sets to the computation, especially in large-scale networked control systems.

The defender is allowed to select at most \( n_s \) monitor vertices to place sensors. Thus, if the defender selects \( k \) \((k \leq n_s)\) vertices, the defender has \( k \)-combinations of the vertex set \( \mathcal{V} \). Next, we compute the number of all the possible subsets of the vertex set \( \mathcal{V} \) in which each subset has at most \( n_s \) elements. Let us denote the number of possible subsets of the vertex set \( \mathcal{V} \)
Algorithm 2 Stackelberg optimal action

Input:  The vertex set $\mathcal{V}$, the edge set $\mathcal{E}$, the self-loop gains $\theta_i$, the alarm thresholds $\delta_i$, $\forall i \in \mathcal{V}$, the sensor budget $n_s$, the cost of utilized sensors $c(|M|)$, and the conditional probabilities $\pi_a(\rho|a)$ and $\pi_d(\rho|a)$. The defender is the leader and the malicious adversary is the follower of the Stackelberg security game.

Output: The best set of monitor vertices $M^*$ and the best attack vertex $a^*(M^*)$.

Initialize: $\mathbb{D} = \emptyset$

1: for every subset $M \subseteq \mathcal{V}$ where $|M| \leq n_s$ do
2: if $M$ fulfills the condition (IV.18) then append $M$ to $\mathbb{D}$
3: end if
4: end for
5: for every pair of $M \in \mathbb{D}$ and $a \in \mathcal{V}$ do
6: for every performance vertex $\rho \in \mathcal{V}_{-a}$ do
7: solve (IV.10) to obtain the worst-case impact of stealthy attacks $J_{\rho}(a,M)$.
8: end for
9: Compute the cost for the defender $R(a,M)$ through (IV.11) and the average worst-case impact of stealthy attacks $Q(a,M)$ through (IV.12).
10: end for
11: For each action $M \in \mathbb{D}$ by the defender, find the best response $a^*(M)$ through solving (IV.21).
12: The defender (the leader) selects their best action $M^*$ by solving (IV.20).
13: The malicious adversary (the follower) selects their best response $a^*(M^*)$ by solving (IV.22).

as $S(N,n_s)$ where $N$ is the number of vertices in the network and $n_s$ is the sensor budget. This number $S(N,n_s)$ can be computed as follows:

$$S(N,n_s) = \sum_{k=1}^{n_s} \binom{N}{k}.$$  \hspace{1cm} (IV.23)

This number $S(N,n_s)$ grows dramatically when either the number of vertices $N$ or the sensor budget $n_s$ increases due to $S(N,n_s) = \mathcal{O}(N^{n_s})$, where $\mathcal{O}$ stands for Big O notation.

Let us take some numerical examples to illustrate the above claim. For $n_s = 3$ and $N = 50$, one has $S(50,3) = \sum_{k=1}^{3} \binom{50}{k} = 20875$; for $n_s = 3$ and $N = 100$, one has $S(100,3) = \sum_{k=1}^{3} \binom{100}{k} = 166750$; for $n_s = 4$ and $N = 50$
Given the sensor budget $n_s = 3$, the number of subsets of the vertex set $V$ with respect to the number of vertices has the same slope as $O(N^3)$. The number of dominating sets is given through Monte-Carlo simulation with 500 samples.

One has $S(50, 4) = \sum_{k=1}^{4} \binom{50}{k} = 251175$. It is noticed that $S(100, 3)$ is almost eight times as much as $S(50, 3)$ when we just double the number of vertices. On the other hand, $S(50, 4)$ is almost twelve times as much as $S(50, 3)$ when the sensor budget slightly increases from 3 to 4. An illustration of the dramatic increase of $S(N, n_s)$ with respect to $N$ (blue dashed-dotted line) can be found in Figure IV.2 where it has the same slope as $O(N^3)$ (red dashed line). In Figure IV.2, we also conduct Monte-Carlo simulations with 500 samples to count the number of dominating sets with respect to the size of the graph $N$, which is denoted as the black dashed-dotted line. In the Monte-Carlo simulations, we examine Erdős–Rényi random undirected connected graphs $G(N, q)$ where $N$ is the number of vertices and an edge is included to connect two vertices with probability $q = 0.5$ [151].

Since the number $S(N, n_s)$ in (IV.23) represents the possible actions available to the defender, the defender should examine all of these actions to seek their optimal action against the malicious adversary. However, as the number of vertices increases, the number of possible actions grows significantly (see Figure IV.2), making it increasingly difficult to investigate large-scale systems. In contrast, the number of dominating sets typically decreases with respect to the size of random graphs (see an example in Fig-
6. Numerical Example

In the first part of this section, step-by-step of Algorithm 2 will be run to validate the result in Theorem 2 and to find the Stackelberg optimal action for the defender and the malicious adversary in an example. In the remainder of this section, the alleviation in the computational complexity will be examined.

To demonstrate the obtained results, let us consider an example of a 50-vertex networked control system depicted in Figure IV.3. Parameters of the system are selected as follows: \( \theta_i = 0.5, \delta_i = 1, \forall i \in \mathcal{V}; \) the cost for the number of utilized sensors is set as \( c(|\mathcal{M}|) = e^{\kappa |\mathcal{M}|} \) where \( \kappa = 0.2; \) beliefs of
the defender and the malicious adversary in the location of the performance vertex given an attack vertex are assumed to be uniformly distributed, i.e., \( \pi^a(\rho|a) = 1/(N-1) \) and \( \pi^d(\rho|a) = 1/(N-1) \); and the sensor budget \( n_s = 3 \).

6.1 Computing Stackelberg Optimal Action

First, we start at lines 1-4 of Algorithm 2. By investigating all the subsets \( M \subset V \) where \( |M| \leq n_s \), twenty subsets satisfy the necessary and sufficient condition (IV.18), which are dominating sets. One of those dominating sets is illustrated in Figure IV.3 where elements of a dominating set are coded blue. From Figure IV.3, let us consider a system \( \Sigma_{m_k} \overset{\Delta}{=} (-\bar{L}, e_a, e^T_{m_k}, 0) \) where \( e_a \) represents the input at any vertex and \( e_{m_k} \) represents the monitor output at a blue vertex. We simply examine that there exists at least one blue vertex such that the relative degree of \( \Sigma_{m_k} \) is never greater than one. Thus, the cost for the defender and the expected worst-case impact of stealthy attacks conducted at the input of an arbitrary vertex are always bounded according to the result in Theorem 2. This result, then, affords us to proceed to lines 5-10 of Algorithm 2 to compute the worst-case impact of stealthy attacks \( J(\rho, M) \), the cost \( R(\rho, M) \) defined in (IV.11) for the defender, and the expected worst-case impact of stealthy attacks \( Q(\rho, M) \) defined in (IV.12) for the malicious adversary. Through simulation, the maximum cost for the defender and the maximum expected worst-case impact of stealthy attacks are obtained as follows: \( R(\rho, M) \leq 50.2456 \) and \( Q(\rho, M) \leq 48.4235 \) for an arbitrary pair of a vertex \( \rho \in V \) and a dominating set \( M \), which verifies the result in Theorem 2. Finally, let us go from line 11 to line 13 of Algorithm 2 to find the Stackelberg optimal action for the defender and the malicious adversary. The optimal action \( \mathcal{M}^* \) for the defender consists of three blue vertices in Figure IV.3 that yields the minimum cost of \( R(a^*(\mathcal{M}^*), M^*) = 49.7985 \). Given such an optimal action \( \mathcal{M}^* \), the malicious adversary chooses the red vertex \( a^*(\mathcal{M}^*) \) in Figure IV.3 that allows them to maximize the expected worst-case impact of stealthy attacks at \( Q(a^*(\mathcal{M}^*), M^*) = 47.9764 \).

6.2 Computational Complexity

As discussed above, the 50-vertex networked control system (see Figure IV.3) gives us twenty dominating sets where the sensor budget is three \( (n_s = 3) \). This number is extremely smaller than the number of subsets of the vertex set which has at most \( n_s \) elements, i.e., \( S(50, 3) = 20875 \). There are 50 possibilities of attack vertex \( \rho \) due to \( \rho \neq a \) (see Assumption 1). Thus, we only need to solve \( 20 \times 50 \times 49 = 49000 \) optimization problems compared to \( 20875 \times 50 \times 49 = \).
51143750 optimization problems for investigating all the possible monitor sets. We did an experiment of solving optimization problems (IV.10) by using CVX with Matlab version 2021a [144] on a personal computer which has a configuration: CPU Intel Core i7-10700 2.9 GHz and 16 Gb RAM DDR4. It took an average of 5.12 seconds to solve the optimization problem (IV.10) once. Hence, the proposed algorithm through the concept of dominating sets in this paper approximately took 70 hours instead of 72738 hours.
7 Conclusion

In this paper, we investigated the security allocation problem in a networked control system when faced with a stealthy data injection attack. The uncertain performance vertex allowed us to formulate the objective functions of the defender and the adversary through considering probabilistic locations of the local performance. We presented a necessary and sufficient condition based on dominating sets under which the defender guarantees the boundedness of their cost and the expected worst-case impact of stealthy attacks. Since the defender should decide their action regardless of the presence of the adversary, we cast the security allocation problem in the Stackelberg game-theoretic framework. Then, we provided an algorithm to show the procedure of finding the Stackelberg optimal action with the defender as the leader and the adversary as the follower of the game. The advantage of the proposed security allocation scheme was highlighted in the context of large-scale networks via a discussion on the computational burden and several numerical simulations.

Appendix A: Proof of Lemma 1

Showing (IV.13) is trivial when the monitor vertex set $\mathcal{M}$ has only one vertex. We assume that $\mathcal{M}$ has more than one monitor vertex. From the worst-case impact of stealthy attacks (IV.7), let us introduce the following optimization by removing $|\mathcal{M}| - 1$ constraints except the constraint corresponding to a monitor vertex $m_k \in \mathcal{M}$ as follows:

$$J_\rho(a, m_k) = \sup_{x(0) = 0, \zeta \in L^2} \|y_\rho\|^2_{L^2}$$

$$\text{s.t.} \quad \|y_{m_k}\|^2_{L^2} \leq \delta_{m_k}. \quad (IV.24)$$

The design of the optimization problem (IV.24) tells us that its feasible set contains the feasible set of the optimization problem (IV.7). Further, the two optimization problems (IV.7) and (IV.24) have the same objective function. This implies that $J_\rho(a, \mathcal{M}) \leq J_\rho(a, m_k)$ for all $m_k \in \mathcal{M}$, directly resulting in (IV.13).

Appendix B: Proof of Lemma 3

Let us denote a tuple $(\bar{\lambda}_{m_k}, \bar{x}_{m_k}, \bar{g}_{m_k}) \in \mathbb{C} \times \mathbb{C}^N \times \mathbb{C}$ as a zero dynamics of $\Sigma_{m_k}$, where a finite $\bar{\lambda}_{m_k}$ is called a finite invariant zero of $\Sigma_{m_k}$. From
Definition 1, one has that the tuple \((\bar{\lambda}_{mk}, \bar{x}_{mk}, \bar{g}_{mk})\) satisfies
\[
\begin{bmatrix}
\bar{\lambda}_{mk} I + \bar{L} & -e_a \\
 e_{mk}^T & 0
\end{bmatrix}
\begin{bmatrix}
\bar{x}_{mk} \\
\bar{g}_{mk}
\end{bmatrix}
= \begin{bmatrix}
0 \\
0
\end{bmatrix}.
\] (IV.25)

The above equation is rewritten as
\[
\begin{bmatrix}
(\bar{\lambda}_{mk} - \theta_0) I + \bar{L} & -e_a \\
 e_{mk}^T & 0
\end{bmatrix}
\begin{bmatrix}
\bar{x}_{mk} \\
\bar{g}_{mk}
\end{bmatrix}
= \begin{bmatrix}
0 \\
0
\end{bmatrix},
\] (IV.26)

where \(\theta_0 \in \mathbb{R}_+\) is a uniform offset self-loop control gain. From (IV.26), the finite value \((\bar{\lambda}_{mk} - \theta_0) \in \mathbb{C}\) is an invariant zero of a new state-space model \(\hat{\Sigma}_{mk} \triangleq (-\bar{L} - \theta_0 I, e_a, e_{mk}^T, 0)\). For all \(\bar{\lambda}_{mk} \in \mathbb{C}\) satisfying (IV.26), the control gain \(\theta_0\) can be adjusted such that \(\theta_0 > \text{Re}(\bar{\lambda}_{mk})\), resulting in that \(\hat{\Sigma}_{mk}\) has no finite unstable zero. Then, the self-loop control gains \(\theta_i, i \in \{1, 2, \ldots, N\}\), in (IV.2) are tuned with \(\theta_0\) such that the system \(\Sigma_{mk}\) is identical with \(\hat{\Sigma}_{mk}\). By this tuning procedure, the system \(\Sigma_{mk}\) also has no finite unstable invariant zero.

**Appendix C: Proof of Theorem 1**

The result in Lemma 2 enables us to investigate invariant zeros of the systems \(\Sigma_\rho\) and \(\Sigma_{mk}, \forall m_k \in \mathcal{M}\). Based on Lemma 3, \(\Sigma_{mk}\) has no finite unstable invariant zero, which leaves us to analyze infinite invariant zeros of those systems. Recall the equivalence between the relative degree of a SISO system and the degree of its infinite zero (see Remark 2), a necessary condition to guarantee the feasibility of the optimization problem (IV.14) is that there exists at least one system \(\Sigma_{mk}(m_k \in \mathcal{M})\) such that the number of its infinite invariant zeros is not greater than that of the system \(\Sigma_\rho\). This implies \(r_{(mk, a)} \leq r_{(\rho, a)}\). For sufficiency, it remains to show that if \(r_{(mk, a)} \leq r_{(\rho, a)}\), all the infinite zeros of the system \(\Sigma_{mk}\) are also infinite zeros of the system \(\Sigma_\rho\). The following proof is adapted from our previous results in [137, Th. 7].

In the investigation, we make use of the definition of infinite invariant zeros in [134, Def. 2.4]. We investigate infinite zeros of \(\Sigma_{mk}\) and \(\Sigma_\rho\) by starting from their transfer functions with zero initial states
\[
G_{(\rho, a)}(s) = e_{\rho}^T (sI + \bar{L})^{-1} e_a = \frac{P_{(\rho, a)}(s)}{Q(s)},
\]
\[
G_{(mk, a)}(s) = e_{mk}^T (sI + \bar{L})^{-1} e_a = \frac{P_{(mk, a)}(s)}{Q(s)},
\] (IV.27)

where \(s \in \mathbb{C}\) is the Laplace complex variable. Based on Remark 2, it gives that \(P_{(\rho, a)}(s), P_{(mk, a)}(s), \text{ and } Q(s)\) are the polynomials of degrees \(N - r_{(\rho, a)}\),
\(N - r(m_k,a), \) and \(N,\) respectively. Let us denote \(z_\tau = \sigma_\tau + j\omega_\tau \in \mathbb{C}, \ \tau \in \{1,2,\ldots,r(m_k,a)\}\) with infinite module as infinite invariant zeros of \(\Sigma_{m_k}.\)

Indeed, the zero \(z_\tau (1 \leq \tau \leq r(m_k,a))\) is an infinite invariant zero of maximal degree \(r(m_k,a)\) of the system \(\Sigma_{m_k}\) [134, Def. 2.4] if it satisfies

\[
\lim_{\|z_\tau\| \to \infty} z_\tau^q G(m_k,a)(z_\tau) = 0, \quad (0 \leq q \leq r(m_k,a) - 1),
\]

\[
\lim_{\|z_\tau\| \to \infty} z_\tau^{r(m_k,a)} G(m_k,a)(z_\tau) \neq 0.
\]

Further, with \(0 \leq q \leq r(m_k,a) - 1,\) we also basically have

\[
\lim_{\|z_\tau\| \to \infty} z_\tau^q G(p,a)(z_\tau) = \lim_{\|z_\tau\| \to \infty} \frac{z_\tau^q P(p,a)(z_\tau)}{Q(z_\tau)} = 0.
\]

The above limit (IV.29) holds because the denominator \(z_\tau^q P(p,a)(z_\tau)\) is the polynomial of degree \(N - r(p,a) + q \leq N - 1 < N,\) where \(N\) is the degree of the polynomial \(Q(z_\tau)\). This implies that any infinite zeros \(z_\tau\) of maximal degree \(r(m_k,a)\) of the system \(\Sigma_{m_k}\) are also infinite zeros of degree \(r(m_k,a)\) of the system \(\Sigma_{p}.

### Appendix D: Proof of Lemma 4

Let us decompose \(C(M) = C_A(M) + C_I(M)\) where \(C_A(M) = \sum_{m_k \in M} A e_{m_k}\) and \(C_I(M) = \sum_{m_k \in M} e_{m_k}.\) Entry \(i\)-th of \(C_I(M)\) takes 0 if vertex \(i\) does not belong to \(M\) and 1 if vertex \(i\) belongs to \(M.\) Entry \(i\)-th of \(C_A(M)\) takes 0 if all the neighbors of vertex \(i\) do not belong to \(M\) and a non-zero value if at least one neighbor of vertex \(i\) belongs to \(M.\) Thus, entry \(i\)-th of \(C(M)\) takes 0 if vertex \(i\) and all of its neighbors do not belong to \(M;\) takes a non-zero value if vertex \(i\) or one of its neighbors belong to \(M.\) If the condition (IV.18) fulfills, the vector \(C(M)\) has no zero entry. This implies that an arbitrary vertex in \(V\) is either a vertex of \(M\) or a neighbor of a vertex of \(M,\) resulting in that \(M\) is a dominating set.
Recent licentiate theses from the Department of Information Technology

2023-002 Philipp Pilar: Integrating Prior Knowledge into Machine Learning Models with Applications in Physics

2023-001 Häkan Runvik: Modeling and Estimation of Impulsive Biomedical Systems

2022-003 Camille Clouard: Computational Statistical Methods for Genotyping Biallelic DNA Markers from Pooled Experiments

2022-002 Gustaf Borgström: Making Sampled Simulations Faster by Minimizing Warming Time

2022-001 Sam Hylamia: Secure In-body Communication and Sensing

2021-002 Karl Bengtsson Bernander: Improving Training of Deep Learning for Biomedical Image Analysis and Computational Physics

2021-001 Niklas Gunnarsson: On the Registration and Modeling of Sequential Medical Images

2020-006 David Widmann: Calibration of Probabilistic Predictive Models

2020-005 Anna Wigren: Exploiting Conjugacy in State-Space Models with Sequential Monte Carlo

2020-004 Muhammad Osama: Machine Learning for Spatially Varying Data

2020-003 Christos Sakalis: Securing the Memory Hierarchy from Speculative Side-Channel Attacks

2020-002 Ulrika Sundin: Global Radial Basis Function Collocation Methods for PDEs